

FEDERAL COURT

B E T W E N:

KEVIN A. MCLEAN

Applicant

• and -

Royal Canadian Mounted Police, Michael Duheme, Jeff Ball and Stephane Brisson

Respondents

Motion Record:Applicant's NOM #2; and Application Record (2nd Updated)

**DATE MADE: JUNE 28, 2026 (Date of Hearing: Tuesday, June 30, 2026
for NOM #2 and as proposed, NOM #1 and Application**

Pursuant to the Federal Courts Act and Federal Courts Rules

Applicant

Mr. Kevin A. McLean (BA, JD, CIM)

Applicant

Pro Se and Pro Bono Publico

68 Abell St. (Receptionist desk)

Toronto, ON

M6J 0B1

mclean@searchandseizure.ca

Fax number: 647.370.9354

Telephone number: 416.352.0055

Respondents:

Place of hearing for NOM #2: The Principal Office of Ottawa

Exclusively to the attention of the Primus Inter Pares of the Federal Court of Canada, The Honourable Justice Madam St. Louis

Date of Hearing for NOM #2: June 30, 2026 (Tuesday)



TABLE OF CONTENTS

Tab	Sub-Tab	Documents	Date	Pages	Sub-pages
0		Notice of Motion #2 Re: Acting CJ, Current ACJ self-assigning the Proceeding and Hearings to herself (see: Ruffo; 1997 Provincial Judicial Independence Reference; Baldovi; Tobias; Girouard; Dugre	June 23, 2026	I-XII	
		VOLUME #1(A): THE APPLICANT’S NOA (FORM 301)			
1		The Applicant’s Form 301 Applicant for Judicial Review pursuant to, inter alia, ss. 18 and 18.1 of the Federal Courts Act et al, and Rule 300 and 301 of the Federal Courts Rules	May 15, 2026	1-24	
		Relief Sought			6-9
		VOLUME #1(B): THE APPLICANT’S RULE 317 REQUEST			
2		THE APPLICANT’S RULE 317 REQUEST (which by its very nature include factual and legal grounds, along with meticulous particulars and pre-emptive submissions to assist with the General Principle under the Federal Courts Rules)	May 19, 2026	25-64	
		SCHEDULE OF REQUEST MATERIALS IN THE POSSESSION OF THE TRIBUNAL THAT ARE RELEVANT TO THIS APPLICATION			30-31
		VOLUME #1(C): THE APPLICANT’S PROOF OF SERVICE FOR TABS 1 AND 2			
3		THE APPLICANT’S PROOF OF SERVICE OF MAY 19, 2026 for the Applicant’s NOA (May 15, 2026) and the Applicant’s Rule 317 Request (May 19, 2026)	May 19, 2026	65-114	

		VOLUME #2: NOTICE OF MOTION OF THE APPLICANT (HEARD ON WEDNESDAY, JUNE 17, 2026)	June 10, 2026		
4		Form 359: Notice of Motion of the Applicant (“NOM #1”)	June 10, 2026	115-120	
5		Memorandum of Fact and Law for NOM #1	Jun 10, 2026	121-157	
6		Draft Order for NOM #1	June 10, 2026	158-164	
		VOLUME #3: DOCUMENTS FROM FILED APPLICATION RECORD OF JUNE 3, 2026, AND MOFL FOR JUDICIAL REVIEW APPLICATION (FORM 301) OF JUNE 3, 2026			
		Volume 3, Chapter 1 (Tabs 5 and 6): The Privacy Act (Federal) PII Access Request (March 11 2026); and Canada Post confirmed delivery			
7		The Applicant’s PII Access Request (March 11 2026) sent via mail (express post tracking) to the RCMP (Ottawa) seeking foundational metadata (not a live CPIC search in March 2026) but rather requests for, <i>inter alia</i>, the following: 1. The Foundational Metadata including the: (i) originating agency ("law enforcement applicant") identifier (“ORI”); (ii) issuing court level; (iii) issuing court “county” or “administrative region”; (iv) name of judicial officer; and (v) system identification number; 2. The Purged/Amended Data in the Offline Database (including hexadecimal dumps (if any)) (i.e. if the originally input data into CPIC was subsequently amended into congruent data with the falsification (i.e. the matching up or dovetailing of the fraud) Subjects: SUBJECT I: Statutory Request for Access to Personal Information under the Privacy Act (Canada)	March 11, 2026 (delivered)	165-172	

		SUBJECT II: Exaction of Canadian Police Information Centre Metadata Pertaining to the Promulgation of Judicial Authorizations and Concomitant Arrest Warrants SUBJECT III: Formal Demand for the Production of Offline Historical Database Audit Trails, Transaction Logs, Originating Agency Identifiers, and Systemic Non-Repudiation Artifacts			
8		The Canada Post Confirmed delivery Tracking Number: 0105952990142328 Delivered: March 11, 2026	March 11, 2026	173-174	
		VOLUME 3, CHAPTER 2: EMAILS IN THE <i>PRIVACY ACT</i> REQUEST #1, PII ACCESS REQUEST (MARCH 11 2026)			
9		Emails in the <i>Privacy Act</i> PII Access Request (March 11 2026) <i>Privacy Act</i> request P-2025-16999 / F339, Your File N/A, (nota bene: wrong year contained in the RCMP ATIP Branch file number)	March 16 to May 6, 2026	175-255	
	A	Email from Applicant to RCMP ATIP on March 16, 2026 Subject: Applicant to the RCMP in response to the below email from Ms. Simpson	March 16, 2026		176-202
	B	Initial email from Melissa Simpson of the RCMP ATIP and responses from the Applicant	March 16, 2026		203-237
	C	The False Information Package of the RCMP with the Police Case ID: 457197 with a footer on only some of the page CCO-2-000-1-C-e (rev. 10/20) (nota bene; missing on page 3 of 5 (which is the purported “warrant in the first” without the digital signature or any “signature” of a Judge let alone that of the JP Jiri with the fake logo OCJ with JP) (missing on page 4 of 5)	Falsified in 2024 – filed in OCJ 10 Armoury Street Courthouse		238-243
		Defects in the RCMP “Information Package” (Police Case ID 457197) (undisputed to be the RCMP)			

As Compared to the Authentic Criminal Code Information Package of the Lincoln County Law Association (Niagara) (Pages 4–5 of 6)

1. Missing Mandatory Page 4 of 6 – the Swearing, Attestation, and Judicial Authorization Page

What an authentic page contains (per uploaded pro forma):

Page 4 of 6 includes the statutory attestation and judicial-authorization block, including:

- **Information Number**
- **“To be completed where information is laid other than in person”**
- **“Deemed to be sworn / Réputée être faite sous serment”**
- **“Sworn/affirmed before me at the ___ of ___ in the Province of Ontario this ___ day of __, 20”**
(quoted from the uploaded document: *“Sworn/affirmed before me at the ... in the Province of Ontario this ... day of ... 20...”*)
- Name of Informant
- Name and signature block for **Justice of the Peace / Judge**
- Boxes for:
 - Appearance Notice
 - Promise to Appear
 - Recognizance
- Mandatory “Check one of the following”:
 1. Cancelled – police to notify defendant
 2. Cancelled – summons
 3. Confirmed on (date)
 4. Cancelled – warrant issued
- Signature/date line for the JP
- **Crown Election** (summary vs. indictment)
- **Election of Mode of Trial** (Judge, Judge & Jury, OCJ Judge)
- **Preliminary Hearing Requested**
- **Plea (guilty/not guilty)**
- **Disposition grid** (Committed to stand trial / Discharged / Found guilty / Found not guilty)
- **Judicial signature for consent to proceed without evidence**
(quoted: *“With consent of accused and prosecutor, without taking or recording ... any evidence / further evidence”*)

Defect:

The RCMP Information Package **omits this entire page**, eliminating:

- The **swearing/attestation** required by ss. 507–508 **Criminal Code**
- The **judicial act of receiving the Information**
- The **signature of the JP/Judge**

- The **Crown election**
- The **accused's election and plea fields**
- The **committal/discharge findings**
- The **statutory certification that the Information was sworn**

Legal

consequence:

Without this page, **no Information was sworn**, no judicial officer received it (de jure) and no prosecution could lawfully commence.

2. Missing Mandatory Page 5 of 6 – the Sentencing / Disposition Record Page

What an authentic page contains (per uploaded pro forma):

Page 5 of 6 includes:

- **Count / Chef**
- **Pre-sentence custody**
- **Sentence date**
- **Withdrawn / Stayed / Acquitted**
- **Credit for pre-sentence custody**
- **Type of sentence** (absolute discharge, conditional discharge, suspended sentence, imprisonment, intermittent sentence, conditional sentence, probation)
- **Concurrent / consecutive indicators**
- **Restitution, fines, victim surcharge**
- **Driving prohibitions, weapons prohibitions, SOIRA orders, DNA orders**
- **Judicial signature block**

(Example quoted from the uploaded document: “*Sentence date / Date de détermination de la peine ... Withdrawn / Accusation retirée ... Imprisoned for ... Conditional sentence for ... Probation ...*”)

Defect:

The RCMP Information Package **omits this entire page**, which is indispensable for:

- Recording any **withdrawal, stay, or dismissal**
- Recording any **sentence or credit**
- Recording any **judicial order** (weapons, SOIRA, DNA, etc.)
- Allowing a JP or Judge to determine whether the prosecution is **ongoing, concluded, or defective**

Legal

consequence:

A JP or Judge reviewing the package could not reasonably conclude that a valid criminal proceeding existed, because the **disposition page is structurally required** to confirm the status of the prosecution.

3. Internal Inconsistencies and Missing Footers

You noted that the RCMP package inconsistently includes the footer “**CCO-2-000-1-C-e (rev. 10/20)**”, but:

- It is **missing on page 3 of 5**, which is the purported “Warrant in the First Instance”

		- It is missing on page 4 of 5 - The “warrant” page contains no digital signature, no wet signature, and no signature of JP Jiri, despite the pro forma requiring a judicial signature block Defect: The absence of the footer on pages that purport to be part of the same Form 2 package indicates: Pages were substituted, altered, or not generated from the official template - The “warrant” page is not an authentic Form 7 warrant, nor an authentic Form 2 continuation page - The absence of any judicial signature renders the “warrant” void on its face			
		4. Structural Defect: The Package Contains Only 5 Pages Instead of 6 The authentic Form 2 is a six-page pro forma, as confirmed by the uploaded document. The RCMP package contains only five pages, and two of those five are not authentic. Defect: A Form 2 Information cannot be complete without: - Page 4 (attestation, judicial authorization, elections, pleas) - Page 5 (sentencing/disposition page) The absence of these pages means the document cannot constitute an Information under the Criminal Code and certainly not a “warrant in the first” as fraud unravels everything (see: Landreville v. Town of Boucherville, 1978 CanLII 202 (SCC)). While the putting of a false affidavit into a photocopy machine to copy was a use of it (see: R. v. Smith, 2020 ONCJ 611 (CanLII), at para 104, Additionally, in R. v. Stevenson, 1980 CanLII 2930 (ON CA), [1980] O.J. No. 1621 (C.A.), the court held that putting a false affidavit into a photocopy machine to copy it was a “use” of it. Further, Justice Kerans, in Sebo, notes that R. v. Harris, (1965) Crim. App. R. 330 (U.K. C.C.A.) provides that when a photocopy of a forgery is made for wider distribution that too is a “use” and therefore an uttering of the forged original), the “filing” of the False Information Package rendered what the Criminal Proceeding was in its alleged authentic data, leaving aside the obvious lack of merits at the time or even with a “sober second thought”, was rendered null and void at the time of filing and every step thereafter was “fruit of the falsification tree”. It is the most axiomatic statement of law that if the Criminal Proceeding was null and void so too was the criminal prosecution).			
	D	Analysis of "False Information Package" Discrepancies and GrapeCity Metadata	2025		244-248

		Some 43 plus discrepancies between the False Information Package and the standardized pro-forma from the Lincoln County Law Association (Niagara) involving the same.			
	E	The Lincoln County Law Association (Niagara) Pro Form “Information Package” (see: CCO-2-000-1-C (rev. 06/18))	2018		249-255
		VOLUME #3, CHAPTER 3:ELECTRONIC CORRESPONDENCE INVOLVING PII ACCESS REQUEST (MARCH 11 2026) (PRIVACY ACT (FEDERAL))			
		VOLUME #3, CHAPTER 3(A): EMAIL FROM MAY 6, 2026, TO APRIL 11, 2026			
10		EMAILS FROM THE APPLICANT TO THE RCMP AND FROM THE RCMP TO THE APPLICANT Reverse Chronological Order (May 6, 2026 to March 17, 2026) (under the umbrella and spirit of “access partnership”)	May 6, 2026 to March 17, 2026	256-385	
	A	Email from the Applicant to the Respondents on May 6, 2026	May 6, 2026		257-270
	B	Email from the Applicant to the Respondents on May 5, 2026	May 5, 2026		271-276
	C	Email from the Applicant to the Respondents on May 4, 2026	May 4, 2026		277-281
	D	Email from Mr. Ball (an “Individual Respondent”) of the RCMP ATIP to the Applicant on May 1, 2026 (Friday)	May 1, 2026		282-283
	E	Email from the Applicant to the Respondents on April 29, 2026	April 29, 2026		284-286

	F	Email from Mr. Ball of the RCMP ATIP to the Applicant on April 28, 2026 (Tuesday)	April 28, 2026		287-288
	G	Email from the Applicant to the Respondents on April 27, 2026	April 26, 2026		289-292
	H	Email from the Applicant to the Respondents on April 26, 2026	April 26, 2026		293-209
	I	Email from the Applicant to the Respondents on April 23, 2026	April 23, 2026		300-303
	J	Email from the Applicant to the Respondents on April 19, 2026	April 19, 2026		304-307
	K	Email from the Applicant to the Respondents on April 15, 2026	April 15, 2026		308-309
	L	Email from the Applicant to the Respondents on April 15, 2026 (second email)	April 15, 2026		310-316
		VOLUME 3, CHAPTER 2(B): Day after expiry of first 30 day interval from March 11, 2026 (date of receipt of the Applicant PII Access Request (March 11 2026)) (Respondents invoked time extension albeit on single ground of unreasonable interference with their operations on alleged reasonable grounds on March 17, 2026)			
	M	Email from the Applicant to the Respondents on April 10, 2026	April 10, 2026		317-320

	N	Email from the Applicant to the Respondents on April 10, 2026 (second email)	April 10, 2026		321-324
	O	Email from the Applicant to the Respondents on April 10, 2026	April 10, 2026		325-340
	P	Email from the Applicant to the Respondents on April 7, 2026	April 7, 2026		341-343
	Q	Email from the Applicant to the Respondents on April 7, 2026 (second email)	April 7, 2026		344-351
	R	Email from the Applicant to the Respondents on April 7, 2026 (third email)	April 7, 2026		352
	S	Email from the Applicant to the Respondents on April 7, 2026 (third email)	April 7, 2026		353-365
	T	Email from the Applicant to the Respondents on April 6, 2026 (Monday)	April 6, 2026		366-377
	U	Email from the Applicant to the Respondents on March 25, 2026 (Wednesday)	March 26, 2026		378-385
		Email from Ms. Simpson of the RCMP ATIP Branch to the Applicant: “Thank you for your email. We are currently processing your request and will make every effort to provide it as soon as possible. Please note we legislatively have 30 days to provide a response and have chosen to take an additional extension 30 days due to	March 26, 2026		

		operational requirementsⁱ. We cannot provide you a time line as to when it will be sent as there are other files in the queue that may have an impact on when your request is finalized. Regards, Ms. Melissa Simpson Access to Information and Privacy Branch Mailstop #61 73 Leikin Drive Ottawa, Ontario K1A 0R2”			
		Emails from the Applicant on March 17, 2026: Subject: Re: ATIP File – Confirmation of your purported reliance on a Section 15(a)(i) Extension under the <i>Privacy Act</i> – absent any sufficient particulars as to why the original time limit would unreasonably interfere with the operation of your government institution Interim Disclosure to Facilitate Resolutionⁱⁱ Email from Ms. Simpson of RCMP ATIP Branch to the Applicant on March 17, 2026	March 17, 2026		
		VOLUME #4: THE PURPORTED RESPONSE (OR PURPORTED DISCLOSURE DECISION OR ACCESS DECISION) OF THE RCMP ATIP BRANCH (MR. JEFFREY BALL, DIRECTOR, ATIP BRANCH OF THE RCMP)			
11		RCMP Purported Response under <i>Privacy Act</i>: The Purported Response under the Purported File Number (see: P-2025-16999) and purported release package of an active online search (not Personal Information requested in the PII Access Request (March 11 2026) of the Applicant) of the RCMP ATIP Branch	April 27, 2026	386-397	

	A	THE PURPORTED RESPONSE UNDER THE PURPORTED FILE NUMBER (SEE: P-2025-16999) (nota bene: the PII Access Request (March 11 2026) was made in 2026 and not 2025 so it is terribly concerning that the RCMP ATIP Branch cannot even input the correct year of the request into its filing protocols and it is the steward, custodian and controller of Personal Information and information and records in the RCMP CPIC database)			387-393
	B	AN APPARENT CPIC ONLINE LIVE QUERY INVOLVING MR. KEVIN A. McLEAN (BA, JD, CIM) ON APRIL 14, 2026, WHICH WAS THREE TO FOUR DAYS AFTER THE FIRST 30 DAY PERIOD. (NOTA BENE: bad faith of the RCMP in that the 30 day extension had nothing to do with the alleged or purported unreasonable interference with its operations but merely that it was putting off the required search and then it never conducted the required search of the Applicant's requested Personal Information in the PII Access Request (March 11 2026)			394-398
		VOLUME #5: THE EMAIL LEADING UP TO THE KIDNAPPING OF THE APPLICANT AT THE TPS 14TH DIVISION, BUT WITHOUT A COPY OF THE ARREST WARRANT AND REFUSING TO PRODUCE THE SAME UPON REQUEST (SEE; SECTION 29 OF THE CC) (LEADING BACK TO THE RCMP AS THE INFORMATION "LAW ENFORCEMENT APPLICANT")			
12		EMAILS INVOLVING THE INFAMOUS, SHAMEFUL AND INIQUITOUS EVENTS INVOLVING THE LAW ENFORCEMENT KIDNAPPING OF THE APPLICANT ON OCTOBER 2, 2024 AT TPS 14TH DIVISION (350 DOVERCOURT STREET, TORONTO, ONTARIO) Email from Police Officer Constable Mr. Romano of the TPS 14th Division (night of the arrest by way of "Arrest Warrant"); response of the Applicant to the TPS 14th Division confirming he would attend to obtain his property and email follow up on October 3, 2024	Oct 2 and 3, 2024	398-404	

		VOLUME #6: COMPLAINT AGAINST THE REGIONAL COM MR. MATT PEGGS WHO HAS NOT DENIED THAT HE WAS THE INFORMANT IN THE AUTHENTIC INFORMATION PACKAGE (COMPARED AGAINST THE FALSE INFORMATION PACKAGE)			
13		COMPLAINT BY THE APPLICANT TO THE CIVILIAN REVIEW AND COMPLAINTS COMMISSION FOR THE RCMP REGARDING REGIONAL COM MR. MATT PEGGS complaint by the Applicant on May 11, 2026 involving Regional COM Mr. Matt Peggs (Central Region formerly the “O” Region with the tie to the Toronto West Detachment (“TWD”) in Milton, Ontario (nota bene: tie to the worst jail in the province in Millhaven prison (see: Former RSJ Mr. Currie of the Central West Region did not want to attend; the same Central West Region of the fictitious and falsified JP Mr. Jiri on the fictitious INTAKE COURT ENDORSEMENT (SEPT 23 2024)	May 11, 2026	405-443	
		VOLUME #7: APPLICANT’S EFFORTS WITH RESPECT TO ACCESSING THE UNDERLYING AUTHENTIC RECORDS FROM THE ORIGINATING COURTHOUSE AT THE ORIGINATING COURT OFFICE TO THE RCMP INFORMANT "LAW ENFORCEMENT APPLICANT" AND THE INFORMANT HIMSELF IN REGIONAL COM (SEE: MANIPULATED LANGUAGE OF “ C L (M) “ WITH THE GRAPE CITY MANIPULATION PDF SOFTWARE (WHICH APPARENTLY MR. CURTIS MATHEW CANNOT FIND A SINGLE RECORD IN RELATION TO THE SAME BUT DOES NOT DENY THE RECORDS EXIST)			
14		FORMAL REQUEST FOR PUBLICLY ACCESSIBLE CRIMINAL COURT RECORDS, RELATING TO EVENTS SINCE AT LEAST 2024-10-02 (THE “ARREST DATE”), PURSUANT TO CORRESPONDENCE FROM POLICE OFFICER (CONSTABLE) MR. ANTHONY ROMANO DATED 2024-10-02 (ATTACHED). This request is predicated upon the retrieval of my property from Unit 410-775 King Street West, Toronto, Ontario, M5V 2K3, subsequent to 2024-09-20, and pertains to, inter alia: (i) Information(Criminal Code Form 2 Information) or Information Package, whether sworn or unsworn;(ii) any relevant judicial endorsements from Ontario or federal courts;	Various	444-529	

		and(iii) any processes issued, including Intake Court Endorsements, warrants, orders (including but not limited to arrest warrants, search warrants, general warrants, and production orders).			
	Tab A	Email of the Applicant to Regional COM of the RCMP Mr. Matt Peggs of Mon, May 11, 2026 at 1:13 PM	May 11, 2026		445-467
	Tab B	The MAG CSD Court Information Access Guide (2019) regarding access to court documents, information, information assets, papers, things, et al for the OCJ, SCJ and ONCA (Ontario) (see: pages 277 to 314) along with 1. Lincoln County Law Association (Niagara) Pro Forma Information Package; 2. Driver's Licence: M16514331830325 of the Applicant; 3. The False Information Package (see: page pages 323 to 326); and 4. Canadian passport of the Applicant stolen by the insurance adjuster at three of the four insurance companies for the TDI Group (with ties to OPP and RCMP by his LinkedIn profile) (October 25, 2024)	2019 (Created)		468-518
	Tab C	The unredacted images from the CAMH redacted photos by the Applicant in early May 2025 involving the October 25, 2024, theft of the Applicant's property at CAMH 1025 Queen Street, Toronto, Ontario (known as the "McCain Recovery And Care Complex") in the visitor area which were provided to the Applicant by a paid <i>FIPPA</i> request of CAMH in late October 2024	May 11, 2026		519-529
		VOLUME #8: ATIA REQUESTS OF THE APPLICANT (SEE: APRIL 14, 2026; AND MAY 7, 2026 (DEFINED AS "ATIA REQUEST #1" AND "ATIA REQUEST #2"))			

		VOLUME #8(A): ATIA REQUEST #1 (APRIL 14, 2026)			
15		ATIA REQUEST OF THE APPLICANT (APRIL 14, 2026) (DEFINED AS “ATIA REQUEST #1”) AND FOLLOW UP EMAILS (delivered April 14, 2026: 0105952620936334 (Canada Post tracking number ATIA Request #1 has sought and is seeking: ☐ Investigative Data Bank audit trails (PPU 005) identifying all ADD/MODIFY/CLEAR/CANCEL commands (within specific timeframe) ☐ Raw hexadecimal mainframe dumps of the relevant CPIC entries to bypass GUI-level distortions. ☐ Hardware and terminal metadata (ORI codes, MAC addresses, IP logs) identifying the physical origin of data-entry sessions. ☐ Inter-agency communications between RCMP CPIC governance and the Toronto Police Service regarding authentication failures, matching-protocol errors, or metadata discrepancies. ☐ PDF/vector anomaly logs relating to document-flattening, OCR failures, and the suspected GrapeCity DOC-6507 vector-collapse bug. ☐ Offline historical search results required to reconstruct the true chronology of CPIC transactions. ☐ CPIC governance manuals and MOUs governing the Matching Protocol and Judicial Firewall This Access to Information Act (ATIA Request #1) request seeks disclosure of federal-level institutional, technical, and governance records necessary to verify the cryptographic provenance, jurisdictional integrity, and systemic reliability of CPIC entries associated with the Applicant’s related <i>Privacy Act</i> file (P-2025-16999 / F339) ([sic] (RCMP as it was not delivered in 2025 but in 2026)). Unlike the <i>Privacy Act</i> request—which concerns personal information—this ATIA Request #1 targets the broader federal infrastructure: the audit trails, metadata architecture, and inter-agency communications that govern the national warrant database. Because CPIC is the central nervous system of Canadian law enforcement, the RCMP—as its federal custodian—bears the statutory and fiduciary obligation to ensure the integrity of all entries, including those originating from municipal agencies.	April 14, 2026	530-588	

	A	Applicant's <i>ATIA</i> Request of April 10, 2026 (delivered April 14, 2026) Formal specification of requisitions under the access to information act (<i>ATIA</i>): ○ Cpic systemic integrity; ○ Metadata extraction; and ○ Inter-agency communications	April 14, 2026		531-543
	B	Response of the RCMP ATIP Melissa Simpson on April 23, 2026 (Thursday) this time taking an extension under <i>ATIA</i> but without even the pretense of a reference	April 23, 2026		544-555
	D	Response of the Applicant to the RCMP ATIP on April 23, 2026; and Email of the Applicant to the RCMP ATIP under the <i>ATIA</i> Request #1 on April 24, 2026 (Friday)	April 23 and 24, 2026		556-573
	E	Formal Complaint under the <i>ATIA</i> against the RCMP to the Information Commissioner of Canada involving ATIA Request #1 Subject: Formal complaint pursuant to part ii of the access to information act: Allegations of constructive refusal, systemic dereliction, Bad faith obfuscation, and Procedural nullities by the RCMP			574-588
		VOLUME #8(B): ATIA REQUEST #2 (MAY 7, 2026 TO JUNE 22, 2026)			
16		Applicant's second <i>ATIA</i> Request of May 5, 2026 (delivered on May 7, 2026 with Canada Post tracking: 0105952086612346) ("<i>ATIA</i> Request #2")	May 7-11,2026	589-617	
	A	<i>ATIA</i> Request #2 seeking records as to how long, when, what, where and how the RCMP has utilized GrapeCity PDF manipulation software (see: FORMAL REQUEST UNDER THE ACCESS TO INFORMATION ACT (<i>ATIA</i>) – SOFTWARE	May 7, 2026		590-600

		PROCUREMENT, LICENSING, NTOP ONBOARDING, EMBEDDED IT ARCHITECTURE, AND AZURE CLOUD UTILIZATION RECORDS (GRAPECITY / MESCIUS SDKS))			
	B	Canada Post tracking for the <i>ATIA</i> Request #2	May 8, 2026		601-606
	C	RCMP ATIP Response (A-2026-01933 / F281): Misstated Receipt Date, No s. 9 Extension, Improper 60-Day Complaint Notice, and Failure to Meet s. 7 Deadline.” RCMP ATIP Response (<i>ATIA</i> Request #2 – File A-2026-01933 / F281) Item: Response of RCMP ATIP (“Bryan”) – <i>ATIA</i> Access Request #2 File: A-2026-01933 / F281 Date Issues: Request received: Applicant: May 7, 2026 RCMP asserted receipt: May 8, 2026 (misrepresentation) Summary of RCMP Correspondence: ▪ Generic notice stating the request was “proceeding.” ▪ Extended 60-day complaint rights to the Office of the Information Commissioner (OIC). ▪ No indication of a s. 9 <i>ATIA</i> time extension and no reliance on any clause of s. 9(1)(a)–(c). ▪ No transfer under s. 8 <i>ATIA</i> within the 15-day statutory window (thus RCMP retains “greater interest” in the records). Statutory Deadlines: ▪ <i>ATIA</i> s. 7 deadline: 30 days from receipt → June 6, 2026 (Saturday) → de jure June 8, 2026 (Monday). ▪ No valid extension → RCMP remained bound to provide a compliant s. 7 notice and access determination. Procedural Irregularities Identified: ▪ RCMP’s email did not constitute a lawful s. 9 extension. ▪ Complaint rights were misstated (should arise immediately upon a valid extension, not 60 days after).	May 11, 2026		607-608

		RCMP implicitly conceded: 1. No large-volume search (s. 9(1)(a)); 2. No consultations required (s. 9(1)(b)); 3. No third-party notice (s. 9(1)(c)). Inconsistency: RCMP invoked statutory extension grounds under the <i>Privacy Act</i> for Privacy Request #1, but not under <i>ATIA</i> for Request #2. As of end of business day on June 7, 2026, RCMP defaulted on its obligations under ATIA in relation to ATIA Request #2.			
	D	Applicant's Complaint to the Information Commissioner of Canada under ATIA Request #2: (nota bene: for further evidence (if necessary), the Information Commissioner of Canada confirmed that it did not have jurisdiction until the Respondent RCMP cited an extension of time and the deadline passed of June 6, 2026)	May 11, 2026		609-617
		VOLUME #9: WRITTEN REPRESENTATIONS FOR NOM #1 (SUPPLEMENTAL PREDICATED UPON THE ADDITIONAL DOCUMENTATION FROM ATIA REQUEST #1)			
17		Supp - Written Reps for NOM #1 Appendix A – McLean v RCMP et al - App - E - Signed - Filed - 06-16-24	June 16, 2026	618-673	
18		Federal Court Submission Confirmation – June 16 2026		674-677	
		VOLUME #10: REQUISITIONS FOR HEARING APPLICATION DOCUMENTS (JUNE 12 AND 19, 2026)			

19		Requisition for Hearing Application (with Federal Court of Canada Confirmation Submission and payment)	June 12, 2026	678-686	
20		Requisition for Hearing Application with cover letter, Federal Court of Canada confirmation submission and payment confirmation	June 19, 2026	687-703	
21		Electronic Correspondence associated with the same	June 16 to 22 2026	704-710	
		Volume #10(A): Additional Evidence pursuant to the Canada Evidence Act		711-804	
22		Letter to the Federal Court of Canada Registry as of June 22, 2026 (additional evidence)	June 22, 2026	711-718	
	A	Original ATIA Request #2 Initial Submission Parameters (May 5, 2026).			719-720
	B	Inbound Electronic Transmission from RCMP ATIP Branch (May 11, 2026).			721-723
	C	Applicant's Warning Notice of Statutory Non-Compliance (June 8, 2026).			724-726
	D	Applicant's Warning Notice of Statutory Non-Compliance (June 8, 2026).			727-734

	E	Director Curtis Mathews' Premature "Unable to Locate" Refusal (<i>June 18, 2026</i>)			735-747
	F	Applicant's Comprehensive Statutory Rejection Transmission (<i>June 22, 2026, 8:29 AM</i>).			748-756
	G	Inbound Correspondence from Registry Officers Confirming Processing Status (<i>June 22, 2026</i>).			757-799
		<i>WITH TWO INCLUSIONS POST FILING OF THE SAME IN AN EMAIL FROM MR. CURTIS MATHEW OF THE RCMP ATIP BRANCH IN RELATION TO ATIA REQUEST #2 AND EMAIL TO MS. BEAUDOIN INVOLVING ATIP REQUEST #2</i>			
	H	A/Director General Curtis Mathews' Stay and Intervention Email (<i>June 22, 2026 at 11:51 a.m.</i>)			800-801
	I	Letter to RCMP ATIP Branch regarding ATIA Request #1 (Ms./Madame or Mademoiselle) Beaudoin et al)			802-804
		VOLUME #11: MEMORANDUM OF FACT AND LAW FOR APPLICATION, DRAFT ORDER, BILL OF COSTS, AND SUBMISSIONS ON COSTS			
23		Memorandum of Fact and Law (originally filed June 3, 2026)	June 3, 2026	805-837	
24		Draft Reasons for Order for the Judicial Review Application	June 22, 2026	838-877	
25		Applicant's Draft Bill of Costs	June 22, 2026	878-879	

26		Applicant's Memorandum of Fact and Law for NOM #2	June 23, 2026	880-893	
27		Applicant's Brief of Authorities: hyperlinked	June 23, 2026	894-951	
28		Applicant's Reasons for Order on NOM #1, #2 and Application Draft Order	June 23, 2026	952-1048	

29		The “Direction” of Associate Judge Mr. Crinson	June 24, 2026	1049-1051	
30		Applicant’s letter to the Chief Administrator and the Chief Justice/ACJ of the Federal Court of Canada addressing concerns in the AJ Mr. Crinson “Direction” that require determinations by the Primus Inter Pares of the Federal Court of Canada	June 25, 2026	1052-1061	
31		Emails involving Respondent Mr. Jeffrey Ball on May 19, 2026, and his attached OIPC (MFIPPA) decision involving “ten codes” and ORI codes	May 19, 2026	1062-1079	
32		Access Granted: Restoring Trust in the RCMP Access to Information and Privacy Program, 2020 (OIC Report to RCMP (Brenda Lucki, the RCMP Commissioner as she then was until 2023)	June 25, 2026	1080-1103	

33		Access at issue: The need for leadership Systemic investigation of the RCMP Special Report to Parliament from the Information Commissioner of Canada November 17, 2020	2020	1104-1145	
34		2024-2025 Annual Report to Parliament on the Administration of the <i>Access to Information Act</i>	2024-25	1146-1176	
35		Emails between Mr. Kevin A. McLean (BA, JD, CIM) and Ms. Tina Beaudoin (author being that of Ms. Margarethe Von-Zur Muhlena (see: Word document attachment); and metadata	June 25, 2026	1177-1182	
36		The 1 st Updated Draft Order and Reasons for Order/Judgment as of June 25, 2026 with filing confirmation and the cover letter that was filed together therewith	June 25, 2026	1183-1287	
37		Requisition for Hearing – Application (Form 314) (Ottawa) with filing confirmation	June 25 2026	1288-1295	
38		Emails involving Mr. Curtis Mathew of the RCMP ATIP Branch	June 26, 2026	1296-1307	

39		Evidence why Maggie Von Fur-Muehlen was not an individual with the Office of Primary Interest within the RCMP; evidence of why her and husband (Arun Jupa) likely sold Brassica restaurant in Ottawa (2025) and further evidence of the metadata of the purported clarification document from Ms. Von Fur-Muehlen (not Office of Primary Interest) (all objective evidence – no castigation of her obtaining employment post restaurant industry exist)		1308-1348	
	A	Tab A: public evidence of Ms. Von Fur Muehlen's success in restaurant industry up until 2023 - 24 along with her husband			1309-
		These restaurants are finding the recipe for success in a pandemic			1310
		Arup Jana and Maggie Von Zur-Muehlen in front of their newly opened Westboro eatery, Brassica. Prepaid pickup orders are placed on an overturned milk crate, while chalk Xs on the sidewalk mark off two-metre spaces where customers can wait. (Francis Ferland/CBC			1313
		Arup Jana and Maggie Von Zur-Muehlen, co-owners of Brassica in Westboro, say they've reduced their volume, cut staff and created a system for picking up takeout orders that limits contact between			1314
		Some restaurants pivoting to takeout for NewYear's Eve Restaurateurs say cancellations, staff safety and rising case counts factor into decisions Matthew Kupfer · CBC News · Posted: Dec 30, 2021 4:00 AM			1317-1319
		Ottawa Living Online Publication, "What's new?" Published on March 8, 2020			1320-1327
		Wellington Gastropub celebrates its second birthday By The Ottawa Citizen Published Sep 15, 2008			1328-1337
		Mind and Money Podcast: Ep. 021 Brassica, The Great Food Experience & Adventure in the Kitchen (https://mindandmoney.libsyn.com/ep-021) Corey Butler and Shawn Todd have an opportunity to speak with Arup Jana and Maggie Von Zur-Muehlen - owners of Brassica in Westboro. Arup and Maggie get into talking about what they learned from opening a restaurant in 5 days, what people stole after the Allium fire, how COVID has brought adventure into the kitchen, and where Brassica is heading. Connect with Corey, Shawn, and Ecivda Financial on Instagram, FB,			1338-1342

		LinkedIn, YouTube & Twitter			
	B	Tab B: Arup Jana (husband) - owned and operated Brassica until 2025		1343-1347	
	C	Tab C: Metadata of the clarification (purported) document sent from Ms. Beaudoin to the Applicant (misrepresented as being from Office of Primary Interest) ▪ Nota bene: no castigation of Maggie Von Fur Muehlen per se but indicative of a buy out of her shareholdings and her husband's on or around 2024 or 2025 and subject to a non-compete in the industry and within proximity ▪ In essence, Maggie Von Fur Muehlen, with praise, had to find new and different employment so she found government employment with the RCMP in an administrative capacity ▪ Being an individual in one of the Offices of Primary Interest is a position that requires an incredible amount of skill, acumen, experience and particularly in the niche areas that are at issue herein ▪ One can objectively tell from her writing style (i.e. CPI Centre (not standard acronym) that she is new to the position, without castigation, but certainly not of an OPI. As such, fraud unravels everything. This was a fraudulent misrepresentation by one Ms. Beaudoin to the Applicant ▪ It is also rather shocking from a protection of privacy and Personal Information standpoint that a document would be tendered in Word in such fashion and created on the very day with a few revisions by Maggie Von Fur Muehlen and then last edited by Ms. Beaudoin on the day in question ▪ Simply put, it could never been in retrieval phase if Maggie Von Fur Muehlen was drafting a "clarification note" in the week of June 22 to 26, 2026. ▪ Maggie Von Fur Muehlen must be commended for making the best of her situation from a fire with a restaurant in Allium, creating a new restaurant in Brassica, braving out the pandemic unlike the Freedom Convoy destructive nonsense, but that does not make Ms. Beaudoin's fraudulent misrepresentations better but worse		1347-1348	
		Metadata2Go provides a deeper and more robust look into the metadata compared to the above (see: supra) from a properties search in Microsoft Word (nota bene: the question arises as to "who is pulling the strings" and causing intentional non-compliance with an ATIA Request #1 (April 14, 2026 delivered)	June 27, 2026		

		▪ (nota bene #2: lag times of a day being delivery via Canada Post versus when the RCMP ATIP Branch claims it was received) ▪ (nota bene #3: Ms. Beaudoin's LinkedIn represents that she is a national team leader in the area of RCMP ATIP Branch as follows: ▪ "Team Leader ATIP ▪ Fed gov ▪ Mar 2018 - Present · 8 yrs 4 mos ▪ National Capital Region -Ottawa ▪ https://www.linkedin.com/in/tina-beaudoin-1481a7129/)			
		File Name: Clarification requested June25, 2026 A-2026-00761.docx: inconsistent with the previous representations of Ms. Beaudoin that the ATIA #1 was in retrieval			
		creator: Von Zur-Muehlen, Margarethe(Maggie)(RCMP/GRC)			
		last_modified_byBeaudoin, Tina(RCMP/GRC)			
40				1349-1376	
	A	Documents involving Derek Santosuosso: RCMP Assistant Commissioner (Ret'd) 32+ Years in Policing Leadership Technical Operations National Recruiting Commanding Officer Major Crime & Organized Crime 32 years of policing leadership — from homicide investigations in BC to commanding national technical programs from Ottawa	June 26, 2026		1351
		From Mr. Derek Santosuosso's LinkedIn: I retired in May 2026 as Assistant Commissioner, Technical Operations (RCMP National HQ), where I oversaw seven national program branches delivering advanced investigative and operational capabilities to law enforcement across Canada: covert electronic surveillance, digital forensics, lawful access, protective security, counter-drone operations, airborne law enforcement, missing persons, and the responsible onboarding of emerging technologies	June 26, 2026		

		**KEY POST – TYING Mr. Derek Santosuosso to Mr. Ball under PII Access Request (March 11 2026) in the Privacy Act (Federal) (see: Tab 11, pages 386-397)			1357-
		KEY POST - TIED TO SPECIALIZED POLICING SERVICES (SEE: MR. JEFF BALL IN THE PURPORTED DISCLOSURE DECISION (THE "NON SEARCH DECISION" REFERENCING SPECIALIZED POLICING SERVICES): As the new year has come so has change for me to take on a new role. I'm happy to share that I'm starting anew position as Assistant Commissioner of Technical Operations, Specialized Policing Services at Royal Canadian Mounted Police Gendarmerie royale du Canada (May 2025) (nota bene: odd timing to retire one year after taking on a new role – lack of continuity concerns or otherwise)	June 26, 2026		1357
	B	RCMP formally reaffirms its partnership with Missing Children Society of Canada May 22, 2026	May 22, 2026		1359-
		Our partnership with MCSC is rooted in a shared commitment to collaboration, compassion and results. This agreement reflects our shared dedication to ensuring investigators have the support they need and that families facing the unimaginable know they are not alone. Together we are working towards our common goal of bringing missing persons home. Chief Superintendent Richard Burchill, Acting Assistant Commissioner, Technical Operations, RCMP	May 22, 2026		1361
	C	Post on Twitter (X): The Guy@ProGamerGovRCMP Witness Richard Burchill just tried to claim that mandatory metadata retention isn't mass surveillance, at today's #SECU Committee.#encryption #encryptedmessaging #privacy #backdoors #c22 #lawfulaccess#cdnpoli #canpoli #canadianpolitics9:16 PM · Jun 16, 2026 · 11 Views	June 16, 2026		
	D	Your metadata may be kept for a year under lawful access bill. What to know By • Global News Posted May 21, 2026 6:00 am	May 21, 2026		1359-1376
		The federal government's proposed lawful access bill is raising concerns about the potential lengthy retention of Canadians' metadata that could then be accessed by law enforcement, which privacy experts warn is risky and "unprecedented."			

		Question arises: what about false Foundational Metadata and false Personal Information in Offline Historical Database involving the Applicant and others similarly situated?			
		Bill C-22 includes a new provision that would allow the government to make regulations for “core” telecommunications providers to retain certain types metadata — including transmission and location data — “for reasonable periods of time not exceeding one year.”			1366
		<i>Question arises relating to infra: what if the judicial warrant is falsified like the facts arising herein? What if relied upon in CPIC by other law enforcement agencies, police services et al when it is false? And without access to the underlying documents and records?</i>			
		While government officials insist the data that would be collected does not include actual online content like search histories or emails, and that the metadata itself can only be collected by investigators through a judicial warrant, experts warn the retention policy alone is concerning			1367
		MASSIVE HAYSTACK OF DATA – USING THE NEEDLE WHEN "law enforcement applicant" FEELS FIT The government’s building this massive haystack of data with the thought that they might need to find the needle every once in a while,” said Michael Geist, a professor at the University of Ottawa and the Canada research chairing internet and e-commerce law. “But in doing so, they’re creating huge privacy risks for Canadians.” ▪ (nota bene: creates more urgency for purposes of the NOM #1, NOM #2 and Application being heard and decided with a decision given to not only the Applicant and Respondents but also the public at large)			1367
		What is metadata? ▪ Metadata is broadly defined as “data about data,” or what Geist calls “the information around” something like an online communication rather than the content itself. ▪ This includes dates, times and locations those messages were sent, the IP addresses used to send them, and broad identifiers like the names of senders and receivers and what type of file or message it was. ▪ It also involves tracking data and transmission data that is collected every time a cellphone connects to a cell tower, Geist explained, “which is all the time” because most people’s phones remain turned on even when not in use.			1368

		▪ “Anytime you communicate with someone, what device did you use? Where were you located? When did you communicate? All of those things about your activities. That’s what metadata is,” he said.			
		Robert Diab, a law professor at Thompson Rivers University in Kamloops, B.C., who focuses on online privacy, said courts have recognized for decades that “the mosaic of information that you can assemble through metadata can really reveal quite a lot about a person’s life.”			1369
		RICHARD BURCHILL QUOTE (NEW DIRECTOR OF TECHNICAL OPERATIONS FOR RCMP SINCE MAY 2026 (FOUR DAYS AFTER THE NON-ASSIGNMENT DECISION OF RCMP ATIP BRANCH (I.E. WITHOUT ANY ASSIGNMENT TO THE OFFICE OF PRIMARY INTEREST FROM RCMP ATIP BRANCH THEN NO SEARCH WOULD BE CONDUCTED)) Richard Burchill, director-general of technical investigative services for the RCMP, told the House of Commons public safety committee this month that internet transmission data and <u>cell tower signalling data would be of particular interest</u> ▪ Nota bene: THE OPENING OF PANDORA’S BOX THEME			1370
		Why are experts concerned? Diab noted that under existing Canadian law, police must seek a warrant asking a telecommunications provider to retain a specific person’s metadata for only a limited amount of time, such as a month or 90 days, for an investigative purpose ▪ (NOTA BENE: Regional COM Mr. Matt Peggs non-responsive to requests in accordance with the MAG CSD Court Information Access Guide (2019) and demands for property			1371
		“The reason Parliament has done that ... is that it recognizes that the creation of a record is itself an interference” of privacy, he said. ▪ (nota bene: this speaks to the issue of falsification (much worse) of Information Packages, CC Form 2 Informations and CC Form 4 Indictments and CC Form 7 "Warrant For Arrest"			
		“The reason Parliament has done that ... is that it recognizes that the creation of a record is itself an interference” of privacy, he said. “In this case, the minister tells Telus, ‘go and save it for a year.’ ... The idea is the same: if you create a record, if you order a third party to preserve a			1373

		citizen's records of their communications, you are interfering with their privacy because you're conducting a form of surveillance. You are creating a situation in which their movements, their communications are being watched or are being made watchable in a sense. And that's what matters			
		MISSTATEMENT OF LAW (SEE: FORCED PRODUCTION IS A SEIZURE OR SEARCH (SEE: MCLEAN V. LSBC CASES; AND MULGREW V. POST MEDIA AND OTHERS): Hiegel told the House of Commons committee that the government does not equate a company's retention of data with a "seizure" as defined by the Charter because there is no production order involved until a judicial warrant is approved			1374
41		Documents involving Lawful Access Act (Bil C-22, 2026); Standing Committee on Public Safety and National Security NUMBER 036 Tuesday, May 5, 2026; CBA publication on Bill C-22 (Lawful Access Act, 2026); Bill C-22; 1st Session, 45th Parliament, 3-4 Charles III, 2025-2026		1377-1494	
	A	Tab A: 45th PARLIAMENT, 1st SESSION Standing Committee on Public Safety and National Security EVIDENCE NUMBER 036 Tuesday, May 5, 2026		1378	
		My name is Mike McGuire. I'm the director general of international and border policy at Public Safety Canada. I'm pleased to be here with colleagues, as was just mentioned, from the Department of Justice, the Department of Public Safety, the RCMP and CSIS to answer technical questions on Bill C-22, an act respecting lawful access.			
		Richard Burchill (Director General, Technical Investigation Services, Royal Canadian Mounted Police): The confirmation of service demand is very front-end, at the beginning of an investigation, to enable us to gather basic information to pursue an investigation. We have very little information—for instance, a phone number or an IP address. Just that yes-or-no confirmation from a telecommunications service provider gives us the ability to verify that this person is with this company. Then, we can start doing investigative work around that to get enough grounds to bring forward a production order to get subscriber information as a next step. We still have to build those investigative grounds in order to bring forward a production order to get subscriber			
		LOWEST THRESHOLD OF "REASONABLE BELIEF" OVER REASONABLE GROUNDS TO BELIEVE ("RGB") (see: distinction elucidated and articulated in R. v. Kang-Brown, SCC)			

		Richard Burchill: As you said, we need a judicial authorization in order to access that data. The timeliness of it is.... There are companies that already retain this metadata (what about falsified warrants for arrest that allow for greater search and seizure powers)			1387
	B	Bill C-22 (Lawful Access Act, 2026)CANADIAN BAR ASSOCIATION CRIMINAL JUSTICE, PRIVACY AND ACCESS TO INFORMATION LAW SECTIONS ANDANTE-CORRUPTION TEAM May 2026			1404
	C	First Session, Forty-fifth Parliament,3-4 Charles III, 2025-2026Première session, quarante-cinquième législature,3-4 Charles III, 2025-2026HOUSE OF COMMONS OF CANADA CHAMBRE DES COMMUNES DU CANADA BILL C-22 PROJET DE LOI C-22An Act respecting lawful access Loi concernant l'accès légalFIRST READING, MARCH 12, 2026 PREMIÈRE LECTURE LE 12 MARS 2026			1423
42				1495-1579	
		<i>Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness)</i> , 2019 FC 1279 (CanLII)			1496-1543
		<i>Fabunmi v. Canada (Citizenship and Immigration)</i> , 2020 FC 1009 (CanLII)			1545-1556
		<i>Canadian Broadcasting Corporation v. Canada (Parole Board)</i>			1557-1579

All of which is respectfully submitted and filed by the Applicant (absent service on the non-appearing, non-opposing and non-contesting Respondents) certified as true, accurate and complete as if it were sworn, affirmed or declared evidence contained therein and so adopted herein formally, on June 28, 2026:

A handwritten signature in black ink, appearing to read 'Kevin A. McLean', with a stylized flourish at the end.

Mr. Kevin A. McLean (BA, JD, CIM)
68 Abell St. (Receptionist desk) Toronto, ON M6J 0B1
Self-represented
Appearing Pro Se
mclean@searchandseizure.ca

ENDNOTES

ⁱIn effect, the legal position changed from an “(i) meeting the original time limit would unreasonably interfere with the operations of the government institution” to “operational requirements”

ⁱⁱIn the interim, and in the spirit of cooperation, you can readily provide the following personal information elements associated with my WANT record, each of which is discrete, easily retrievable, and directly tied to my identity” (nota bene: seeking of the: (i) ORI; (ii) court level; (iii) court location; (iv) name of judicial officer: and (v) system identification number

Tab 0

FORM 359 Rule 359

Notice of Motion

Court File No. T-2448-26

FEDERAL COURT

BETWEEN:

KEVIN ALEXANDER McLEAN

Applicant

– and –

ROYAL CANADIAN MOUNTED POLICE, COMMISSIONER MICHAEL DUHEME,
ATTORNEY GENERAL OF CANADA, and HIS MAJESTY THE KING IN RIGHT OF
CANADA

Respondents

NOTICE OF MOTION*(Motion in Writing under Rule 369; Form 359)*

TAKE NOTICE that the Applicant, **Kevin Alexander McLean (BA, JD, CIM)**, will make a **motion in writing** under **Rule 369** of the *Federal Courts Rules* to a Judge of the Federal Court, and respectfully requests that this motion be **self-assigned and determined by the Acting Chief Justice of the Federal Court, the Honourable Martine St-Louis**, in her capacity as Chief Justice and Associate Chief Justice of the Federal Court.

The motion is to be determined **in writing**, without the attendance of the parties, on Tuesday, June 30, 2026, and on the basis of the written materials submitted to the Federal Court of Canada by the Applicant, whether electronic, mail,

delivered or faxed (if consent was so provided) and contained within the court file between the Applicant and the Federal Court of Canada Toronto Court Office Registry (if not contained in the NOM #2 Motion Record).

A. RELIEF SOUGHT

The Applicant seeks the following Orders:

1. Self-Assignment by the Acting Chief Justice

1. **An Order declaring that this proceeding constitutes a “Chief Justice’s Case”** within the meaning of *R. v. Baldovi*, 2016 MBQB 167, and *Ruffo v. Conseil de la magistrature*, [1995] 4 SCR 267, and that the nature of the challenges, controversies, and integrity issues engaged requires the **direct stewardship and self-assignment** of the Acting Chief Justice of the Federal Court.
 2. **An Order that this Notice of Motion (NOM #2) and the underlying Form 301 Application** be placed before the Acting Chief Justice **forthwith** for consideration of self-assignment and directions.
-

2. Abridgement of Time and Validation of Irregularities

3. **An Order abridging any applicable time limits** under the *Federal Courts Rules*, including Rules 8 and 369, as necessary to permit this motion to be determined on or before **June 30, 2026**, or as soon thereafter as the Acting Chief Justice directs.
 4. **An Order validating nunc pro tunc** any irregularity in the form, timing, or filing of this Notice of Motion, including the use of Form 359 for a Rule 369 motion, as of the date of electronic submission and/or hand delivery to the Toronto Local Office.
-

3. Transmission to the Principal Office (Ottawa)

5. **A direction under Rules 23–25** that the Toronto Local Office **forthwith transmit** this Notice of Motion and all related paper-filed materials to the **Principal Office in Ottawa**, and that the Principal Office ensure that the materials are placed before the Acting Chief Justice without delay.
-

4. Regularization of the Application Record and Requisition

6. **An Order confirming** that the Applicant’s **Application Record** (electronically submitted June 22, 2026 and courier-filed June 23, 2026 at 8:51 a.m. EST) is **properly before the Court**, and that any mischaracterization of the proceeding as an “Application for Leave” is **set aside**.
 7. **An Order that the Applicant’s Form 314 Requisition for Hearing**, for which fees have been paid **twice**, be **processed, stamped as filed, and treated as effective** as of the earlier of the dates of electronic submission or hand delivery.
-

5. Relief Respecting Service and Default

8. **An Order confirming** that pursuant to **Rule 308**, the Respondents are **not entitled to notice of further steps** due to their failure to file a Notice of Appearance under Rule 305 and their failure to transmit the Certified Tribunal Record (“CTR”) under Rule 318.
 9. **An Order that the Applicant is not required to serve** further materials unless the Court directs otherwise.
-

6. Certified Tribunal Record and Registry Correspondence

10. **An Order declaring** that the RCMP’s failure to transmit the CTR within 20 days under Rule 318, and its failure to file any objection under Rule 318(2), constitutes a **procedural default** and a **reviewable error**, and that the Application may proceed on the existing evidentiary record.
 11. **An Order requiring the Registrar of the Toronto Local Office** to produce and file **all correspondence** between the Applicant and the Toronto Registry not already contained in the Application Record, including internal routing or processing communications.
-

7. Direction of Court Staff in Matters Assigned by Law to the Judiciary

12. **An Order declaring** that in matters assigned by law to the judiciary — including judicial review under ss. 18, 18.1, and 18.3 of the *Federal Courts Act* — **registrars, court clerks, and court staff must act at the direction**
-

of the **Chief Justice**, consistent with the constitutional principle recognized in **Sydel v. Canada (AG), 2013 FC 1116** and the inherent administrative independence of the Court.

8. General Powers, Equity, and Special Circumstances

13. **An Order under Rules 3, 5, 24, and 55** varying or dispensing with any Rules necessary to ensure the most expeditious and just determination of this motion.

14. **Such further and other relief** as this Honourable Court may deem just.

B. GROUNDS INTENDED TO BE ARGUED

The Applicant relies on the following grounds, without limiting the generality of the relief sought:

1. Procedural Posture and Respondents' Default

15. The Respondents were served on **May 19, 2026**. They have **not filed a Notice of Appearance** within the 10-day period mandated by **Rule 305(1)**, nor at any time thereafter.

16. The Respondents have **not transmitted the Certified Tribunal Record ("CTR")** within the 20-day period mandated by **Rule 318(1)**, nor filed any objection under **Rule 318(2)**.

17. Under **Rule 308**, the Respondents are **not entitled to notice of further steps**, and the Application proceeds **unopposed**.

18. The Applicant's **Form 301 Application, Rule 317 Request (filed and accepted May 19, 2026), Proof of Service (filed and accepted May 19, 2026), Application Record of June 3, 2026, Motion Record of June 11, 2026, Written Representations of June 16, 2026, and Application Record of June 22/23, 2026** collectively constitute a **properly constituted judicial review** under ss. 18, 18.1, and 18.3 of the *Federal Courts Act*.

19. There is **no leave requirement**. The Application was filed within 30 days of the RCMP's decision.

2. This Proceeding Is a "Chief Justice's Case"

20. Certain proceedings, by virtue of their **challenges, controversies, or institutional implications**, require the direct stewardship of the Chief Justice. These are known as “**Chief Justice’s Cases**”, as articulated in:

- *R. v. Baldovi*, 2016 MBQB 167
- *Ruffo v. Conseil de la magistrature*, [1995] 4 SCR 267
- *Provincial Judges Reference*, [1997] 3 SCR 3

21. This proceeding is a **paradigmatic Chief Justice’s Case**. It involves:

- systemic irregularities within the RCMP;
- contradictory statutory positions under the *Privacy Act* and *ATIA*;
- a refusal to search a non-exempt Personal Information Bank (unprecedented in Canadian jurisprudence);
- registry mischaracterization of the proceeding;
- failure to process filings;
- and the need for urgent judicial oversight before summer recess.

22. Only the Acting Chief Justice can ensure the **actual and perceived integrity** of the Court is preserved.

3. Evolution of Primus Inter Pares and the Chief Justice’s Inherent Powers

23. The doctrine of **primus inter pares** has evolved significantly in Canadian law. Early references (1875, 1946, 1980, 1986) were non-judicial. It was not until **Ruffo (1995)** that the Supreme Court applied the doctrine to the judiciary.

24. Since *Ruffo*, the Chief Justice’s role has been recognized as **substantive**, not ceremonial. The Chief Justice bears inherent responsibilities, including:

- **Master of the Roster**
- **Self-Assignment Power**
- **Administrative Stewardship**
- **Institutional Reputation Guardianship**
- **Ethical Oversight**

- **Complaint-Laying Authority**
- **Power to Relieve or Reassign Judges Not Yet Seized**
- **Moral Authority Over the Judicial Collective**

25. These principles were reaffirmed in:

- *Canadian Judicial Council v. Girouard*, 2019 FCA 148, paras. 42–44
- *Dugré c. Canada (AG)*, 2019 FC 1604, para. 21

26. The Chief Justice’s supervisory powers over judicial conduct and court administration are **inherent** and **do not require legislative authorization**.

27. Given the systemic issues engaged here, the Acting Chief Justice must exercise her **self-assignment power**.

4. Direction of Court Staff in Matters Assigned by Law to the Judiciary

28. Although the *Federal Courts Act* does not contain a provision identical to **s. 76 of the Courts of Justice Act (Ontario)**, the underlying constitutional principle is the same: **where matters are assigned by law to the judiciary, registrars and court staff must act at the direction of the Chief Justice**.

29. In *Sydel v. Canada (AG)*, 2013 FC 1116, the Federal Court confirmed that the **judicial branch directs the executive** in matters of court administration that bear directly on adjudicative functions.

30. This proceeding — a judicial review under ss. 18, 18.1, and 18.3 of the *Federal Courts Act* — is **assigned by law to the judiciary**. The Acting Chief Justice therefore has the constitutional authority to direct:

- the processing of the Requisition for Hearing;
- the correction of registry mischaracterizations;
- the transmission of documents to the Principal Office;
- and the docketing of the Application Record.

5. Pre-emptive Necessity: Assignment Before a Judge Becomes Seized

31. In **High-Crest Enterprises Ltd. v. Canada**, 2017 FCA 88, the Federal Court of Appeal confirmed that **a judge who is not yet seized may be stripped of a matter**, but once seized, reassignment becomes significantly constrained.

32. This motion is therefore **pre-emptive**. It seeks assignment **before** any puisne judge becomes seized, ensuring:

- the Acting Chief Justice may self-assign;
- no inadvertent assignment occurs;
- no conflict or prior involvement arises;
- and the integrity of the proceeding is preserved.

6. Judicial Review Is Decided on the Record — **Keeprite, Sticky Nuggz, Vavilov, Yatar**

33. Judicial review is a **record-based proceeding**, as held in:

- *Vavilov*, 2019 SCC 65
- *Yatar v. TD Insurance*, 2024 ONCA 446

34. The **Keeprite standard** (*Keeprite Workers' Independent Union v. Keeprite Products Ltd.*, 1980 CanLII 1877 (ON CA)) limits affidavit evidence to:

- showing an absence of evidence on an essential point; or
- proving a breach of natural justice not apparent on the record.

35. The Federal Court's structure under **Rules 317–318** mirrors this: the **CTR is the evidentiary foundation**.

36. The RCMP's refusal to transmit the CTR creates an **evidentiary vacuum of its own making**. The Applicant cannot be faulted for declining to file affidavits, particularly where:

- the RCMP's own correspondence contains **binding admissions**;
- Parliament created a **presumption of integrity** for electronic documents under **s. 31.1 of the Canada Evidence Act**;
- and affidavits would invite delay through cross-examination.

7. No Complaint Mechanism Exists for a Refusal to Search — Judicial Review Is the Only Remedy

37. Section 29 of the *Privacy Act* exhaustively enumerates complaint grounds. **Refusal to search** is not among them.
38. The RCMP's refusal to search a **non-exempt Personal Information Bank** is unprecedented in Canadian jurisprudence.
39. The Applicant cannot file a complaint. The Privacy Commissioner cannot investigate. The Commissioner cannot compel a search.
40. Judicial review and mandamus are therefore the **only available remedies**.
41. With respect to Mr. Ball, **it is what he did not say** that is most revealing: he never identified a statutory basis for refusing to search, nor any mechanism for challenging such refusal.
-

8. Local Office → Principal Office Transmission (Rule 25)

42. Under **Rule 25(1)**, any document filed at a Local Office must be transmitted to the **Principal Office**.
43. The Applicant's **8:51 a.m. courier filing** on June 23, 2026 triggered this mandatory transmission.
44. This ensures the matter is placed before the Acting Chief Justice **immediately**, bypassing local administrative delay.
-

9. Equity, the General Principle, and Special Circumstances

45. The **General Principle** requires proceedings to be conducted on the **most expeditious basis**.
46. The Applicant seeks no tactical advantage — only:
- a hearing date,
 - a judge,
 - a record,
 - and a decision.
47. The combination of:
- RCMP default;

- registry irregularities;
- mischaracterization of the proceeding;
- absence of a complaint mechanism;
- public importance of RCMP data integrity;
- and the impending summer recess

constitutes **special circumstances** under **Rule 55**, warranting variation or dispensation of any Rules necessary to ensure justice.

C. STATUTORY PROVISIONS AND RULES RELIED ON

The Applicant relies on the following statutory provisions, rules, and constitutional principles:

Federal Courts Act, RSC 1985, c F-7

- ss. 2, 18, 18.1, 18.3 (judicial review jurisdiction)
- ss. 50, 52 (powers of the Court)

Federal Courts Rules, SOR/98-106

- **Rule 3** — General Principle (most expeditious determination)
- **Rule 5** — Dispensing with compliance
- **Rule 8** — Abridgement of time
- **Rules 23–25** — Filing, transmission, and registry duties
- **Rules 300–305** — Applications generally
- **Rule 308** — Consequences of failure to file Notice of Appearance
- **Rule 314** — Requisition for Hearing
- **Rules 317–318** — Certified Tribunal Record
- **Rule 359** — Notice of Motion
- **Rule 369** — Motion in writing

- **Rule 55** — Special circumstances
- **Rule 75** — Amendments and nunc pro tunc relief

Privacy Act, RSC 1985, c P-21

- ss. 4, 6, 12, 14 (search, access, correction)
- s. 29 (complaint jurisdiction — exhaustive grounds)

Access to Information Act, RSC 1985, c A-1

- s. 4(2.1) — Duty to assist
- ss. 9–10 — Extensions and deemed refusals

Canada Evidence Act, RSC 1985, c C-5

- ss. 30, 31.1 — Electronic documents and presumption of integrity

Constitutional Principles

- **Judicial independence** (Beauregard; Valente; MacKeigan)
- **Administrative independence** (Valente; Provincial Judges Reference)
- **Primus inter pares** (Ruffo; Girouard; Dugré)
- **Chief Justice's inherent supervisory powers**
- **Rule of law and access to justice**

Authorities Relied On

- *R. v. Baldovi*, 2016 MBQB 167
- *Ruffo v. Conseil de la magistrature*, [1995] 4 SCR 267
- *Canadian Judicial Council v. Girouard*, 2019 FCA 148
- *Dugré c. Canada (AG)*, 2019 FC 1604
- *High-Crest Enterprises Ltd. v. Canada*, 2017 FCA 88
- *Keeprite Workers' Independent Union v. Keeprite Products Ltd.*, 1980 CanLII 1877 (ON CA)
- *Vavilov*, 2019 SCC 65
- *Yatar v. TD Insurance*, 2024 ONCA 446

- *Sydel v. Canada (AG)*, 2013 FC 1116

D. DOCUMENTS AND MATERIAL TO BE USED ON THE MOTION

The Applicant intends to rely on the following documents:

1. **Form 301 Application** (filed and accepted May 15, 2026).
2. **Rule 317 Request** (filed and accepted May 19, 2026).
3. **Proof of Service** (filed and accepted May 19, 2026).
4. **Application Record of June 3, 2026** (Tabs 1–25).
5. **Motion Record of June 11, 2026 (NOM #1)**.
6. **Memorandum of Fact and Law on the Application** (June 3, 2026).
7. **Memorandum of Fact and Law on NOM #1** (June 11, 2026).
8. **Written Representations** (June 16, 2026).
9. **Updated Application Record** (electronically submitted June 22, 2026).
10. **Hard-copy Application Record** courier-filed June 23, 2026 at 8:51 a.m. EST.
11. **Draft Reasons for Order/Judgment** (Tab 24).
12. **Draft Order** (Tab 25).
13. **Cover Letter dated June 23, 2026** to the Toronto Local Office.
14. **Any correspondence** between the Applicant and the Toronto Registry not already in the record, including internal routing communications, as may be produced pursuant to this motion.
15. **Motion Record for NOM #2**, to be filed separately, including:
 - Memorandum of Fact and Law for NOM #2
 - Draft Order for NOM #2
 - Updated Bill of Costs
16. **Such further materials** as the Court may permit.

E. SIGNATURE

DATED at Toronto, Ontario, this 23rd day of June, 2026.



Kevin Alexander McLean (BA, JD, CIM)

Applicant, Self-Represented

Proo Se

68 Abell Street (Reception Desk)

Toronto, Ontario M6J 0B1

Email: **mclean@searchandseizure.ca**

x

Tab 1



(Court Seal)

FORM 301 - Rule 301
NOTICE OF APPLICATION

e-document-é		T-2448-26 ID 1	
F I L E D	FEDERAL COURT COUR FÉDÉRALE		D É P O S É
May 15, 2026 15 mai 2026			
Tristan Mercieca			
TOR		1	

Court File No. _____

FEDERAL COURT

BETWEEN:

KEVIN A. MCLEAN

and

Applicant

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, and
STEPHANE BRISSON

Respondents

APPLICATION UNDER sections 18, 18.1 and 18.2 of the *Federal Courts Act*, R.S.C. 1985, c. F-7, and the Rule 300-301
Federal Courts Rules, SOR/98-106, Part -1,

NOTICE OF APPLICATION

TO THE RESPONDENTS:

A PROCEEDING HAS BEEN COMMENCED by the applicant. The relief claimed by the applicant appears on the
following page.

3
THIS APPLICATION will be heard by the Court at a time and place to be fixed by the Judicial Administrator. Unless the Court orders otherwise, the place of hearing will be as requested by the applicant. The applicant requests that this application be heard at **Toronto, Ontario**.

IF YOU WISH TO OPPOSE THIS APPLICATION, to receive notice of any step in the application or to be served with any documents in the application, you or a solicitor acting for you must prepare a notice of appearance in Form 305 prescribed by the Federal Courts Rules and serve it on the applicant’s solicitor, or where the applicant is self-represented, on the applicant, WITHIN 10 DAYS after being served with this notice of application.

Copies of the Federal Courts Rules information concerning the local offices of the Court and other necessary information may be obtained on request to the Administrator of this Court at Ottawa (telephone 613-992-4238) or at any local office.

IF YOU FAIL TO OPPOSE THIS APPLICATION, JUDGMENT MAY BE GIVEN IN YOUR ABSENCE AND WITHOUT FURTHER NOTICE TO YOU.

Date: _____

Issued by: _____

(Registry Officer)

Issued on: May 19, 2026
Issued by: Tristan Mercieca (Registry Officer)
Address of Local Office: Toronto Local Office / Bureau local de Toronto 180 Queen St. W., Suite 200 /180, rue Queen O., Bureau 200 Toronto, Ontario M5V 3L6

Address of local office: _____

Federal Court Registry
180 Queen Street West,
Suite 200
Toronto, Ontario
M5V 3L6

TO (name and address of each respondent): _____

TO: _____

RCMP National Headquarters 73 Leikin Drive Ottawa, ON K1A 0R2 Canada
Email: Legal_Services@rcmp-grc.gc.ca

TO: _____

Commissioner of the RCMP Mr. Michael Duheme 73 Leikin Drive Ottawa, ON K1A 0R2 Canada

Email: Michael.Duheme@rcmp-grc.gc.ca

4
TO:

Director General of RCMP Access To Information and Privacy Branch (the “ATIP Branch”) Mr. Stephane Brisson 73
Leikin Drive Ottawa, ON K1A 0R2 Canada
Email: stephane.brisson@rcmp-grc.gc.ca

TO:

Director, Privacy, RCMP ATIP Branch Mr. Jeff Ball 73 Leikin Drive Ottawa, ON K1A 0R2 Canada
Email: Jeff.ball@rcmp-grc.gc.ca

NAME AND ADDRESS of every other person required to be served

TO:

Mr. Matt Peggs
Assistant Commissioner of the RCMP
Regional Commander of the Central Region of Ontario (formerly the “O” Region (O Division, Ontario, Commanding
Officer, ‘O’ Division)) for the RCMP
RCMP Central Region Headquarters
Royal Canadian Mounted Police

130 Dufferin Avenue
London, Ontario N6A 4K3
Canada
Telephone : 519-640-7254
Alternate Telephone : 1-800-387-0020
Fax : 519-640-7425
TDD : 519-640-7495

(Originating Agency Identifier in Canadian Police Information Centre (“CPIC”): **ON80300**)

AND TO:

The RCMP Milton Detachment known as the Toronto West Detachment (the “TWD”)
TORONTO WEST - MILTON DETACHMENT
2755 High Point Drive
Milton, Ontario L9T 5E8
Canada
Telephone : 905-876-9500
Fax : 905-876-9595
Attention: Regional COM Mr. Matt Peggs
Attention: Officer-in-Charge
(Originating Agency Identifier in Canadian Police Information Centre (“CPIC”): **ON80313**)

APPLICATION

(Where the application is an application for judicial review)

5

This is an application for judicial review in respect of:

(Identify the tribunal)

The Royal Canadian Mounted Police (“RCMP”)

The Applicant notes that the RCMP is a “Tribunal” under the Federal Courts Rules (*FCR*) under Rule 317 and by cross-reference to section 2(1) of the *Federal Courts Act* (the “*FCA*”) under the “Other Tribunal” component of the definition of: “**federal board, commission or other tribunal**” means any body, person or persons having, exercising or purporting to exercise jurisdiction or powers conferred by or under an Act of Parliament or by or under an order made under a prerogative of the Crown, other than the Tax Court of Canada or any of its judges or associate judges, any such body constituted or established by or under a law of a province or any such person or persons appointed under or in accordance with a law of a province or under section 96 of the Constitution Act, 1867.

Section 2 of the *FCR* states: tribunal has the same meaning as “**federal board, commission or other tribunal**” in the Act. Ergo, the RCMP is a Tribunal under the Court Rules and under the *Federal Courts Act*.

Moreover, the person or persons, exercising validly pursuant to delegation by the Head of the Government Institution (RCMP) or purporting to exercise powers pursuant to an Act of Parliament (specifically the *Privacy Act* and/or *ATIA*) are part of the definition of Tribunal or “**Federal Commission, Board, or Other Tribunal**” under the *FCA*. Pursuant to section 73(1) of the *Privacy Act*, Mr. Brisson is listed as the Director General ATIPB of the RCMP, and Mr. Jeff Ball has represented himself to be a Director of Privacy with the RCMP.

(Set out the date and details of the decision, order or other matter in respect of which judicial review is sought)

In relation to the decisions, orders, or other matters in respect of which judicial review is sought, some involve that which could be considered an “Order” (see: section 2 of the *FCR*) as they involve a decision or other disposition of a Tribunal.

The other matters in respect of which judicial review is sought involve the purported exercising of jurisdiction or powers under the *Privacy Act* which stem from documents in the possession of the Applicant but also documents not in the possession of the Applicant.

The details of the decision, order or other matter in respect of which judicial review is sought involving the failure to search issue, which constitutes an Order under the *FCA* and *FCR*, was on April 27, 2026, and so communicated to the Applicant by the RCMP via email. Nonetheless, the Respondent took an extension of time of some 60 days from the date of receipt of the Applicant’s express mail, with tracking, access request under the *Privacy Act*, which was received by the RCMP on March 11, 2026. 60 days from said date was May 11, 2026.

The RCMP did not communicate to the Applicant that it conducted any further searches of the required repositories including but not limited to: Foundational Metadata Repositories for the Foundational Metadata; and the Offline Historical Database with respect to any hexadecimal dumps involving any potential amended or purged data that was consistent or not consistent with the “False Information Package” which was filed in a transferee courthouse known as the OCJ 10 Armoury Street Courthouse. The failure to search decision of the RCMP and the individual Respondents, some or all (as known to each), is the subject of the mandamus relief *infra*.

The details of the decision, order or other matter also involve the neglect or failure to consider the requirement of the Head of the RCMP to consider whether, pursuant to ss. 8(2), particularly clause 8(2)(m) of the *Privacy Act*, and expressly or by

implication section 19 of the *ATIA*, to disclose to the Applicant any Personal Information and to the public at large or certain segments of the public any record under the *ATIA* requests of the Applicant in April and May 2026.

6

1. The applicant makes application for:

a. **Loss of Jurisdiction by the RCMP Tribunal:**

1. **A Declaration** that the RCMP Tribunal, pursuant to section 2 of the FCR and section 2 of the FCA lost jurisdiction over, or acted without jurisdiction in relation to, Matter No. **P-2025-16999** (albeit the PII Access Request (March 11 2026) was made and delivered on March 11, 2026) by reason of: a. a breach of the duties of good faith and procedural fairness; b. the presence of conflicts of interest, actual bias, and/or a reasonable apprehension of bias; and c. a profound lack of operational independence and impartiality;
 2. **A Declaration** that the Respondent exceeded its statutory mandate, refused to exercise its mandatory jurisdiction, and/or improperly purported to exercise powers outside of its jurisdiction in an *ultra vires* manner, rendering any and all steps, proceedings, and decisions in Matter No. **P-2025-16999** void *ab initio*;
- b. **Mandamus:** An Order in the nature of writ of mandamus compelling the RCMP to discharge its public duty to act to the Applicant to search for the requested Personal Information;
- c. **Mandamus:** An Order in the nature of Writ of Mandamus compelling the RCMP, through the Head of the RCMP in the RCMP Commissioner, Mr. Michael Duheme, to discharge its public duty to consider whether a public interest disclosure is required under section 8(2)(m) of the *Privacy Act* with reference to section 19 of the *Access to Information Act*;
- d. **Compliance Confirmation:** An Order directing the RCMP to provide a sworn affidavit or declaration from a qualified person detailing the searches conducted pursuant to this Order, including audits of the Foundational Metadata Request and hexadecimal searches of the Offline Historical Database relating to the Applicant's Personal Information. An Order that this affidavit or declaration shall be served on the Applicant and filed with this Honourable Court within five (5) days of the date of this Order;
- e. **Prohibition:** An Order in the nature of writ of prohibition enjoining the Respondent, its delegates, administrators, custodians, and any affiliated bodies from expunging, altering, transferring, sanitizing, migrating, obfuscating, or archiving beyond rapid retrieval any metadata, system logs, or historical audit trails associated with Police Case ID: 457197 (and any related TPS Case File or Occurrence Number) pending the final adjudication of this Application and the exhaustion of all appeals;
- f. **Prohibition:** An Order in the nature of writ of prohibition or injunctive relief restraining from searching repositories that were not within the scope of PII Access Request (March 11 2026) for the purposes of said access request;
- g. **Judicial Oversight:** An Order that this Honourable Court remain seized of this matter to oversee compliance with the Orders herein and to address any subsequent issues arising from the Respondent's execution of these directives;
- h. **Interim and injunctive relief:** An Order granting immediate interim injunctive relief pending the final disposition of this Application;
- i. **Permanent injunctive relief:** An Order granting permanent injunctive relief to abate the ongoing statutory breaches;
- j. **Bad faith and improper motives:** A Declaration that by failing to discharge public ministerial or executory duties to act to the Applicant at first instance and in the face of demands by the Applicant, the Respondents engaged in improper motives, bad faith, abuse of process, or other impermissible

reasons for purporting to exercise a power pursuant to an Act of Parliament or refusing to exercise jurisdiction or a power under an Act of Parliament;

- k. **Breach of Fiduciary duties:** A Declaration that the Respondents breached their duties of good faith and/or fiduciary duties to the Applicant and the public by their conduct herein;
- l. **Procedural unfairness:** A Declaration that the Respondents breached their duties owed to the Applicant of procedural fairness, natural justice, and administrative fairness;
- m. **Decision making bias, dependence and partiality:** A Declaration that the Respondents were actually biased towards the Applicant and/or exhibited the appearance of bias to a reasonable and informed observer. A further **Declaration** that there was and is a reasonable apprehension of bias, lack of independence, lack of impartiality amongst the Respondents and all of those within the ATIP Branch and the RCMP policing forces as it relates to the issues and grounds in this Proceeding herein;
- n. **Dependence and partiality:** A Declaration that the Respondents were operating under, or had the reasonable appearance of, a conflict of interest, a lack of institutional independence, and/or a lack of impartiality;
- o. **Police Case ID: 457197:** A Declaration that the Police Case ID: 457197 or part of that number is a jurisdictional identifier uniquely assigned by the RCMP;
- p. **Admissions and Estoppel by record:** A Declaration that the April 27, 2026, letter signed by Ms. Worrell on behalf of Mr. Jeff Ball, Director, Privacy (RCMP) with a metadata author of Kristen Wardrop, and the appended three page document from the RCMP, when measured against the referenced letter appended by the appellant under MFIPPA involving the Halton Regional Police Services Board (indexed as 2024 CanLII 67092 (ON IPC) (Order MO-4542; Appeal MA21-00096) (the “Halton Police 2024 Case”)), amounts to an admission at law or, in the alternative, that Respondents are estopped by record as end notedⁱ;
- q. **Unrequested search of Specialized Policing Services of RCMP:** A Declaration that the Respondent, RCMP, and Mr. Ball’s inclusion of an admission that it searched in the “Specialized Policing Services” amounts to an institutional admission that the Applicant’s Personal Information migrated out of standard divisional boundaries and directly into the RCMP’s national operational and technological commandⁱⁱ;
- r. **Originating Police Agency (RCMP):** A Declaration that the RCMP was the originating law enforcement agency by reference to either the RCMP former Ontario (“O” or “O Division”) Headquarters, later renamed to “Central Region” in London, Ontario, with an ORI Number of ON80300 under CPIC (the “CPIC Number 80300”) and its RCMP Regional Commander (“Reg. COM”), Mr. Matt Peggs or the RCMP Toronto West Detachment located in Milton, Ontario (the “Toronto West Detachment” or “TWD”) with CPIC ORI Number ON803313, which is responsible for Toronto West;
- s. **TPS 14th Division in Toronto (West) without copy of INTAKE COURT ENDORSEMENT (SEPT 23 2024) and/or “warrant in the first”:** A Declaration that one of the underlying reasons the Toronto Police Services Board (“TPS”), 14th Division did not have a copy of the purported process(es) or warrants and the arresting Police Officers did not have a copy on “him” or “her” and were unable to produce it when formally requested to do so, pursuant to the Applicant’s Charter rights and section 29 of the Criminal Code, was because the RCMP had sole possession, control and custody in its file under Police Case ID: 457197 or otherwise, and the respective RCMP and TPS digital architectures do not synchronize;
- t. **The most convenient fictitious Justice for the False Information Package:** A Declaration that the underlying reason Justice of the Peace Mr. George Jiri was utilized as the fictitious authorizing justice of the peace was due to, inter alia, his proximity in Peel Regional Police Services (OCJ Brampton) to the OCJ Brampton Courthouse which was the closest courthouse to the RCMP TWD (Milton);
- u. **RCMP possession of Authentic Information Package:** A Declaration that the RCMP has maintained possession (actual and sole, as it relates to Executive Branches of government of law

enforcement) of the underlying authentic, completed, sworn (deemed or in person) Information package (the “Authentic Information Package”), alongside any endorsements or warrants, since their completion, including any transcription by the “law enforcement applicant” of an in-person judicial chambers appearance and/or via telecommunication that “produced a writing” and/or that did “not produce a writing”;

- v. **RCMP denoted unlawful seizure and search:** A Declaration that the RCMP through designated agents on its behalf unlawfully seized the Applicant’s property (primarily chattels including private, confidential and/or privileged documentation from this residence at Unit 410-775 King Street West, City of Toronto, Province of Ontario, M5V 2K3) and/or without lawful execution upon him with a search and/or seizure warrant, on or after September 20, 2024 and prior to October 2, 2024;
- w. **Improper motives to not search the PIB and other repositories:** A Declaration that the sole reason the RCMP ATIP Branch did not search the Personal Information Bank request and any locations under the control of it was because it knew, or was deemed to know, that it would have irrevocably implicated the RCMP Specialized Policing Services’ (the “SPS”) unit or an alternate RCMP department;
- x. **Forthwith search of Foundational Metadata Location and Offline Historical Database Location:** An Order that, on account of the RCMP SPS’ unit being involved with the Applicant commencing in 2024 but concealed from the Applicant, such a search of the RCMP CPIC database, including Foundational and Offline Historical Database repositories, must be executed forthwith, and that the RCMP ATIP Branch must assign qualified individuals to conduct an audit under the Foundational Metadata Request alongside a specialized, qualified individual to conduct the specialized mainframe analysis of hexadecimal dumps and hexadecimal inputs;
- y. **Privacy Act, section 10:** A Declaration that the Applicant is legally entitled to all of his personal information under the control of the Government Institution (RCMP) that has been used, is being used, or is available for use for an administrative purpose pursuant to ss. 10(1)(a) of the *Privacy Act*, or is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual (see: ss. 10(1)(b) of the *Privacy Act*);
- z. **Temporal computation declaration:** A Declaration that the Applicant provided, by his PII Access Request (March 11 2026), received on said date and not March 12, 2026, sufficiently specific information regarding the location of the information as to render it reasonably retrievable by the government institution;
- aa. **Offline Historical Database:**
 - 1. A Declaration that the RCMP has exclusively control of the Offline Historical Database over any and all other police service board and police services in the country;
 - 2. A Declaration and Order that the Applicant is entitled to any and all transactional logs including “ADD”, “MODIFY”, “CLEAR”, and “CANCEL”, but solely in relation to Personal Information concerning himselfⁱⁱⁱ;
- bb. **Inapplicability of Privacy Act, ss. 19(1)(d):**
 - 1. A Declaration that ss. 19(1)(d) of the *Privacy Act* bears no applicability to the Personal Information sought by the Applicant in a PIB or otherwise, as such Personal Information relates to that which was uploaded or input into CPIC, as those inputs provide the ultimate source of truth in relation to public court records like an Information or an Indictment, court endorsements, a summons, and/or an arrest warrant, which are universally publicly available after a process has been issued and/or an individual has been arrested;
 - 2. A Further Declaration that not only is the Applicant legally entitled to the same but so is the public at large, and no equitable duty of confidence arises as the Personal Information of the Applicant—also the Personal Information of a presiding Judge, of which they are both entitled to the same under the *Privacy Act* and the public under *ATIA*, along with the name of the fictitiously input Justice of the Peace under the *Privacy Act*—is unequivocally public information and constitutes public records subject to the ss. 19(2) of the *Privacy Act* override;

cc. Duty of Confidence never arises with non-exempt PIB's and CPIC:

1. A further Declaration that the Personal Information sought by the Applicant in a PIB and in any repository involving CPIC or related to CPIC could not meet the common law test for "confidential information" because whether classified as Personal Information or information (i.e. transactional logs, terminal ID's, issuing court, issuing court level, geographic location, system identification numbers, modification to WANT records) (i) such information was not communicated in a relationship of confidence; (ii) the information by its very nature is NOT confidential; and/or (iii) the information was not communicated for a purpose that necessitates confidentiality;
- dd. PII Access Request (March 11 2026) related to administrative data (not "intelligence"):** A Declaration that the Personal Information that the Applicant was seeking under the *Privacy Act* constituted administrative data of himself and not intelligence per se, but rather the administrative record of a transaction on a federal mainframe (CPIC), and the likes of the Terminal ID, ORI, issuing authority, name of a judicial officer, and system identification number (SID) are structural artifacts of the RCMP's own system architecture, and not confidential communications;
- ee. Section 19 inapplicable when RCMP is the originating police force:** A Declaration of Law that Parliament did not include the likes of a federal government established by or pursuant to an Act of the legislature or a province, or an institution of such a government, under ss. 19(1)(d), and to the extent that the RCMP was strictly responsible for its entry, the RCMP can never rely on ss. 19(1)(d) in relation to requests for administrative Personal Information residing in a PIB or in CPIC, alongside Foundational Metadata and Offline Historical Database Personal Information;
- ff. Section 22(1)(b) without merit in relation to PII Access Request (March 11 2026):** A Declaration that the RCMP's reliance on section 22(1)(b), entirely absent the searching of the storage, repositories, or locations housing the Foundational Metadata Request and Offline Historical Database Request, does not fall under ss. 22(1)(b), and by relying on such a subsection, the RCMP admitted that the Applicant had not received access to or disclosure of his own **Personal Information**, which acts as the source of truth to be measured against the "Open Court Principle"^{iv};
- gg. Warrant spent on October 2, 2024:** A Declaration that once the warrant (arrest), when signed or not signed by the undisclosed presiding Judge in an "Ex Parte In Camera Hearing", whether in person in judicial chambers or via telecommunication that did or did not produce a writing, was executed on October 2, 2024, the investigative necessity of the CPIC entry definitively expired and transformed into a historical artifact, thus section 22(1)(b) holds no relevance *ab initio* or thereafter despite the blatant absence of a search;
- hh. Identity of the municipal or regional government:** A Declaration that the RCMP is statutorily required to provide the identity of the municipal government or "regional government" that it was vaguely referring to under section 19(1)(d) in its April 27, 2026, letter;
- ii. Consequential Relief:** An Order granting any consequential relief that flows from the above, or the required materials to be filed by the Tribunal that were in its possession at the time of making any decisions, orders, or other matters subject to judicial review herein known or to be known;
- jj. Leave to make further submissions:** An Order granting the Applicant leave to make further submissions and tender further evidence pre- and post-granting of the orders herein to avoid any multiplicity of proceedings and the avoidance of wasteful and deleterious government spending, alongside the inefficient use of government resources;
- kk. Costs:** An Order granting the costs of this Application on a full indemnity basis;
- ll. Interest:** An Order granting prejudgment and post judgment interest on any costs awards or otherwise; and
- mm. Residual Relief:** An Order granting such further and other relief as this Honourable Court may deem just and equitable.

The grounds for the application are:

The Applicant and the Foundational Factual Matrix: A Contextual Substratum of Systemic Obfuscation

Introduction and Jurisdictional Nullification

2. It is respectfully submitted that a profound, unprecedented, and systemic manipulation of judicial instruments was effectuated *post facto* to the arrest of Mr. Kevin A. McLean (the “**Applicant**”) on October 2, 2024. Consequently, the purported processes, including the underlying criminal proceedings (the “**Criminal Proceeding**”), were rendered void *ab initio* upon the fabrication of a fraudulent document, in direct contravention of the *Criminal Code*, RSC 1985, c C-46 (the “**Criminal Code**”), and upon its subsequent filing within the Ontario Court of Justice 10 Armoury Street Courthouse (the “**Armoury Street Courthouse**”). It must be categorically established *in limine* that the aforementioned fabrication constitutes an absolute nullity, and cannot be construed as a mere procedural irregularity, given the direct contravention of statutory mandates, common law precepts, and equitable principles.
3. The designation of the aforementioned fabrication as an unprecedented information package (the “**False Information Package**”) is utilized meticulously, as the historical jurisprudence and public disciplinary registries of this jurisdiction are devoid of any analogous manifestation of malfeasance. The documented transgressions delineate circumstances wherein law enforcement authorities not merely manipulated the endorsement of a process or an arrest warrant through the impersonation of a judicial officer, but effectuated the wholesale falsification of an entire information package, purportedly assembled pursuant to the *Criminal Code*.^v

Jurisprudential Distinctions: Subfacial Deficiencies versus Absolute Nullities

4. To substantiate the gravity of subfacial and facial fabrications, reliance is placed upon *R. v. Schertzer*, 2015 ONCA 259 (the “**Schertzer Decision**”), and *R. v. Hansen*, 2018 ONCA 46 (the “**Hansen Decision**”). These appellate authorities adjudicated instances of subfacial fabrication, wherein ostensibly valid judicial authorizations were rendered constitutionally defective due to underlying prevarications promulgated by law enforcement officials regarding the scope of their investigations and the purported existence of reasonable grounds to believe (the “**Reasonable Grounds To Believe**”).
5. The **Schertzer Decision** involved the falsification of police notes designed to conceal an unlawful search, whereas the **Hansen Decision** addressed the invalidation of search warrants predicated upon misleading information sworn by affiants. Applying the legal principles elucidated therein to the present factual matrix, it is evident that the actions deployed against the Applicant transcend mere subfacial deficiencies; they constitute overt, absolute fabrications of judicial processes *ab initio*.

- 11** 6. A comparative analysis necessitates an examination of *Silva v. R.*, 2021 QCCS 4627, and *Silva v. R.*, 2021 QCCS 4131 (collectively, the “**R. v. Silva Decisions**”). The factual matrix therein involved an officer of the Service de Police de la Ville de Montréal (the “**SPVM**”), Officer Guillaume Joly-Tessier, who temporarily misappropriated a judicial stamp belonging to a Justice of the Peace to forge an arrest warrant. The target of said fabrication was a highly dangerous, convicted fugitive possessing a documented history of severe, violent criminality, including armed robbery and murder. While the misconduct elucidated in the “**R. v. Silva Decisions**” was undeniably deplorable, it was rationalized internally as a manifestation of noble-cause corruption, undertaken *in extremis* to apprehend a significant threat to public safety.
7. Conversely, the circumstances surrounding the Applicant, an individual devoid of any criminal antecedents but for the soundly defeating of the RCMP and former RCMP officers while retained by the soon to be defunct LSBC, stand in stark contrast to the preceding authorities. The fabrication of the *Criminal Code Form 2 Information* (the “**Form Two Information**”) within the False Information Package involved the installation of a Toronto Region Court Officer, Mrs. Frugoni-Rojas, as a fabricated informant (the “**Fictitious Informant**”). Furthermore, the process ostensibly engaged a fictitious Justice of the Peace, Mr. George Jiri, improperly ascribed to the Ontario Court of Justice Brampton Courthouse (the “**Brampton Courthouse**”). The Applicant maintained no residential or jurisdictional nexus to the Brampton Courthouse. Geographically and jurisdictionally, the Royal Canadian Mounted Police Milton Detachment (the “**RCMP Milton Detachment**”) operated with proximity and oversight regarding specific federal matters within Toronto West. Simply put, unprecedented fraud on two levels of court involving a fictitious informant and fictitious judicial officer. More colourfully put, Mr. Jeff Ball, Director, Privacy, of the RCMP ATIB Branch has the audacity to represent that he cannot search the Foundational Metadata Repository and Offline Historical Database Repository. The Applicant pleads that the RCMP ATIB Branch must search but it does not want to search for fear of what it will discover.

Systemic Institutional Obfuscation and the Absence of Competent Jurisdiction

8. The systemic manipulation extended to the purported identification mechanisms, specifically Police Case ID: 457197 and the altered designation “C L (M)”, which, calculated upon a balance of probabilities, referenced the Regional Commander of the Central Region, Mr. Matt Peggs (the “**Regional Commander**”), potentially in connection with his investiture into the Order of Merit of the Police Forces. Subsequent investigations executed by the Applicant, initially in March 2025 and subsequently verified directly at the Armoury Street Courthouse in June 2025, confirmed the absolute non-involvement of any legitimately appointed judicial officer from the Toronto Region.
9. Consequently, the purported *ex parte in camera* proceeding (the “**Ex Parte Hearing**”) was discovered to have been ostensibly situated at the Superior Court of Justice 361 University Avenue Courthouse (the “**Originating**”).

- 12** Courthouse”). It was subsequently unveiled that the originating office was the family law division situated on the primary level of the Originating Courthouse. This geographical and structural anomaly illuminated the improper involvement of Madam Justice Shore, who, during her tenure as practicing counsel, provided representation to the former spouse of the Applicant’s former common-law partner, Mr. Papadimitropoulos.
10. At the material times, Mr. Papadimitropoulos operated as the Statutory Accident Benefits Schedule manager (the “**SABS Manager**”) at the TD Insurance Group, wherein he perpetrated a multifaceted fraud concerning the administration of the Applicant’s accident benefits. These benefits originated from an automobile collision devoid of fault on the part of the Applicant, which occurred on August 31, 2022. Following the discovery of fraudulent signatures effectuated by Mr. Papadimitropoulos, he was subsequently dismissed from his employment in January 2025. Upon the Applicant's discovery of the aforementioned fraudulent activities on September 19, 2024, the Applicant was subjected to an unlawful exclusion from his residence on September 20, 2024, ostensibly facilitated by proximate law enforcement personnel.
 11. The fabricated endorsement, dated September 23, 2024 (the “**Intake Court Endorsement**”), remained facially irregular and evocative of family law or insolvency proceedings, rather than criminal adjudication. The Applicant’s subsequent efforts to secure a copy of the *Criminal Code Form 7 Warrant for Arrest* (the “**Form Seven Warrant**”) were systematically thwarted by the administrative apparatus at room 241 of the Originating Courthouse.
 12. *Nota bene*: It might be argued by the Respondents that the utilization of family court facilities or mislabeled endorsements merely constitutes an administrative irregularity capable of being cured under equitable principles or procedural rules. However, applying Herbert Broom's maxim *actus curiae neminem gravabit* (an act of the court shall prejudice no man), alongside the strict doctrine of jurisdictional competence, it is submitted that a proceeding commenced in a wholly inappropriate division by way of forged documentation constitutes a fundamental nullity, rendering all subsequent enforcement actions *ultra vires*. The Royal Canadian Mounted Police (the “**RCMP**”) is consequently bound to produce the unredacted evidentiary materials pursuant to *Rule 317* of the *Federal Courts Rules*, SOR/98-106 (the “**Federal Courts Rules**”).

Digital Forgery and the Mandate for Remedial Disclosure

13. It must be emphasized that the execution of the False Information Package was facilitated utilizing GrapeCity manipulation software, currently operating under the nomenclature “Mescius” (the “**GrapeCity Software**”). The metadata extracted from the impugned documentation corroborates the deployment of version 6.0.2.0 of the GrapeCity Software. This revelation, which is the subject of two formalized requests under the *Access to Information Act*, RSC 1985, c A-1 (the “**ATIA**”), funded and submitted by the Applicant in the vernal season of 2026, cements the unprecedented nature of this malfeasance. The imperative is unequivocally placed upon the Head of the Government Institution (the “**Institution Head**”) to issue public disclosure notices pursuant to paragraph

13 8(2)(m) of the *Privacy Act*, RSC 1985, c P-21 (the “**Privacy Act**”), and section 19 of the *ATIA*, to prevent the perpetuation of this systemic abuse, restoring the *status quo ante* for any other members of the populace who may be subjected to similar covert manipulations.

14. The Criminal Proceeding was rendered a nullity, at law, *ab initio* at the precise moment of its digital fabrication.

The Respondents: Statutory Delegates, Fiduciary Obligations, and the Federal Apparatus

15. The Royal Canadian Mounted Police (the “**RCMP**”) is a federal institution and Government Institution under the Privacy constituted and governed by the strictures of the *Royal Canadian Mounted Police Act* (the “**RCMP Act**”).

16. Commissioner Michael Duheme, in his capacity as the apex of the institution, is inextricably bound by the administrative and fiduciary obligations legislated by Parliament.

17. Director General Stephane Brisson and Privacy Director Jeff Ball, acting as delegates within the Access to Information and Privacy Branch, are similarly constrained by the unyielding imperatives of statutory compliance.

18. The paramount importance of the *RCMP Act* is underscored by the solemn statutory duties articulated under section 37 thereof, which compels adherence to the highest standard of conduct. This obligation is further entrenched by the oaths sworn by the Respondents to uphold the law, fundamentally precluding any *ultra vires* administrative shielding or institutional complicity.

EQUITABLE REMEDIES IN THE NATURE OF MANDAMUS: COMPELLING THE EXECUTION OF NON-DISCRETIONARY PUBLIC DUTIES

19. Relief in the nature of mandamus constitutes an imperative and equitable prerogative remedy, available to compel the performance of a public duty that has been unlawfully disregarded.

20. The rigorous legal test for mandamus is demonstrably satisfied, as delineated by the Federal Court of Appeal in *Apotex Inc. v. Canada (Attorney General)* (the “*Apotex*”).

21. It is self-evident that clear, unequivocally articulated demands were effectuated by the Applicant, triggering the Respondents’ strict legal duties to conduct searches of the Foundational Metadata Repository and the Offline Historical Database Repository. The ensuing period of administrative silence and *de facto* refusal necessitates judicial intervention *in limine* to restore the *status quo ante* and compel the execution of the statutory mandate.

PREROGATIVE RELIEF IN THE NATURE OF PROHIBITION: ENJOINING PROSPECTIVE MALFEASANCE AND DIGITAL SPOILIATION

22. An order of prohibition is sought *in limine* to permanently enjoin the Respondents, and any delegated subordinates, from the spoliation, deletion, alteration, or obfuscation of immutable digital artifacts residing within the federal architecture.

- 14** 23. The tripartite test for prohibition is incontrovertibly met, predicated upon *prima facie* evidence of impending administrative malfeasance, rendering such extraordinary relief imperative to safeguard the integrity of the administration of justice.
24. The entitlement to such relief is crystallized by the imperative to safeguard the foundational metadata and hexadecimal arrays residing within the Canadian Police Information Centre (the “CPIC”).

DECLARATORY JUDGMENTS: ESTABLISHING JURISDICTIONAL NULLITY AND VINDICATING SUBSTANTIVE RIGHTS

25. Declaratory judgments are within the absolute discretion of a court with equitable jurisdiction (not to be conflated with Inherent Jurisdiction) like the FCC. They serve as potent instruments of judicial oversight, invoked to authoritatively pronounce upon the rights of the parties and the legal characterization of *acta* undertaken by public bodies
26. While acknowledging the inherently discretionary purview of the Federal Court of Canada (the “FCC”), the test for declaratory relief is incontrovertibly satisfied by the presence of a real, substantial, and immediate dispute wherein the Applicant possesses a vital interest.
27. The utility of such declarations is paramount in exposing the systemic bypass of mandatory legislative frameworks, thereby establishing an authoritative and permanent record of the nullity of the manipulated judicial instruments.

OUSTER OF INSTITUTIONAL JURISDICTION: FATAL APPREHENSION OF BIAS, FUTILITY, AND STRUCTURAL INCOMPETENCE

28. **The Test for Losing Jurisdiction:** It is an established principle of administrative law that a reviewing court will completely strip a tribunal of its jurisdiction—refusing to remit the matter back—only under exceptional circumstances where the tribunal is rendered legally incapable of providing a fair or valid rehearing.
29. **The Core Legal Test:** To displace the standard remedy of remitting a case back to a tribunal, an applicant must demonstrate that remittal would be futile, unfair, or fundamentally break the administration of justice. The court rigorously examines whether the tribunal can still fulfill its statutory duty impartially and effectively.
30. **Reasonable Apprehension of Bias (Conflict of Interest):** The Respondents operate under a reasonable apprehension of systemic bias and conflict of interest, rendering the tribunal legally incapable of providing an independent review, thereby necessitating that this Honourable Court retain absolute jurisdiction over the matter.

15 31. **Failure or Refusal to Exercise Jurisdiction:** The Tribunal fundamentally misinterpreted its statutory mandate and displayed a persistent unwillingness to apply the law, culminating in a grave jurisdictional error that requires direct judicial intervention to prevent repeated procedural failures.

32. **The Futility and Operational Exception:** Based on the totality of the Respondents’ inadequate responses under the *Privacy Act* and *ATIA*, remitting this matter back to the Tribunal would be futile, serve no practical legal purpose, and constitute an unjustifiable waste of public resources.

33. **Severe Lack of Institutional Competence:** The statutory duty imposed on the Commissioner to determine public interest disclosure places the RCMP in an inherent conflict, irreparably compromising its independence and establishing a structural incapacity to conduct a procedurally fair adjudication of the Applicant’s requests.

FORENSIC AND TECHNICAL METADATA IMPERATIVES: EXPOSING THE DIGITAL METAMORPHOSIS OF JUDICIAL INSTRUMENTS

34. **Forensic Analysis of Automated Document Generation:** It is submitted that the impugned document identified as “Information Package 4810 998 24 48129169-00”, affixed post facto and no earlier than November 1, 2024, (with first appearance of the Applicant scheduled for November 13, 2024, pursuant to a Criminal Code Form 10 Undertaking which was begrudgingly prepared by the TPS on account of the Applicant demanding incessantly and admittedly, while incarcerated, with passion, and notably without any reference to Police Case ID: 457197 contained in the Criminal Code Form 10 Undertaking) exhibits catastrophic structural anomalies. A critical component of this forensic reality is the identification of *GrapeCity Documents for PDF* version 6.0.2.0 as the document producer—a software development kit (“the SDK”) rather than a standard end-user application. The presence of this metadata inextricably proves that the document was generated via an automated back-end script, thereby constituting an unauthorized procedural bypass of the *FRANK/ICON* case management systems.

35. **Integrated Analysis of the False Information Package (the “FIP”):** The table below delineates the profound factual errors, technical metadata failures, and procedural diversions characterizing the FIP:

Category	Specific Deficiency	Location	Legal Implication & Forensic Depth

Case ID: 16 Indexing	Police Case ID: 457197	Page 3	The Barcode of Fraud: Valid ICON/CCO Case IDs are strictly 7 digits. This anomaly signifies an entirely fabricated or transposed file architecture. TPS Case ID and/or occurrence numbers contain the year with hyphen and eight digits. Ergo, the remaining portion of a non-particularized police force confirms, by deduction and exclusionary logic, that the RCMP was the originating police force (nota bene: RCMP refers to its policing units as “forces” whereas the TPS refers to themselves as “services” by way of divisions)

THE TEMPORAL ANOMALY AND ALGORITHMIC SURVEILLANCE AUDIT TRAIL: PRIMA FACIE EVIDENCE OF PRE-EMPTIVE SURVEILLANCE

36. The documentary record reveals a glaring chronological discrepancy within the RCMP’s purported *Privacy Act* response dated April 27, 2026. Despite acknowledging receipt of the Applicant’s request on March 17, 2026, the matter was unilaterally assigned the federal file identifier P-2025-16999.
37. In the rigorous domain of federal records management, this prefix irrevocably denotes the year the file was initiated. This temporal anomaly establishes *prima facie* evidence that the RCMP had already commenced an active intelligence, surveillance, or audit file concerning the Applicant in 2025, operating in parallel with concurrent civil litigation, thereby completely demolishing the fiction that this was ever a localized municipal matter.
38. Furthermore, the generation of a specific maximum-threshold algorithm log in April 2026, inextricably paired with the query “Q PERS+ REM:000330500”, constitutes incontrovertible digital proof that federal actors were actively hunting, verifying, or manipulating the precise identity of the Applicant within a secured federal network.

THE RULE 317 MANDATE: EXTRACTION AND COMPULSORY PRODUCTION OF THE CERTIFIED TRIBUNAL RECORD

39. To secure the comprehensive adjudication of this Application, the transmission of the complete Certified Tribunal Record (the “CTR”) is mandated pursuant to Rule 317 of the *Federal Courts Rules*.
40. The evidentiary matrix necessitates the extraction and certification of three distinct tiers of Personal Information currently suppressed by the Respondents:

Data Type	Primary Source	Level of Effort	Forensic Value
Active Warrant Status	CPIC “Persons” File	Low (Routine Query)	Operational verification only.

Foundational Metadata (PI, Terminal ID)	Transaction Logs (PPU 005)	Moderate (Requires Audit)	Identifies the true genesis of the digital record.
Amended/Purged Data (The “Frankendoc”)	Offline Historical Database	High (Specialized Extraction)	Exposes post-execution structural metamorphosis and unauthorized jurisdictional transfers.

41. The mandatory certification of these materials, circumventing the pervasive administrative deflections, is legally indispensable for exposing the unauthorized post-execution alterations regarding the identity of the authorizing judicial officer, the date, and the true jurisdictional origin of the warrant, thereby ensuring the Court is equipped to adjudicate the jurisdictional nullity *de novo*. The Applicant repeats and relies upon the exhaustive factual and legal grounds particularized within the Applicant’s standalone Written Request and Supporting Submission Pursuant to Rule 317 of the Federal Courts Rules, served upon the Respondents concurrently on May 18, 2026. The Applicant states that the explicit invocation of remedies in the nature of Prerogative Writs of Mandamus and Prohibition, conjoined with specific allegations of bad faith, institutional bias, and systemic conflict of interest involving Regional Commander Mr. Matt Peggs (Central Region), legally expands the mandatory disclosure test of the Certified Tribunal Record (the “CTR”) to encompass all 18 categories of raw historical metadata, transaction logs, application software library artifacts, and core charging instruments housed within Personal Information Bank (PIB RCMP PPU 005). Said PIB is not an exempt bank under any regulation under the *Privacy Act*.

ACTIONABLE NEGLECT OF STATUTORY DUTY, DOCTRINAL IMPERATIVES, AND INSTITUTIONAL MALFEASANCE

42. It is averred that the impugned conduct transcends mere administrative oversight, constituting an actionable neglect of duty, administrative malfeasance, and the deliberate spoliation of digital evidence orchestrated at the highest echelons of the Central Region Command, specifically implicating Regional Commander Mr. Matt Peggs.
43. The systemic, institutionalized suppression of publicly accessible judicial records fundamentally rebuts the presumption of *omnia praesumuntur rite et solemniter esse acta*, necessitating immediate judicial intervention to enforce the maxim *ubi jus ibi remedium*.
44. The foundational nullities embedded within the orchestrated process invoke the immutable doctrine of *quod ab initio non valet, in tractu temporis non convalescit*, permanently vitiating the Respondent’s purported jurisdictional authority. Furthermore, pursuant to the doctrine of *respondeat superior*, the Tribunal bears ultimate vicarious and institutional liability for the orchestrated obfuscation effectuated by its delegates and regional commanders. In light of the unlawful seizure and deprivation of property detailed herein, the equitable principle of *spoliatus debet ante*

THE EXCEPTION TO PLEADING EVIDENCE: PLEADING OF SIMILAR FACT EVIDENCE

45. It is acknowledged that the incorporation of evidentiary particulars within procedural pleadings is conventionally prohibited; notwithstanding said prohibition, an indispensable exception is effectuated when advancing similar fact evidence *in limine*. The extrapolation of overarching legal principles dictates that to establish a nexus of systemic malfeasance, the foundational factual substratum must be delineated with precision to demonstrate a continuing course of conduct. It might be asserted by opposing entities that such evidentiary inclusions contravene the *Rules of Civil Procedure* pertaining to the pleading of material facts exclusive of evidence. This presumption is comprehensively rebutted by the jurisprudential mandate articulated in *R. v. Handy, 2002 SCC 56* (the “*Handy Jurisprudence*”). In the *Handy Jurisprudence*, the Supreme Court of Canada elucidated the doctrine of similar fact evidence, establishing that where the probative value of antecedent conduct demonstrates a systemic pattern or characteristic methodology, such probative value substantially eclipses any purported prejudicial effect. Applied to the present circumstances, the pleading of systemic state-sponsored harassment is not merely permissible but legally mandatory to establish the requisite factual nexus of institutional malfeasance.

The Nullification of State Action and the Clandestine Extraction of Digital Memory

46. Whereas the aforementioned falsification of the documentation (the “**False Information Package**”) transcends rational comprehension, similar fact evidence is concurrently pleaded herein implicating the Royal Canadian Mounted Police (the “**RCMP**”) and specific former constabulary personnel affiliated therewith, notably Colin Cree and Laurie Windover, operating under the corporate auspices of EFS e-Forensic Services Inc. (the “**Forensic Corporation**”). It is submitted that the Forensic Corporation was retained to execute a forensic duplication of the primary storage apparatus utilized during the period of affiliation with the Law Society of British Columbia (the “**LSBC**”). Said entities were complicit in the clandestine and concealed extraction of the random access memory (the “**Random Access Memory**”), utilizing an invasive and malicious software application designated as “DumpIt”. Said application operated independently of the primary hard drive apparatus to execute a covert technological interception.

47. The potentiality of said clandestine extraction of the Random Access Memory was ascertained in the year 2021, prompting the invocation of statutory mechanisms pursuant to the *Freedom of Information and Protection of Privacy Act* directed toward the LSBC. Subsequent to said statutory demands, an extraction iteration was procured in hexadecimal format (the “**Hexadecimal Format**”), necessitating extraordinary technological investigation to

decipher. Consequently, compulsory demands for exculpatory documentation, explanations, and personal information (the “**Personal Information**”) were levied upon Mr. Cree and Mr. Windover. It is documented that Mr. Windover, manifesting profound indignation ostensibly resultant from the exposition of the malfeasance orchestrated by the LSBC and the Forensic Corporation, instituted technological barricades against the electronic correspondence address utilized for communications, specifically mclean@searchandseizure.ca (the “**Electronic Mail Address**”).

48. *Nota bene*: An analytical evaluation must address the classification of the utilization of the aforementioned malicious software. It is explicitly categorized not as a mere procedural irregularity, but as an absolute nullity *ab initio*, as it constituted a direct contravention of statutory privacy mandates and equitable principles. Pursuant to the legal maxims compiled in Herbert Broom’s *A Selection of Legal Maxims*, the principle of *Omnia praesumuntur contra spoliatores* (every presumption is made against a wrongdoer) is inextricably engaged. The clandestine extraction constitutes an *ultra vires* assumption of investigative authority, rendering the derived *acta* entirely devoid of legal force.

Frivolous Prosecutorial Initiations and Post Facto Fabrications

49. Extrapolating further upon the systemic pattern of harassment, an antecedent fabrication of criminal culpability was orchestrated by the detachment of the RCMP, as the sole police force in North Vancouver by way of agreement between the province and the federal government, situated in North Vancouver, British Columbia, in the year 2017. The allegations promulgated therein were determined by the reviewing Crown Counsel to be so conspicuously frivolous, vexatious, and bereft of substantive merit that prosecutorial authorization was summarily declined *ipso facto*, thereby preserving the *status quo ante*.

Nullity of Seizure and Calculated Ruses of Incarceration for extended captivity, inability to advance legal matters, serious injury, premature death and/or death

50. It is further submitted that upon the realization by the RCMP that a substantively deficient and unlawful investigative maneuver had been executed, culminating in an unlawful lockout and property confiscation concerning the principal residence located at Unit 410-775 King Street West, City of Toronto, Province of Ontario, M5V 2K3 (the “**Principal Residence**”), a meticulously calculated ruse was engineered. The aforementioned lockout, being a direct contravention of overarching common law property rights and the *Residential Tenancies Act, 2006, S.O. 2006, c. 17* (the “*RTA*”), is asserted to constitute an indisputable and irremediable nullity. In this regard, the RCMP clearly waited until the unlawful lockouts occurred to denote the Applicant as “NFA”.

- 20 51. Following demands for the restitution of chattels purportedly retained within the Principal Residence, the RCMP systematically transferred the unlawfully confiscated property from the RCMP Toronto West Detachment situated in Milton, Ontario, to a Toronto Police Service (the “TPS”) division designated as “Toronto West”. It is advanced that this geographical relocation was a premeditated subterfuge designed to orchestrate a physical apprehension, effectuating an incarceration without the provision of bail.
52. The underlying objective of this apprehension was the deliberate neutralization of formidable *pro se* litigation capabilities, representing at minimum the third manifestation of such strategic deprivation. Initial representations articulated by personnel of the TPS 14th Division indicated an impending transportation to an alternative maximum-security detention facility, presumably the Millhaven Institution, which is jurisprudentially recognized for its severe custodial conditions. The orchestration was purportedly designed to maximize systemic disadvantage, exploiting the absence of a principal residence and familial support infrastructure within the jurisdictional boundaries of Toronto, Ontario.

GOVERNING STATUTORY AND REGULATORY FRAMEWORKS RELIED UPON

53. The Applicant repeats and relies upon the authorities contained within communications between himself and the RCMP vis-à-vis his access requests under the *Privacy Act* and ATIA, along with any other documents provided to it. The Applicant relies upon the statutory and regulatory frameworks meticulously outlined in the following legislation:
- a. *Privacy Act*, R.S.C., 1985, c. P-21;
 - b. *Privacy Regulations*, SOR/83-508;
 - c. *Exempt Personal Information Bank Order, No. 5 (ND)*, SOR/85-38;
 - d. *Exempt Personal Information Bank Order, No. 13 (RCMP)*, SOR/90-149;
 - e. *Exempt Personal Information Bank Order, No. 14 (CSIS)*, SOR/92-688;
 - f. *Exempt Personal Information Bank Order, No. 25 (RCMP)*, SOR/93-272;
 - g. *Access to Information Act*, R.S.C., 1985, c. A-1 (the “*ATIA*”)
 - h. *Access to Information Regulations*, SOR/83-507;
 - i. *Federal Courts Act*, R.S.C., 1985, c. F-7;
 - j. *Federal Courts Rules*, SOR/98-106;
 - k. *Canada Evidence Act*, R.S.C., 1985, c. C-5, Part 1;
 - l. *Secure Electronic Signature Regulations*, SOR/2005-30, Part 1;
 - m. *Royal Canadian Mounted Police Act*, R.S.C., 1985, c. R-10;
 - n. *Royal Canadian Mounted Police Regulations, 2014*, SOR/2014-281;
 - o. *Commissioner’s Standing Orders (Conduct)*, SOR/2014-291;
 - p. *Commissioner’s Standing Orders (Classification Redress Process for Members)*, SOR/2001-248;
 - q. *Commissioner’s Standing Orders (Employment Requirements)*, SOR/2014-292;
 - r. *Commissioner’s Standing Orders (General Administration)*, SOR/2014-293;
 - s. *Commissioner’s Standing Orders (Grievances and Appeals)*, SOR/2014-289;
 - t. *Royal Canadian Mounted Police Public Complaints Commission Rules of Practice*, SOR/93-17;
 - u. *Enhancing Royal Canadian Mounted Police Accountability Act*, S.C. 2013, c. 18;
 - v. *Public Complaints and Review Commission Act*, S.C. 2024, c. 25;

- w. *Interpretation Act*, R.S.C., 1985, c. I-21;
- x. *Criminal Code*, R.S.C., 1985, c. C-46; and
- y. *Security Offences Act*, R.S.C., 1985, c. S-7.

This application will be supported by the following material:

54. The Affidavit^{vi} of Mr. Kevin A. McLean (BA, JD, CIM) or on his behalf, to be sworn, and the documentary exhibits attached thereto, including:
- a. Tab 1: The Applicant's statutory access request under the *Privacy Act*, dated February 27, 2026, and received by the Respondents on March 11, 2026, requesting the extraction of foundational metadata, raw hexadecimal dumps, and offline historical transaction logs from the CPIC database.
 - b. Tab 2: The Canada Post tracking and delivery confirmation certificate, verifying physical delivery and statutory service of the Applicant's *Privacy Act* request at the Respondents' Ottawa headquarters on March 11, 2026
 - c. Tab 3: Correspondence from mid-March 2026, containing the Applicant's detailed technical disclosure of relevant Toronto Police Service (TPS) Originating Agency Identifiers (ORIs), Case IDs, and a digital forensic metadata analysis identifying 43 structural anomalies tied to the GrapeCity PDF engine and the "CL (M)" software artifact
 - d. Tab 4: Administrative correspondence and records spanning March and April 2026, documenting the Respondents' unilateral 30-day time extension, the subsequent failure to search, and the formal dispute concerning the execution of superficial "live" terminal queries versus the requested offline database extractions
 - e. Tab 5: The purported statutory response from the RCMP ATIP branch, dated April 27, 2026, including the selective application of statutory exemptions to active 2025 data pools and the omission of 2024 historical transaction logs.
 - f. Tab 6: Electronic mail communications dated October 2, 2024, involving Constable Anthony Romano of the TPS (14 Division) regarding property retrieval, the Applicant's detention, and the processing of the underlying judicial authorizations.
 - g. Tab 7: The formal statutory complaint submitted by the Applicant to the Civilian Review and Complaints Commission for the RCMP (CRCC), concerning the administrative handling and tracking of records under the direction of Assistant Commissioner Matthew Peggs.
 - h. Tab 8: Unanswered written demands served upon Assistant Commissioner Matthew Peggs, seeking the production of authentic system metadata, verification of the "CL (M)" system artifact, and the return of property seized between September 20, 2024, and October 2, 2024.
 - i. Tab 9: The parallel statutory access request submitted by the Applicant under the *Access to Information Act* (ATIA) on May 5, 2026, targeting the National Technology Onboarding Program (NTOP) software procurement logs, enterprise licensing, and server-side deployment files for the MESCIUS / GrapeCity PDF software libraries.
 - j. Tab 10: Copies of the formal structural complaints submitted to the Office of the Privacy Commissioner of Canada (OPCC) regarding systemic data suppression, unauthorized search paths into Specialized Policing Services, and the ongoing refusal to search Personal Information Bank (PIB) RCMP PPU 005.
 - k. Tab 11: Documents and decision from LECA in Spring 2025;
 - l. Tab 12: Rule 317 of the *FCR* request of March 18, 2026;
 - m. Tab 13: documents involving the Similar Fact Evidence ("SFE") doctrine above;
 - n. Tab 14: Residual records: records, documents et al not captured by the above but relevant to the Application; and
 - o. Such further and other material as the Applicant may advise and this Honourable Court may permit.

22 55. The Applicant hereby requests that the Respondents send a certified copy of the material particularized in the Exhaustive Schedule of the standalone Written Request served upon the RCMP Tribunal on May 18, 2026, which is incorporated by reference herein:

SCHEDULE OF REQUESTED MATERIALS FOR PURPOSES OF A CERTIFIED TRIBUNAL RECORD

SCHEDULE OF REQUESTED MATERIALS

Item Number	Category of Material	Specific Records and Metadata Requested
1	Access Request Administrative Files	The complete internal administrative file, tracking sheets, and analyst worksheets concerning <i>Privacy Act</i> file P-2025-16999.
2	System Logs Initialization	The complete, unredacted system entry logs from the automated sequential registry system detailing the exact date, millisecond timestamp, and file initialization sequence that generated the prefix year “2025” for an access request delivered to the Respondent on March 11, 2026.
3	Executive and Inter-Directorate Communications	All electronic communications, emails, instant messages, memorandum chains, and briefing notes concerning the Applicant or file P-2025-16999 exchanged between Director Jeff Ball, Delegate Melissa Simpson, Director General Stéphane Brisson, Regional Commander Matt Peggs, or their authorized agents, and Chief of Staff Tanya Mirsky spanning April 1, 2026, to the present.
4	Internal Legal and Operational Advice	All legal or operational advice solicited or received internally regarding the Applicant’s statutory demand for access to the Canadian Police Information Centre (“CPIC”) Offline Historical Database metadata, including the Foundational Metadata Request and the Offline Historical Database Request.
5	Raw Mainframe Records Forensic Ledger	The raw, unredacted transaction logs, audit trails, and hexadecimal dumps residing within the secure CPIC Offline Historical Database associated with Personal Information Bank RCMP PPU 005 tied to the Applicant’s name, identifiers, or cross-referenced occurrence numbers (2024-2028093, 24-2082035, and Court File/Case ID 457197) spanning September 15, 2024, to December 31, 2024, inclusive.
6	Cryptographic Trails Audit	The complete cryptographic audit trails capturing all ADD, MODIFY, CLEAR, and CANCEL command strings, along with terminal identifiers, physical hardware addresses, Originating Agency Identifiers (“ORIs”), and unstructured narrative fields for each sequential transaction executed during the aforementioned temporal window.
7	Forensic Metadata of Search Methodology	The complete electronic system logs generated by Operator NBOISVERT on April 14, 2026, at 07:35:43, detailing the complete input syntax, query parameters, and system constraints utilized to execute the front-facing “Q PERS+” and “Q CNI” live database queries.
8	Internal Directives and Exclusion Policies	Any internal directives, policy documents, or operational notes instructing the Access to Information and Privacy (“ATIP”) Branch analysts to omit an interrogation of the Offline Historical Database in response to the Applicant’s explicit, specialized request for historical data.
9	Trans-Directorate Processing Records	The complete, unredacted administrative processing file, tracking timelines, and internal analyst notes concerning the concurrent <i>Access to Information Act</i> (“ATIA”) request submitted by the Applicant, explicitly targeting the procurement, enterprise licensing, and National Technology Onboarding Program (“NTOP”) integration logs of the Mescius SDK / GrapeCity.Documents.PDF.6.0.2.0 developer engines within the CPIC infrastructure.
10	Automated Linking Records File	All internal processing records showing any administrative coordination, automated file linking, or database cross-referencing executed between the privacy division handling <i>Privacy Act</i> request P-2025-16999 and the information access branch processing the parallel ATIA files.
11	Software Logs Exception	Any software error tracking logs, system exception reports, or developer audit alerts generated by the core CPIC mainframe database management system involving database inquiries or structural PDF modifications tied to the Applicant’s biographical identifiers or transaction history.
12	Executive Briefing Notes and Action Logs Suite	All briefing notes, corporate risk assessments, institutional action logs, and communications generated by or sent to Commissioner Michael Duheme and Director General Stéphane Brisson regarding the Applicant’s personal information or file P-2025-16999.
13	Central Command Communications Region	All emails, letters, instant messages, and administrative directives sent or received by Assistant Commissioner Matthew Peggs (Central Region Command) concerning Police Case ID: 457197, the “Adult Common Information Package,” or the collection and retention of the Applicant’s property from September 15, 2024, to the present.

Third-Party Transfer Ledgers	Data Ingestion	All cross-jurisdictional system logs showing the electronic receipt, intake vetting, and cryptographic mapping of data transferred from the Toronto Police Service (TPS) or Ontario Court of Justice (OCJ) to the RCMP <i>infrastructure</i> involving the Applicant's biographical profiles.
Primary Charging Instruments	Statutory	A certified copy of the Criminal Code Form 2 "Information" and/or Criminal Code Form 4 "Indictment" purportedly generated, indexed, or uploaded into federal tracking streams regarding the Applicant's underlying file.
Core Intake Endorsements	Courthouse	A certified copy of the Intake Court Endorsement represented on Page 3 of 5 within the disputed "False Information Package," capturing any handwriting, initials, or automated metadata strings applied during processing.
Originating Authorizations	Judicial	A certified copy of the alleged warrant in the first instance executed, tracked, or registered within the CPIC network in relation to the Applicant's identifiers.
Comprehensive Judicial and Executive Orders		Any and all ancillary orders, determinations, statutory authorizations, variances, or judicial directions issued by a Court of competent jurisdiction or a federal board concerning the collection, retrieval, manipulation, or preservation of the Applicant's personal information or physical property.

Date: May 18, 2026



Mr. Kevin A. McLean (BA, JD, CIM)
Applicant (Self-Represented)
68 Abell Street
(Receptionist desk)
Toronto, Ontario
M6J 0B1
Email: mclean@searchandseizure.ca
Fax: 416.352.0055

SOR/2004-283, ss. 35 and 38

ⁱ The RCMP did not conduct a search for records, as required by the Applicant's PII Access Request (March 11 2026), in the manner they executed in the Halton Police 2024 Case;
The RCMP's representation that it conducted a search in CPIC and Specialized Policing Services is fundamentally flawed as the Applicant did not request a search "in" Specialized Policing Services;
The RCMP did not rely upon ss. 16(2) of the *Privacy Act* as it did in the Halton Police Case, thereby defeating any implication of an ongoing investigation or the utilization of sensitive techniques, and the RCMP has waived that protection for the purposes of this judicial review herein;
The RCMP represented in the Halton Police Case that, "The *Privacy Act* has established the right of applicants to access federally maintained records which contain personal information concerning themselves" whereas in the McLean v. RCMP proceeding, it stated, "The *Privacy Act* has established the right of applicants to access federally maintained records" WITHOUT reference to Personal Information, consistent with the

24 exceptions relied upon by the RCMP only referencing “information” and “Personal Information of the Applicant,” leading to a clear jurisdictional path for judicial review on issues outside of the scope of section 29 and 41 of the *Privacy Act*;

The RCMP in the McLean RCMP Proceeding utilized the language of “If this matter concerned another police department, they may have information of interest to you. The *Privacy Act* does not authorize the RCMP to search files or to disclose information belonging to other police forces” whereas in the Halton Police Case the language used by the RCMP was: “if you were involved with another police department or service, they may have information that concerns you. The *Privacy Act* does not authorize the RCMP to search files or to disclose information belonging to other police forces”. The factual inference is that the RCMP only referred to another “department” which be of itself and the RCMP does not have a legal justification under an Act of Parliament to refuse to search the Foundational Metadata and Offline Historical Database so requested by the Applicant including PPU 005, when a request is solely constrained to CPIC, because the RCMP Specialized Policing Services were involved, directly or indirectly;

ⁱⁱ i. A further Declaration that the Respondents’ search of the Specialized Policing Services was arbitrary, devoid of an explicit request, and strictly unauthorized in relation to the PII Access Request (March 11 2026);

ii. A further Declaration that the Respondents orchestrated a purported extension of time on March 17, 2026, so communicated to the Applicant, because after querying the Applicant’s initial identifiers the system did not trigger a police file tied to the TPS but rather triggered a hit tied to a program or database managed under the national SPS umbrella, housing elite federal units—such as Covert Operations, Cyber, and Regional Communications (implicating managers like Regional Commander Mr. Matt Peggs (see: “C” “L” and “(M)” in the False Information Package);

iii. A further Declaration that the RCMP’s Specialized Policing Services is the precise department that owns, manages, and builds the RCMP’s centralized high-tech *infrastructure* including the software development kit of GrapeCity.Documents.PDF that was utilized to manipulate the authentic “Adult Common Information Package” after the inputs were already finalized and then provided to the undisclosed SCJ Judge in the “Ex Parte In Camera Hearing” on or around September 2024;

iv. A further Declaration that the RCMP was inherently responsible for the structural manipulation of the “Adult Common Information Package”;

ⁱⁱⁱ For absolute clarity, said Order includes Personal Information about him in relation to the type of Personal Information that one would be entitled to obtain post-arrest, including any and all Informations and Indictments, arrest warrants, and/or endorsements;

^{iv} The Applicant was not and is not requesting “investigative techniques” and “confidential sources,” but rather an audit trail of a definitively concluded “Intake Court Endorsement” and “judicial authorization”;

^v In accordance with the legal maxims compiled by Herbert Broom, specifically *fraus omnia corrumpit* (fraud vitiates everything) and *ex dolo malo non oritur actio* (no right of action arises from a deceitful wrong), the entirety of the acta executed under such pretenses is irremediably vitiated and rendered *coram non iudice*.

^{vi} And/or by way of Application Record by comprehensive Application and/or by way of singular or multiple affidavits

Tab 2

From: Mr. Kevin A. McLean (BA, JD, CIM)

Email: mclean@searchandseizure.ca

Party: Applicant

Document type: PDF signed request pursuant to Rule 317 of the FCR

Short title: *McLean v. RCMP et al*

Court Level: Federal Court of Canada

Court Office: City of Toronto (180 Queen Street West, Suite 200)

e-document-é		T-2448-26 ID 5	
F	I	FEDERAL COURT	D
L	E	COUR FÉDÉRALE	É
D			P
			O
			S
			É
		May 20, 2026	
		20 mai 2026	
		Diane Lopez	
TOR		2	

COURT FILE NUMBER: T-2448-26

May 19, 2026

**COMPREHENSIVE WRITTEN REQUEST OF THE RCMP (TRIBUNAL)
PURSUANT TO RULE 317 OF THE *FEDERAL COURT RULES*, WHICH IS
TITLED “MATERIAL IN THE POSSESSION OF THE TRIBUNAL” (AS
DEFINED UNDER *FCR*, S. 317 AND *FCA*, S. 2)**

Served on the RCMP in its capacity as a “Tribunal” as defined under *Federal Court Rules*, section 2, where *tribunal* has the same meaning as *federal board, commission or other tribunal* under section 2(1) of the *Federal Courts Act*) on **May 18, 2026**.

Table of Contents

WRITTEN REQUEST OF THE RCMP (TRIBUNAL) PURSUANT TO RULE 317 OF THE <i>FEDERAL COURT RULES</i> , WHICH IS TITLED “MATERIAL IN THE POSSESSION OF THE TRIBUNAL” (AS DEFINED UNDER <i>FCR</i> , S. 317 AND <i>FCA</i> , S. 2)	1
PART 1: statement of rule 317 request and overview of seminal principles under rule 317 to 319 of the <i>FCR</i>	4
Part 1(A): schedule of materials requested from the Applicant to the RCMP (tribunal)	5
Volume #1(C): Rule 317 Jurisprudence: the requirement of certified tribunal record (the “CTR”).....	6
Volume #1(C)(I): Unsearched Repositories; and the RCMP Tribunal (through Mr. Ball) did not rely on any exemption under s. 18	7
Volume #1(C)(II): For sake of completeness: Review of Exempt PIB’s	8
Volume #1(C)(I)(a): Conclusion on the inapplicability of Exempt Banks to the PII Access Request (March 11 2026) and this NOA for Judicial Review	8
Volume #1(D): The Failure to Search by the RCMP	9
VOLUME #1(D)(I): THE LEGAL TEST FOR RELEVANCE	11
VOLUME #1(D)(II): APPLICATION OF <i>DOUZE V. CANADA</i> (CITIZENSHIP AND IMMIGRATION), 2010 FC 1086.....	11
VOLUME #1(E): WHY NOTICES OF APPLICATION FOR MANDAMUS NECESSITATE AN EXPANDED INTERPRETATION OF THE CTR	11

VOLUME #1(F): JUDICIAL REVIEWS ARE DISTINCT FROM APPEALS – RULE 317 EXCLUSIVELY 27 OKED WITHIN APPLICATIONS	12
VOLUME #1(G): THE PRECAUTIONARY PRINCIPLE AND THE RULE OF LAW PRECLUDE SPECULATION	12
VOLUME #1(H): THE DISCOVERY OF IMPROPER MOTIVE FACILITATES MEANINGFUL JUDICIAL REVIEW	12
VOLUME #1(I): THE DIFFERENTIAL LEGAL TEST FOR PROHIBITION UNDER RULE 317	13
Volume #1(H)(ii): Judicial Treatment of Air Passenger Rights	13
VOLUME #1(I): THE IMPERATIVE OF A FORMAL REQUEST	14
VOLUME #1(J): AUTHORITY FOR THE APPLICABILITY OF RULE 317 UNDER AN ATIA REVIEW	14
VOLUME #2: STATEMENT OF ISSUES	14
VOLUME #3: Legal Bases	17
VOLUME #3(A): THE OFFICE OF THE PRIVACY COMMISSIONER DETERMINES THE EXTENT OF THE RCMP’S STATUTORY DUTY AND PARAMOUNTCY OF CONTROL OVER MULTI-JURISDICTIONAL ENTRIES WITHIN THE CANADIAN POLICE INFORMATION CENTRE (THE “CPIC”).....	17
The Genesis of the Disclosed Intelligence:	17
Jurisprudential Analysis and Determinations of the OPCC	18
Analysis of Paragraph 8(2)(f) (Agreements with Foreign States for Law Enforcement):	18
The Finding of the Commissioner.....	18
Analysis of Paragraph 8(2)(a) (The Consistent Use Doctrine):	18
The Intransigence of the RCMP.....	19
Volume #3(A)(I): Summary of Jurisprudential Effect Regarding the Inputting of False or Inaccurate Data into CPIC by any Law Enforcement Apparatus	19
Paramount Stewardship of the Bilateral Agreement	20
The Imperative for Active Policy and Architectural Safeguards	20
Volume #3(B): The Novel Legal Issues Formulated for Adjudication	20
The First Novel and Untested Issue	20
The Second Novel and Untested Issue.....	20
Volume #3(C): The Jurisprudential Doctrine of Possession under the Federal Court Rules	21
The Definition of Possession in the Strict Context of Rule 317	21
The Tripartite Categorization of Possession	21
Volume #3(D): A Comparative Linguistic Analysis of the RCMP’s Decisions (The Halton Police Case vs. The McLean RCMP Proceeding).....	22
Volume #3(D)(I): The RCMP Decision in the Halton Police FIPPA Case	22
Volume #3(D)(II): The Distinctions Possessing Profound Legal Significance.....	23
VOLUME #4: without a search, correction rights cease to exist as legislated by parliament	24
Volume #4(A): Personal Information is akin to one’s ownership	24
Volume #4(B): Constructive and Joint Possession within Decentralized Database Architectures	25
Volume #4(C): The RCMP as the Paramount Custodian and Sovereign Administrative Steward	25
Volume #4(D): The Absolute Nullity of the “Third-Party Ownership” Defense	25

28	Volume #4(E): The Statutory Absurdity and the Frustration of Correction Rights under Subsection 12(2) of the Privacy Act.....	26
	Volume #4(E)(I): The Paramountcy of the Initial Search and the “Meaningful Exercise” of Subsection 12(2)	26
	Volume #4(E)(II): The Competing Interests and the Disclosure of Authorizing Identities (Paragraphs 3(g) and 3(i))	27
	Volume #4(F): The Operational Exclusivity of “Off-Line Searches” and the Reductio ad Absurdum of Delegated Control.....	27
	Volume #4(G): The Jurisprudence of “Control”: The Right of Demand and the Purposive Interpretation of Access Legislation.....	28
	Volume #4(G)(I): The Broad, Liberal, and Purposive Interpretation of Control	28
	Volume #4(G)(II): The Binding Precedent of Hale v. Ontario (Criminal Code Review Board)	28
	Volume #4(G)(III): Application to the Present Factual Matrix: Offline Historical Data and Amended, Purged Records.....	29
	Volume #4(H): The Jurisprudential Significance of the Unsolicited Inquiry into Specialized Policing Services and the Involuntary Institutional Admission of Centralized Systemic Manipulation.....	29
	Volume #4(H)(I): The Inference and the “Data Trigger”	29
	Volume #4(H)(II): The Proverbial “Pandora’s Box” and the MESCIUS / GrapeCity SDK Software Connection	30
	Volume #4(H)(III): The Statutory Validation via the Treasury Board of Canada	30
	Volume #4(H)(IV): The Indispensable Role of Regional Communications as Cross-Jurisdictional Intermediaries and the Implication of Mr. Matt Peggs	30
	Volume #4(H)(V): The Crystallization of the Rule 317 Mandate Regarding Regional Communication Logs.....	31
	Volume #4(H)(VI): The Evidentiary “Smoking Gun” and the Absurdity of the Delegated Deflection	31
	Volume #5: Conclusion	31
	I. The Tactical Avoidance of Paragraph 22(1)(a) and the Unmet Burden under Paragraph 22(1)(b).....	31
	II. The High Threshold of “Injury to the Enforcement of Law” and the Rule of Law	32
	III. The Temporal Ceiling of Investigative Exemptions and the Impact of R. v. Jordan	32
	IV. The Fallacy of Informant Privilege in Relation to Public Court Records and Metadata.....	32
	V. Ultra Vires Conduct, Fraudulent Manipulation, and the Limits of “Lawful Investigations”	33
	VI. The Jurisdictional Legerdemain: Section 19(1)(d) and the Central Region Metamorphosis	33
	VII. The Application of Equitable Maxims: Fraud Upon the Law and the Vitiating of Administrative Acts.....	34
	VIII. The Fiduciary Duty of Disclosure and the Equitable Interest in Personal Information: The Application of McInerney v. MacDonald.....	35
	Appendices	37
	Appendix #1	38
	Appendix #2:	39

PART 1: STATEMENT OF RULE 317 REQUEST AND OVERVIEW OF SEMINAL PRINCIPLES UNDER RULE 317 TO 319 OF THE *FCR*

1. Rule 317 of the *Federal Courts Rules* is titled “**Material from Tribunal**” and it authorizes a party to request material relevant to an “Application” (see: section 2 of the FCR, which means a proceeding referred to in rule 300) that is in the possession of a “Tribunal” (see: section 2 of the FCA and section 2 of the FCR) whose “Order” (see: section 2 of the FCR) is subject of the Application and not in possession of the party by serving on the Tribunal and filing a written request, identifying the material requested.
2. “Material” is not defined under the FCA or FCR, and the Interpretation Act is not of assistance in this regard but based on statutory interpretation principles, “Material” including that which can be reproduced and where it cannot, the original “Materials” to the Registry. The FCC Registry holds that “Original Material” in trust and it is returned to the Tribunal after the Applicant has been heard subject to the Court’s directions. In essence, it is entire collective body of documents, physical items, data, papers, things, records, information, Personal Information et al that are in the possession of the Tribunal.
3. Document discovery in our country varies from province to province and has varied over time with respect to whether the test is “materiality” or “relevance”. The latter is a much broader and lower standard for the threshold as to whether the “materials” must be disclosed to the other party(ies). In the context of an Application to the FCC, a document is relevant to an application for judicial review if it may affect the decision that the Court will make on the application. the relevance of the documents requested must necessarily be determined in relation to the grounds of review set forth in the originating notice and evidence filed by a moving party (see: *infra*, Douze, the Honourable Madam Justice Tremblay-Lamer explicitly adopted the instruction provided by the Court of Appeal in Canada (Human Rights Commission) v. Pathak, 1995 CanLII 3591 (FCA), [1995] 2 F.C. 455, 54 A.C.W.S. (3d) 1344 (C.A.) (Pathak), regarding the parameters of relevance under Rule 317). The reason for the finding as to evidence filed by the Applicant, along with the grounds in the Application, is encompassed by the 20 days after service of the Rule 317 request.
4. “Possession” is not defined under the FCA or FCR, and the Interpretation Act (Federal) does not assist either. This is much like the *Privacy Act*, along with the likes of the provincial privacy protection statutes that do not define the word “control”.
5. “Control” has been interpreted by the FCC and FCA since 1995 to encompass the following wherein Letourneau J.A., writing for the court, held as follows, at p. 245:

“The notion of control referred to in [the Act] is left undefined and unlimited. Parliament did not see fit to distinguish between ultimate and immediate, full and partial, transient and lasting, or “de jure” and “de facto” control. Had Parliament intended to qualify and restrict the notion of control to the power to dispose of the information, as suggested by the appellant, it could certainly have done so by limiting the citizen's right of access only to those documents that the government can dispose of or which are under the lasting or ultimate control of the government.”

(see: *Canada Post Corp. v. Canada (Minister of Public Works)* (1995), 1995 CanLII 3574 (FCA), 30 Admin. L.R. (2d) 242, [1995] 2 F.C. 110, cited with approval by the ONCA *Ontario Criminal Code Review Board v. Hale*, 1999 CanLII 3805 (ON CA)).

6. In Ontario Criminal Review Board, the tribunal therein was found to have control of backup audio tapes created by an independent contractor as the tribunal itself had the power to make a demand for those tapes. It was irrelevant whether they existed or not or what state they were in. The lack of a contractual provision compelling the court reporter to deliver the tapes does not negate the Board's control over them (para 35).
7. However, are “control” and “possession” ‘one and the same’? That question need not be answered herein.
8. Nonetheless, the types of possession include all the various types of possession including:
 - a. De facto;

- b. De jure;
 - c. Actual;
 - d. Constructive;
 - e. Sole;
 - f. Joint; and
 - g. Others (denoted *infra*).
9. As the Respondent RCMP Tribunal is required to transmit all material (which may not be Personal Information of the Applicant) to the FCC that is in its possession whose “Orders” (which include decisions or dispositions by the Tribunal) and that is not in the possession of the Applicant, the issue of whether the Respondent RCMP Tribunal has control of requested Personal Information becomes somewhat moot. Nonetheless, the RCMP’s constructive possession is unique herein because it is the custodian, controller and operator of the CPIC architecture so it has constructive possession, at the very least, of materials therein that are relevant to this JR Application before the FCC.
10. While certain decisions have and continue to focus on what was before or available to the Tribunal at the time of the decision, the scope of disclosure broadens significantly when an applicant has sought writs of mandamus, writs of prohibition and alleged conflicts of interest and bias (individual and institutional) et al (see: *infra* for the authorities in this regard).

PART 1(A): SCHEDULE OF MATERIALS REQUESTED FROM THE APPLICANT TO THE RCMP (TRIBUNAL)

11. With that segue, the Applicant is and has requested, upon service of this written request pursuant to Rule 317 of the Federal Courts Rules, SOR/98-106, Part -1 (the “*Federal Courts Rules*” or the “*FCR*”), materials, particularized *infra*, in possession of the RCMP tribunal (the “Tribunal”). The schedule of material sought herein is as follows:

SCHEDULE OF REQUESTED MATERIALS

Item Number	Category of Material	Specific Records and Metadata Requested
1	Access Request Administrative Files	The complete internal administrative file, tracking sheets, and analyst worksheets concerning <i>Privacy Act</i> file P-2025-16999 .
2	System Initialization Logs	The complete, unredacted system entry logs from the automated sequential registry system detailing the exact date, millisecond timestamp, and file initialization sequence that generated the prefix year “ 2025 ” for an access request delivered to the Respondent on March 11, 2026.
3	Executive and Inter-Directorate Communications	All electronic communications, emails, instant messages, memorandum chains, and briefing notes concerning the Applicant or file P-2025-16999 exchanged between Director Jeff Ball, Delegate Melissa Simpson, Director General Stéphane Brisson, Regional Commander Matt Peggs, or their authorized agents, and Chief of Staff Tanya Mirsky spanning April 1, 2026, to the present.
4	Internal Legal and Operational Advice	All legal or operational advice solicited or received internally regarding the Applicant’s statutory demand for access to the Canadian Police Information Centre (“ CPIC ”) Offline Historical Database metadata, including the Foundational Metadata Request and the Offline Historical Database Request.
5	Raw Forensic Mainframe Ledger Records	The raw, unredacted transaction logs, audit trails, and hexadecimal dumps residing within the secure CPIC Offline Historical Database associated with Personal Information Bank RCMP PPU 005 tied to the Applicant’s name, identifiers, or cross-referenced occurrence numbers (2024-2028093, 24-2082035, and Court File/Case ID 457197) spanning September 15, 2024, to December 31, 2024, inclusive.
6	Cryptographic Audit Trails	The complete cryptographic audit trails capturing all ADD , MODIFY , CLEAR , and CANCEL command strings, along with terminal identifiers, physical hardware addresses, Originating Agency Identifiers (“ ORIs ”), and unstructured narrative fields for each sequential transaction executed during the aforementioned temporal window.

	Forensic Metadata of Search Methodology	The complete electronic system logs generated by Operator NBOISVERT on April 14, 2026, at 07:35:43, detailing the complete input syntax, query parameters, and system constraints utilized to execute the front-facing “Q PERS+” and “Q CNP” live database queries.
8	Internal Directives and Exclusion Policies	Any internal directives, policy documents, or operational notes instructing the Access to Information and Privacy (“ATIP”) Branch analysts to omit an interrogation of the Offline Historical Database in response to the Applicant’s explicit, specialized request for historical data.
9	Trans-Directorate Processing Records	The complete, unredacted administrative processing file, tracking timelines, and internal analyst notes concerning the concurrent <i>Access to Information Act</i> (“ATIA”) request submitted by the Applicant, explicitly targeting the procurement, enterprise licensing, and National Technology Onboarding Program (“NTOP”) integration logs of the Mescius SDK / GrapeCity.Documents.PDF.6.0.2.0 developer engines within the CPIC infrastructure.
10	Automated File Linking Records	All internal processing records showing any administrative coordination, automated file linking, or database cross-referencing executed between the privacy division handling <i>Privacy Act</i> request P-2025-16999 and the information access branch processing the parallel ATIA files.
11	Software Exception Logs	Any software error tracking logs, system exception reports, or developer audit alerts generated by the core CPIC mainframe database management system involving database inquiries or structural PDF modifications tied to the Applicant’s biographical identifiers or transaction history.
12	Executive Suite Briefing Notes and Action Logs	All briefing notes, corporate risk assessments, institutional action logs, and communications generated by or sent to Commissioner Michael Duheme and Director General Stéphane Brisson regarding the Applicant’s personal information or file P-2025-16999.
13	Central Region Command Communications	All emails, letters, instant messages, and administrative directives sent or received by Assistant Commissioner Matthew Peggs (Central Region Command) concerning Police Case ID: 457197, the “Adult Common Information Package,” or the collection and retention of the Applicant’s property from September 15, 2024, to the present.
14	Third-Party Data Transfer Ingestion Ledgers	All cross-jurisdictional system logs showing the electronic receipt, intake vetting, and cryptographic mapping of data transferred from the Toronto Police Service (TPS) or Ontario Court of Justice (OCJ) to the RCMP infrastructure involving the Applicant’s biographical profiles.
15	Primary Statutory Charging Instruments	A certified copy of the Criminal Code Form 2 “Information” and/or Criminal Code Form 4 “Indictment” purportedly generated, indexed, or uploaded into federal tracking streams regarding the Applicant’s underlying file.
16	Core Courthouse Intake Endorsements	A certified copy of the Intake Court Endorsement represented on Page 3 of 5 within the disputed “False Information Package,” capturing any handwriting, initials, or automated metadata strings applied during processing.
17	Originating Judicial Authorizations	A certified copy of the alleged warrant in the first instance executed, tracked, or registered within the CPIC network in relation to the Applicant’s identifiers.
18	Comprehensive Judicial and Executive Orders	Any and all ancillary orders, determinations, statutory authorizations, variances, or judicial directions issued by a Court of competent jurisdiction or a federal board concerning the collection, retrieval, manipulation, or preservation of the Applicant’s personal information or physical property.

VOLUME #1(C): RULE 317 JURISPRUDENCE: THE REQUIREMENT OF CERTIFIED TRIBUNAL RECORD (THE “CTR”)

12. Consistent with settled jurisprudence regarding the open court principle (the “**Open Court Principle**”) entrenched within section 2(b) of the *Canadian Charter of Rights and Freedoms* (the “**Charter**”), informations and indictments (the “**Informations**” and “**Indictments**”) are unequivocally treated as public court documents upon the issuance of a process and/or the service of a Criminal Code Summons or the execution of a Criminal Code Form 7 Arrest Warrant. Furthermore, any corresponding endorsements by a judicial officer (“**Endorsements**”) thereto are to be made available upon formal request by an accused party (devoid of prescribed fees) or the public writ large, subject to the prescribed fee schedule delineated within *Regulation 158/03*.
13. Analogously, within the taxation context, it has been established that the Canada Revenue Agency, pursuant to a request under *Rule 317* of the *FCR*, forwarded a certified copy of an information (the “**Information**”) to the

- 32 Registry. Said document was subsequently treated by the Registry as a public document, with a copy concurrently remitted to the applicant's counsel: *Rémillard v. Canada (National Revenue)*, 2020 FC 1061 at para 5.
14. Documentation transmitted pursuant to *Rule 318* of the *FCR* is strictly incorporated into the receiving Court's official records and is governed *ipso facto* by the **Open Court Principle** (see: *Rémillard*, at paras 25–26 and 37–38). Sections 23 and 26 of the *FCR* mandate that the Court file and its annexes be treated as publicly accessible, subject exclusively to statutory confidentiality or specific judicial sealing orders.
 15. The procedural mechanism outlined in *Rules 317* and *318* of the *FCR* is strictly operational and non-exploratory; its function is solely to transition relevant materials into the possession of the Registry, distinguishable from private discoveries which are executed beyond the purview of the Court file (see: *Rémillard*, at paras 57–59 and 65–66). Private discoveries are governed by the implied undertaking rule subject to questions from discovery being read into the court record by affidavit or at a hearing.
 16. Should the **Respondent RCMP Tribunal** argue that the applicant is utilizing *Rule 317* as an impermissible exploratory discovery mechanism, such an assertion is preemptively defeated by the fact that the requested records constitute foundational administrative documents that inherently form the basis of the tribunal's jurisdiction and subsequent (or omitted) actions.
 17. The protections afforded under section 8 of the *Charter* are rendered inapplicable *in limine*, as no reasonable expectation of privacy ("REOP") can legally persist subsequent to an applicant requisitioning transmission pursuant to *Rule 317* of the *FCR* (see: *Rémillard*, at paras 163–165).
 18. Generally, *Rule 317* of the *FCR* encompasses exclusively the material that was available to the administrative decision-maker at the time the decision was rendered (at paras 23, 39, and 41–42). However, a substantially broader scope of disclosure is mandated in circumstances where procedural fairness, reasonable apprehension of bias, or analogous equitable grounds are explicitly contained within the Notice of Application and supported by a cogent evidentiary foundation: *Lill v. Canada*, 2023 FC 1364. Such grounds are unequivocally established herein by the notice of application (the "**JR NOA**") filed by the applicant (the "**Applicant**").

Volume #1(C)(I): Unsearched Repositories; and the RCMP Tribunal (through Mr. Ball) did not rely on any exemption under s. 18

19. The circumstances present herein ostensibly construct a paradox; however, a rigorous legal examination reveals that such a paradox is illusory, even if it is averred that the Royal Canadian Mounted Police (the "**RCMP**") neglected to search the requisite repositories for foundational metadata (the "**Foundational Metadata**") and the offline historical database (the "**Offline Historical Database**") (collectively, the "**Unsearched Repositories**"). The jurisprudential test dictates that the determination rests upon what material was legally available to the decision-maker at the material time.

Volume #1(C)(I)(a): The Misstatement of Law in the RCMP Tribunal Decision: "Privacy Act does not authorize search of files...belonging to other police forces"

20. The failure of the RCMP, as admitted predicated upon its representation in the April 27, 2026, letter communicated to the Applicant that the "The *Privacy Act* does not authorize the RCMP to search files....belonging to other police forces" (see: page 1 of 6, paragraph three).
21. "Files" is not defined under the *Privacy Act* but it is mentioned six (6) times under the *Privacy Act* which are:
 - a. EXEMPTIONS
 - i. Exempt Banks
 1. Governor in Council may designate exempt banks
 - a. Subsection 18(1): The Governor in Council may, by order, designate as exempt banks certain personal information banks that contain **files** all of which consist predominantly of personal information described in section 21 or 22.
 2. Contents of order
 - a. Clause 18(3)(b): (3) An order made under subsection (1) shall specify

- i. (b) where a personal information bank is designated that contains files that consist predominantly of personal information described in subparagraph 22(1)(a)(ii), the law concerned.
- b. The auto population of “files” (three to six) involve the review of exempt banks by the Privacy Commissioner of Canada into those exempt banks.

Volume #1(C)(I)(a)(i): Conclusion on the misstatement of law in this context

22. The Respondent RCMP did NOT claim an exemption under section 18(2) of the *Privacy Act* which states for sake of convenience:

“Disclosure may be refused

(2) The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that is contained in a personal information bank designated as an exempt bank under subsection (1).”

23. The Head of the Government Institution is that of Commissioner Mr. Michael Duheme.

Volume #1(C)(II): For sake of completeness: Review of Exempt PIB's

24. Nonetheless, the exempt PIB's are:

a. Department of National Defence Exempt Bank:

- i. Exempt Personal Information Bank Order, No. 5 (ND), SOR/85-38, Part -1: The personal information bank under the control of the Department of National Defence containing the Security and Intelligence Information files No. ND-P70 is hereby designated as an exempt bank on the basis of section 21 of the *Privacy Act*;

b. Criminal Operational Intelligence Records (tied to Personal Information contained at subparagraph 22(1)(a)(ii))

- i. Exempt Personal Information Bank Order, No. 13 (RCMP), SOR/90-149, Part -1: Criminal Operational Intelligence Records, No. CMP/P-PU-015, a personal information bank under the control of the Royal Canadian Mounted Police, is hereby designated as an exempt bank on the basis of section 22 of the *Privacy Act*.
 - 1. or the purposes of paragraph 18(3)(b) of the *Privacy Act*, the laws concerned, in relation to those files that are contained in the exempt bank referred to in section 2 that consist predominantly of personal information described in subparagraph 22(1)(a)(ii) of that Act, are the Criminal Code, the Customs Act, the Excise Act, the Food and Drugs Act, the Immigration and Refugee Protection Act, the Income Tax Act, the Controlled Drugs and Substances Act and the Foreign Interference and Security of Information Act.

c. CSIS Exempt Bank:

- i. Exempt Personal Information Bank Order, No. 14 (CSIS), SOR/92-688, Part -1

d. Exempt Personal Information Bank Order, No. 25 (RCMP), SOR/93-272, Part -1,

- i. For the purposes of paragraph 18(3)(b) of the *Privacy Act*, the laws concerned, in relation to those files that are contained in the exempt bank referred to in section 2 that consist predominantly of personal information described in subparagraph 22(1)(a)(ii) of that Act, are the Criminal Code, the Foreign Interference and Security of Information Act, the Security Offences Act, the Royal Canadian Mounted Police Act and the Canadian Security Intelligence Service Act.

Volume #1(C)(I)(a): Conclusion on the inapplicability of Exempt Banks to the PII Access Request (March 11 2026) and this NOA for Judicial Review

34 25. Leaving aside that the RCMP solely focused on “information” and not “Personal Information”, it explicitly relied in its decision on April 27, 2026, wherein it stated:

“Enclosed is a copy of all of the information to which you are entitled. Please note that some of the information has been exempted pursuant to sections 19(1)(d), 22(1)(b) and 26 of the Act”

26. There is not a single solitary mention of section 18 therein. Ergo, the RCMP Tribunal was not relying on “files contained in a PIB being exempt from disclosure let alone searching.
27. For completeness purposes and to avoid unnecessary and frivolous objections by the RCMP regarding its obligation to transmit a complete, accurate, and full CTR to the FCC and the Applicant, there is also not a single mention of n subparagraph 22(1)(a)(ii). Ergo, any reliance by the RCMP Tribunal on not being able to search files or disclose information (sic) belonging to other police forces is not relevant herein.
28. Hence, the Applicant’s judicial review Notice of Application (Form 301) seeking writs of mandamus and prohibition as the relevant Personal Information sought, of which the Applicant did not seek that which was produced in the three page heavily redacted document accompanying the April 27 decision, has not been searched for.
29. Irrespective of the same, there would remain a judicial review independent of that aforementioned mandamus issue, predicated on the requirement (statutory and common law) for the Head of the Government Institution to consider whether to make a public interest disclosure regarding the manipulation of a “Criminal Code Information Package” into a False Information Package which is unprecedented in Canadian legal history (see: R. v. Scherzer and R. v. Hamilton did not contained falsification of the Criminal Code Information Packages but the falsification of underlying legal bases and notes per se; and R. v. Silva (Quebec) involved the stealing of a Justice of the Peace’s stamp on account of “noble cause corruption” by a young Police Officer in Mr. Jolly as the public was in a state of terror with a notorious gang connected hitman in Mr. Silva).

VOLUME #1(D): THE FAILURE TO SEARCH BY THE RCMP

30. In light of the above uncontroverted syllogism and the sophisms by the RCMP, the *Privacy Act* not only authorizes but obligates the Government Institution to search for Personal Information requested (not “files”) within the scope of an access request whether it is in a Personal Information Bank (a “PIB”) and has been used, is being used or is available for use for an administrative purpose or is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual (see: section 10 of the *Privacy Act*).
31. However, the word “files” is utilized under some of the attendant regulations under the *Privacy Act* where certain PIB’s, pursuant to ss. 18(1) of the *Privacy Act*, making certain PIB’s exempt from search and disclosure.
32. The Applicant requested access to the PIB known as PPU 005 and it is not an exempt PIB. Moreover, the PII Access Request (March 11 2026) was not a request for “files” per se but for Personal Information contained in the PIB (PPU 005) and searches of Foundational Metadata and Offline Historical Database with respect to an executed arrest warrant including any original and amended data therein contained his Personal Information. But for the name of the judicial officer who in fact issued an endorsement including an Arrest Warrant (Criminal Code Form 7) all of the Personal Information therein would be on its face and de facto only involving him per se. In relation to the name of the judicial officer who issued the endorsement (dubbed an “Intake Court Endorsement”) “warrant in the first”, the federal statutory Personal Information definition under section 3(i) (see: means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing...(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual). This is also consistent with the judicial interpretation of Personal Information, and the required interpretation as follows:
 - a. Drawing from jurisprudence in the federal public sector, the definition of personal information must be given a broad and expansive interpretation (Dagg v. Canada (Minister of Finance), [1997] 2 S.C.R., dissenting, 403 at para 68; Canada (Information Commissioner) v. Canada (Transportation Accident

Investigation and Safety Board), 2006 FCA 157; Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police), [2003] 1 S.C.R. 66, 2003 SCC 8, at para 23).

- b. Personal information is information “about” an identifiable individual. “About” means that the information is not just the subject of something but also relates to or concerns the subject (Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157).
- c. Information will be about an “identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information (Gordon v. Canada (Health), 2008 FC 258 (CanLII)).Footnote1 Information need not be recorded for it to constitute personal information. It is sufficient that the information be about an identifiable individual even if the information is not in a recorded form, such as oral conversations, biological samples and real time video surveillance. While the absence of a recording may go to the issue of collection, it does not change the fact that the information is personal information (Morgan v. Alta Flights Inc. (2006) FCA 121, affirming (2005) FC 421).
- d. The same information can be personal to more than one individual, where, for example, it contains the views of one individual about another individual, or where the same information reveals something about two identifiable individuals (Wyndowe v. Rousseau, 2008 FCA 39 (CanLII)).
- e. Information will still be personal information even if it is publicly available within the meaning of the regulations,Footnote2 and is exempt from applicable consent requirements (Englander v. TELUS Communications Inc., 2004 FCA 387 (CanLII)).
- f. Subjective information about an individual may still be personal information even if it is not necessarily accurate (Lawson v. Accusearch Inc. 2007 FC 125).

33. The general principles overall are:

- a. Privacy Rights’ Purpose:
 - i. privacy rights are designed to protect the privacy of individuals with respect to Personal Information held by government institutions and to provide individuals with a right of access to that information;
- b. *Privacy Act*:
 - i. quasi-constitutional;
- c. Exceptions from an individual applicant’s access rights – interpreted narrowly:
 - i. in Lavigne v. Canada (Office of the COMMISSIONER of Official Languages), 2002 SCC 53 (CanLII), [2002] 2 S.C.R. 773, Gonthier J. observed that exceptions from the rights set out in the act should be interpreted narrowly, with any doubt resolved in favour of preserving the right;
- d. Burden of proof:
 - i. the burden of persuasion on the person asserting the exception (at paras. 30-31 of Lavigne);
- e. Privacy Rights only compromised when there is a compelling state interest for doing so:
 - i. in Dagg v. Canada (Minister of Finance), 1997 CanLII 358 (SCC), [1997] 2 S.C.R. 403, the SCC articulated the governing principles of privacy law including that protection of privacy is a fundamental value in modern democracies and is enshrined in ss. 7 and 8 of the Charter, and privacy rights are to be compromised only where there is a compelling state interest for doing so (at paras. 65, 66, 71)

34. It is axiomatic that the RCMP is also subject to the Charter pursuant to section 32 of the Charter.

35. *Lex non cogit ad impossibilia* (the law does not compel the impossible) cannot shield the RCMP where the material was, in fact, extant and obtainable.

36. Inasmuch as Informations, Indictments, and any associated endorsements—including but not limited to arrest warrants—are fundamental components governed by the Open Court Principle (which concurrently protects the rights of listeners pursuant to section 2(b) of the *Charter*), the failure of an originating courthouse or originating court office to produce said documents is immaterial. The RCMP possesses the requisite statutory authority to procure such documentation and is legally obligated to do so pursuant to *Rule 317*. From a policy perspective, the Federal Court of Canada and the RCMP are absolutely bound to discharge this requirement to preserve the integrity

of the rule of law (the “**Rule of Law**”). Invoking Herbert Broome’s maxim, *omnia praesumuntur rite et solemniter esse acta* (all acts are presumed to have been done rightly and regularly), the public is entitled to presume the RCMP will fulfill its legal duties to procure necessary records.

37. Copies of the aforementioned Informations, Indictments, and corresponding endorsements, alongside copies of arrest warrants—as represented by the Toronto Police Service (the “**TPS**” or the “**Arresting Police Division**”) to have been in their possession—are strictly relevant to the JR NOA, specifically concerning the prerogative relief sought in the nature of mandamus and prohibition.
38. Furthermore, the compulsory transmission of these documents will categorically elucidate whether the RCMP was operating *mala fides* by intentionally breaching a public legal duty, or, in the alternative, operating negligently by breaching a public legal duty in a profoundly derelict manner. This evidentiary disclosure is paramount as it directly dictates the quantum and nature of the consequential relief to be awarded.

VOLUME #1(D)(I): THE LEGAL TEST FOR RELEVANCE

39. For the strict purposes of *Rule 317* of the *FCR*, a document is deemed relevant to an application for judicial review if it possesses the capacity to affect the ultimate decision that the Court will render on the application (see: *Douze v. Canada (Citizenship and Immigration)*, 2010 FC 1086 at para 19); *Boudreau v. Canada (Revenue Agency)*, 2022 FC 792 (CanLII), at para 16.

VOLUME #1(D)(II): APPLICATION OF DOUZE V. CANADA (CITIZENSHIP AND IMMIGRATION), 2010 FC 1086

40. In *Douze*, the Honourable Madam Justice Tremblay-Lamer explicitly adopted the instruction provided by the Court of Appeal in *Canada (Human Rights Commission) v. Pathak*, 1995 CanLII 3591 (FCA), [1995] 2 F.C. 455, 54 A.C.W.S. (3d) 1344 (C.A.) (*Pathak*), regarding the parameters of relevance under *Rule 317*:

“A document is relevant to an application for judicial review if it may affect the decision that the Court will make on the application. As the decision of the Court will deal only with the grounds of review invoked by the **Respondent**, the relevance of the documents requested must necessarily be determined in relation to the grounds of review set forth in the originating notice of motion and the affidavit filed by the **Respondent**. (at para. 10)”

41. The ratio decidendi established in *Douze* has been consistently affirmed across numerous subsequent decisions, including:
 - a. *Chopra v. Canada (Public Safety and Emergency Preparedness)*, 2026 CanLII 18896 (FC), at para 10;
 - b. *John Doe I v. Canada (Attorney General)*, 2024 FC 1024, wherein Mr. Justice Diner articulated:
 - i. It is well established that the test for relevance under *Rule 17* is synonymous with that under *Rule 317* of the *FCR* (*Abu* at paras 28 and 43, citing *Douze v. Canada (Citizenship and Immigration)*, 2010 FC 1086 at para 19 and *Nguesso v. Canada (Citizenship and Immigration)*, 2015 FC 102 at para 94). Ergo, a document is classified as “relevant” in this specific context where it “may affect the decision that the Court will make on the application,” determined strictly in relation to “the grounds of review and any affidavit filed in support of the application” (*Abu* at para 43).
 - c. The relevance of the material requisitioned under *Rule 317* of the *FCR* is the determinative factor. For the purposes of *Rule 317*, a document is relevant to an application for judicial review if it may affect the decision that the Court will ultimately make on the application (see: *Douze v. Canada (Citizenship and Immigration)*, 2010 FC 1086 at para 19; *Boudreau v. Canada (Revenue Agency)*, 2022 FC 792 (CanLII), at para 16; and
 - d. Various other binding appellate and trial-level jurisprudence.

VOLUME #1(E): WHY NOTICES OF APPLICATION FOR MANDAMUS NECESSITATE AN EXPANDED INTERPRETATION OF THE CTR

42. In *Abu v. Canada (Citizenship and Immigration)*, 2021 FC 1031, Mr. Justice Norris articulated the distinguished threshold for mandamus applications as follows:
43. “I begin by noting that one of the usual indicators of relevance in the judicial review context—was the document or information before the tribunal when it made its decision?—does not apply in a mandamus application because it is the failure or refusal of the tribunal to make a decision that has prompted the application in the first place. While this is a sound indicator of relevance when a decision is being reviewed, it is not exhaustive of the concept of relevance in the judicial review context generally. It is well established that the test for relevance in the context of the production of a CTR is whether a document in the possession or control of the tribunal in question “may affect the decision that the Court will make on the application” (*Canada (Human Rights Commission) v. Pathak*, 1995 CanLII 3591 (FCA), [1995] 2 F.C. 455 [at page 460], 1995 CarswellNat 666, at paragraph 10 (WL Can.) (C.A.)).

VOLUME #1(F): JUDICIAL REVIEWS ARE DISTINCT FROM APPEALS – RULE 317 EXCLUSIVELY INVOKED WITHIN APPLICATIONS

44. Mirroring the explicit statutory language of the *FCR*, *Beniey v. Canada (Border Services Agency)*, 2024 FC 972 unequivocally affirmed that *Rule 317* applies exclusively to judicial reviews conducted pursuant to the *Federal Courts Act* (the “**FCA**”) and is inapplicable to applications instituted under separate statutory regimes, such as the *Official Languages Act*, RSC 1985, c 31 (4th supp) (the “**OLA**”). This principle was previously crystallized in *Lavigne v. Canada Post Corporation*, 2009 FC 756, wherein it was determined at paragraph 16 that *Rule 317* cannot be invoked against the Commissioner within an application commenced under section 77 of the *OLA*, as the Commissioner’s decision is not formally under review.
45. By logical extrapolation, applications commenced pursuant to section 41 of the *Privacy Act* or under the *Access to Information Act* (the “**ATIA**”) do not constitute judicial reviews under the *FCA* and therefore do not govern the specific issues herein, wherein a tribunal (the “**RCMP Tribunal**”) has explicitly conceded a failure to search delineated repositories.

VOLUME #1(G): THE PRECAUTIONARY PRINCIPLE AND THE RULE OF LAW PRECLUDE SPECULATION

46. As explicated by the Federal Court of Appeal in *Canadian Copyright Licensing Agency (Access Copyright) v. Alberta*, 2015 FCA 268 [*Access Copyright*] (per Stratas JA at para 15):

“Parties before the administrative decision maker will often have in their possession all of the material the administrative decision maker considered in making its decision. But not always. And sometimes parties may be unsure whether they do. Sometimes they wish to confirm exactly what the administrative decision maker actually considered in making its decision. Rule 317 of the Federal Courts Rules provides a means by which parties can achieve those ends

(see also: *Friends of the Earth Canada v. Canada (Attorney General)*, 2023 FC 1438 (CanLII), at para 9).

47. Herein, the Applicant less than little: he has nothing.

VOLUME #1(H): THE DISCOVERY OF IMPROPER MOTIVE FACILITATES MEANINGFUL JUDICIAL REVIEW

48. It is an accepted legal tenet that the certified record and its surrounding context may unveil whether an administrative decision was predicated upon an improper motive or driven by alternative impermissible rationales (*Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65 at para 137).

38 49. In the event that the reviewing court is deprived of the evidentiary foundation relied upon by the administrative decision-maker, the detection of a reviewable error may be rendered an impossibility (*Access Copyright* at para 14). The paramount and overarching consideration is whether the requested disclosure will permit a meaningful and substantive judicial review of the impugned decision (*GCT Canada Limited Partnership v. Vancouver Fraser Port Authority*, 2021 FC 624 at para 26).

VOLUME #1(I): THE DIFFERENTIAL LEGAL TEST FOR PROHIBITION UNDER RULE 317

50. In *Air Passenger Rights v. Canada (Attorney General)*, 2021 FCA 201, Associate Justice Gleason of the Federal Court of Appeal delineated at paragraph 21:

“[21] Turning to the first of the foregoing assertions, as the applicant rightly notes, the breadth of materials that are subject to disclosure under Rules 317 and 318 of the Federal Courts Rules is broader where bias or breach of procedural fairness is alleged, particularly where, as here, relief in the nature of prohibition is sought. In such circumstances, disclosure is not limited to the materials that were before the tribunal when an order was made. Rather, where such arguments are raised, documents in the possession, control or power of a tribunal that are relevant to the allegations of bias or breach of procedural fairness are subject to disclosure.

51. Indeed, were it otherwise, this Court would be deprived of evidence necessary for the disposition of an applicant’s claims of bias or breach of procedural fairness and the availability of relief in the nature of prohibition would be largely illusory: see, e.g., *Humane Society of Canada Foundation v. Canada (National Revenue)*, 2018 FCA 66, 289 A.C.W.S. (3d) 875 at paras. 5-6; *Gagliano v. Canada (Commission of Inquiry into the Sponsorship Program & Advertising Activities)*, 2006 FC 720, 293 F.T.R. 108 at para. 50, aff’d 2007 FCA 131; *Majeed v. Canada (Minister of Employment & Immigration)*, 1997 CarswellNat 1693, [1993] F.C.J. No. 908 (F.C.T.D.) at para. 3, aff’d [1994] F.C.J. No. 1401 (F.C.A.). Thus, the first assertion advanced by the AGC as to the scope of permitted disclosure under Rules 317 and 318 is without merit.”
52. Allegations encompassing bias and profound breaches of procedural fairness have been meticulously pleaded and are comprehensively encapsulated within the operative iteration of the application record (the “**Application Record**”).
53. Concurrently, prerogative relief in the form of a writ of prohibition (the “**Writ of Prohibition**”) is actively sought by the Applicant. Herbert Broom’s maxim *ubi jus ibi remedium* (where there is a right, there is a remedy) dictates that the Court must possess the requisite evidentiary record to formulate such a remedy.
54. *Ipso facto*, given that the remedies of mandamus and prohibition are concurrently pursued, the restrictive test evaluating solely the materials available at the precise moment of the RCMP Tribunal’s decision is fundamentally inapplicable. While the Applicant submits that this narrower threshold would nonetheless be satisfied, the prevailing appellate jurisprudence unequivocally binds the Court, by virtue of vertical *stare decisis*, to compel the RCMP Tribunal to transmit the expansive array of materials in certified format to both the Federal Court and the Applicant.
55. Should it be argued that the broader array of documents falls outside the technical “control” of the decision-maker because they were not explicitly reviewed, such an argument constitutes a logical fallacy. The jurisprudence explicitly overrides this limitation where bad faith, bias, or procedural fairness are pleaded, transferring the metric of discoverability from “what was reviewed” to “what may affect the Court’s disposition of the fairness allegations.”

Volume #1(H)(ii): Judicial Treatment of Air Passenger Rights

56. When allegations of bias or breaches of procedural fairness are advanced within a notice of application, the legally permissible scope of materials subject to mandatory disclosure under *Rules 317 and 318* is substantially broadened. This augmented scope is a jurisprudential imperative designed to guarantee that the reviewing Court is vested with the requisite evidentiary matrix to judiciously dispose of these claims (*Air Passenger Rights v. Canada (Attorney*

General), 2021 FCA 201 at para 21). Consequently, where bias or a breach of procedural fairness is averred, all documentation possessing relevance to such allegations must be subject to compulsory disclosure (*Ron W Cameron Charitable Foundation v. Canada (National Revenue)*, 2023 FCA 175 [Ron W Cameron] at para 26); *Delisle (Kannabis Shop) v. Kahnawake Cannabis Control Board*, 2026 CanLII 14519 (FC), at para 13.

57. In circumstances where an allegation of a breach of procedural fairness, a reasonable apprehension of bias, or actual bias is asserted within a notice of application or notice of appeal, the orthodox convention restricting production to relevant material physically before the decision-maker is invariably expanded. Supplemental documents demonstrating relevance to the specific allegation become subject to production: *Humane Society of Canada Foundation v. Canada (National Revenue)*, 2018 FCA 66 at para 6 (*Humane Society*); *Air Passenger Rights v. Canada (Attorney General)*, 2021 FCA 201 at para 21 (*Air Passenger Rights 2021*). The Federal Court of Appeal definitively codified this expanded obligation in *Air Passenger Rights 2021* (see: paragraph 21); *Jewish National Fund of Canada Inc. v. Canada (National Revenue)*, 2025 FCA 114 (CanLII), at para 13.
58. Furthermore, averments detailing discrimination on the basis of disability or egregious breaches of procedural fairness serve as sufficient independent catalysts to warrant expanded disclosure pursuant to *Rule 317*. When such arguments are substantively raised, documents demonstrating relevance to the allegations—irrespective of whether they were physically reviewed by the decision-maker—are strictly subject to disclosure (*Air Passenger Rights v. Canada (Attorney General)*, 2021 FCA 201 at para 21); *Ron W. Cameron Charitable Foundation v. Canada (National Revenue)*, 2023 FCA 175 (CanLII), at para 26. Application of this law dictates that the Applicant’s pleadings of specific biases mandate production of the entire foundational record to assess the veracity of the tribunal’s omissions.

VOLUME #1(I): THE IMPERATIVE OF A FORMAL REQUEST

59. In *Wheeldon v. Canada (Attorney General)*, 2012 FC 355, Mr. Justice Phelan articulated the absolute necessity of tendering a formal written request, notwithstanding the absence of a strictly prescribed statutory form. The Court observed the fatal deficiency when an applicant sought supplementary information without formalizing the requisite demand pursuant to *Rule 317* of the *FCR*. Specifically, the **Respondent** formally notified the Court that it refrained from producing the entirety of the material pertaining to the impugned decision strictly because the procedural formality of *Rule 317* was not strictly adhered to by the applicant: *Wheeldon v. Canada (Attorney General)*, 2012 FC 355 (CanLII), at para 15.

VOLUME #1(J): AUTHORITY FOR THE APPLICABILITY OF RULE 317 UNDER AN ATIA REVIEW

60. The standard of correctness is universally applicable in determining the applicability of *Rule 317* to a section 44 review under the *ATIA*, as such an inquiry constitutes a pure question of law (at para 11). A review instituted under section 44 retains the fundamental character of a judicial review, as it invariably scrutinizes the administrative decision-maker’s ultimate determination regarding the disclosure of records (at paras 14–15 and 26). The decision itself embodies “the subject of the application,” thereby satisfying the strict statutory language and threshold requirements encapsulated within *Rule 317* (at para 15): *Preventous Collaborative Health v. Canada (Health)*, 2021 FC 253. By applying this doctrine to the present facts, the failure to produce the required documents transforms the administrative inaction into the direct subject matter of the application, thereby triggering the compulsory production requirements of *Rule 317*.

VOLUME #2: STATEMENT OF ISSUES

61. The issues are provided herein to ensure that this proceeding is determined in a manner that is just, most expeditious and least expensive outcome of every proceeding with consideration being given to the principle of proportionality, including consideration of the proceeding’s complexity, the importance of the issues involved and the amount in

dispute (see: rule 3(a) and (b)) and in the event that there is an objection to some of the material requested the Court has the benefit of the relevant issues:

- a. **Definitional Parameters under the *Privacy Act*:** Predicated upon the assertion that the RCMP purported to exercise jurisdiction and powers pursuant to the *Privacy Act*, RSC 1985, c P-21—an Act of Parliament—what is the proper jurisprudential and statutory interpretation of the following operative terms within the context of the present application: i. “Order”; ii. “Material”; and iii. “Relevant”.
- b. **The Legal Doctrine of Possession:** Given the absence of an explicit statutory definition of “possession” within the *Federal Courts Act*, RSC 1985, c F-7, the *FCR*, or the *Interpretation Act*, RSC 1985, c I-21, what is the prevailing common law and jurisprudential definition of “possession” specifically as it applies to the production of records in applications before the Federal Court of Canada?
- c. **Expanded Scope of Disclosure (*Rules 317 and 318*):** To what extent is the legally permissible scope of mandatory disclosure, compelled under *Rules 317 and 318* of the *FCR*, augmented and expanded in circumstances where an applicant explicitly pleads and seeks relief based upon: i. A Writ of Mandamus; ii. A Writ of Prohibition; iii. The reasonable apprehension of bias, existence of a conflict of interest, institutional lack of independence, and/or lack of impartiality; and/or iv. Egregious breaches of the principles of procedural fairness;
- d. **Subsection 19(1)(d) misguided yet revealing reference:**
 - i. **Principal Issue for Determination:**
 1. Whether the invocation of the statutory exemption enumerated within subsection 19(1)(d) of the *Privacy Act* operates, *sub silentio*, as an admission of the originating law enforcement agency status of the federal constabulary; and furthermore, whether the totality of the circumstances encompassing the disposition of the subject chattels, the internal reorganization of the federal institution, the alleged documentary irregularities, and the anomalous remuneration of court personnel furnishes a triable inference of systemic procedural manipulation or institutional impropriety.
 - ii. **Particularized Sub-Issues:**
 1. a) **Disposition of Chattels and Warrant Protocols:** Whether the ostensibly irregular handling of the subject chattels by the municipal police service—specifically, the uncatalogued sequestration thereof within a provisional repository, compounded by ensuing contradictory representations concerning the purported transfer to the Property Evidence Management Unit, and conjoined with the failure to produce an executory warrant of arrest—furnishes sufficient evidentiary weight to support the inference that the federal constabulary, rather than the municipal entity, operated as the primary or originating agency, thereby providing the foundational rationale for the invocation of subsection 19(1)(d).
 - iii. b) **Institutional Reorganization as Statutory Circumvention:**
 1. Whether the redesignation of the federal constabulary’s “O” Division to the “Central Region,” whilst remaining under the continuous administrative authority of the presiding Regional Commander, is liable to be construed as a deliberate structural realignment executed with the specific intent of satisfying the jurisdictional phrasing contained within subsection 19(1)(d) (“regional government established by... an Institution of such a government”), thereby operating as an artifice to insulate agency records from mandatory disclosure.
 - iv. c) **Inherent Prejudice to the Governmental Institution (understandable yet non-legal justification for non-disclosure):**
 1. Whether, by invoking the aforementioned statutory exemption, it is implicitly conceded by the federal institution that the execution of a comprehensive search would invariably yield specific foundational metadata—comprising the Originating Agency Identifier (ORI),

particulars of the issuing tribunal, and the identity of the presiding judicial officer—which would conclusively establish the agency’s direct involvement, thereby occasioning inherent prejudice to the institution.

- v. d) **Alleged Documentary Alteration and Software Exploitation:**
 - 1. In consideration of the publicly documented technical vulnerabilities inherent to the software framework identified as GrapeCity.Documents.PDF 6.0.2.0, whether a balance of probabilities suggests that said framework was utilized to effectuate a systematic obfuscation or manipulation of the primary evidentiary record, thereby converting the Authentic Information Package into the False Information Package.
- vi. e) **Procedural Irregularities Indicative of Federal Agency Practices:**
 - 1. Whether the particularized errors and omissions identifiable within the False Information Package bear a greater indicia of alignment with the administrative practices of a federal agency operating within a regional framework—an entity arguably lacking the high-volume, routine process-issuing expertise characteristic of municipal police forces—than with those of the municipal police service itself.
- vii. f) **Probative Inferences Regarding Personnel Remuneration:**
 - 1. What juridical inferences may be properly drawn from the sudden and material escalation in the remuneration of the named Court Officer, propelling said individual to a publicly disclosed threshold of elevated compensation in the year 2025, in immediate sequence to the allegedly unauthorized utilization of her identity as an informant—an averment she purportedly could not traverse upon confrontation. Furthermore, whether this temporal pattern of compensation raises a triable issue as to the possibility that such financial advancement was furnished as a clandestine commission or improper inducement to secure acquiescence to the aforementioned inclusion of her identity.
- e. **Subsection 22, “Law Enforcement and Investigation”:** the absence of section 22(1)(a) but the inclusion of 22(1)(b) misguided yet enlightening, illuminating and informative reference:
 - i. The central issues in this application for judicial review concern the Royal Canadian Mounted Police’s (the “RCMP”) unlawful withholding of Foundational Metadata and Offline Historical Database records under the *Privacy Act*, R.S.C. 1985, c. P-21 (the “*Act*”). Specifically, the issues are framed as follows:
 - 1. **The Jurisdictional Misdirection:** Did the RCMP ATIP Branch err in law by declining to invoke the specific exemption under paragraph 22(1)(a) of the *Act*—which would require identifying itself as an “investigative body” under the *Privacy Regulations*—and instead relying on paragraph 22(1)(b), thereby assuming an evidentiary burden of proving “injury” that it cannot legally or factually satisfy?
 - 2. **The Failure to Establish a Reasonable Expectation of Injury:** Can the disclosure of historical, transactional, or administrative metadata (including CPIC logs, Foundational Metadata, and offline database entries) be reasonably expected to cause “injury” to the enforcement of any law or the conduct of lawful investigations under paragraph 22(1)(b), particularly where the underlying investigation is stale, inactive, or structurally concluded?
 - 3. **The Temporal and Procedural Boundaries of “Investigations”:** Can the RCMP assert an ongoing investigative character over CPIC transactions that merely log the completion of past, expired, or time-barred administrative processes (such as a summons or arrest warrant), particularly where any potential prosecution is long-concluded or barred under the constitutional ceilings established in *R. v. Jordan*?
 - 4. **The Mischaracterization of Public Court Records as Confidential Sources:** Does paragraph 22(1)(b)(ii) permit the withholding of ministerial metadata (such as Originating Agency [ORI] codes, court levels, court locations, names of judicial officers, or Source Identifiers [SID]) under the guise of protecting a “confidential source,” when the informant

on a Criminal Code Form 2 Information is a matter of public record post-arrest or post-issuance of process?

5. **The Exclusion of Ultra Vires Conduct from “Lawful Investigations”:** Applying the doctrine of the indivisibility of the Crown (*Benedict v. Ontario*), can information generated through, or corrupted by, fraudulent manipulation or the compilation of false information packages ever be characterized as “obtained” or “prepared” in the course of a “lawful investigation” under subsection 22(1)?
- f. **Pre-emptive Resolution of Anticipated Objections (The Establishment of Novel Precedent):** In the event the RCMP (the “**RCMP Tribunal**”) neglects its statutory duty to transmit all relevant material to the Registry and the applicant (the “**Applicant**”), does the present factual matrix warrant the establishment of a novel legal precedent? Specifically, where there exists an underlying allegation of fraud perpetrated by law enforcement in concert with Crown Counsel during a criminal proceeding that is strictly *void ab initio*, and where a criminal prosecution could not lawfully have been sustained due to the deliberate filing of an admittedly false information package into a transferee courthouse (the Ontario Court of Justice, 10 Armoury Street Courthouse), is the RCMP Tribunal precluded from relying upon spurious legal justifications to outright refuse a requisite search for the Personal Information of the Applicant?

VOLUME #3: LEGAL BASES

VOLUME #3(A): THE OFFICE OF THE PRIVACY COMMISSIONER DETERMINES THE EXTENT OF THE RCMP’S STATUTORY DUTY AND PARAMOUNTCY OF CONTROL OVER MULTI-JURISDICTIONAL ENTRIES WITHIN THE CANADIAN POLICE INFORMATION CENTRE (THE “CPIC”)

62. The Office of the Privacy Commissioner of Canada (the “**OPCC**”) previously initiated a comprehensive investigation pertaining to formal complaints registered against the Royal Canadian Mounted Police (the “**RCMP**”) which was titled by the OPCC, Disclosure of information about complainant’s attempted suicide to US (United States) Customs and Border Protection not authorized under the *Privacy Act* (see: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170419_rcmp/).
63. Said complaints concerned the unauthorized extraterritorial disclosure of personal information (the “**Personal Information**”) regarding an individual’s historical medical distress—specifically, a suicide attempt—to the United States Customs and Border Protection (the “**CBP**”). The impugned data, originally uploaded by the Toronto Police Service (the “**TPS**”) to the CPIC database, was subsequently weaponized by the CBP to formally deny the complainant entry into the United States. The OPCC determined the complaints to be entirely well-founded, conclusively ruling that the dissemination constituted a direct contravention of the *Privacy Act*, RSC 1985, c P-21, as it satisfied neither the rigid parameters of a valid “law enforcement” exemption nor the doctrine of “consistent use”.
64. In November 2013, the complainant was engaged in transnational travel originating from Toronto Pearson International Airport. During the preclearance protocol, CBP agents detained the individual, subjecting her to interrogatory measures predicated upon a historical medical emergency dated June 2012.
65. The complainant was formally deemed inadmissible to the United States pursuant to the *Immigration and Nationality Act* (United States), predicated strictly upon health-related statutory grounds (specifically, the categorization of a mental disorder allegedly posing a threat to public safety).

The Genesis of the Disclosed Intelligence:

- 43 66. The CBP extracted this sensitive intelligence directly via the CPIC mainframe. The TPS had previously instituted a “Caution flag” denoting “Suicidal Tendencies,” running concurrently with a “Special Interest Police” (the “SIP”) entry categorized as “Mental Health - Attempted Suicide - Drugs,” following their deployment to the complainant’s 2012 medical distress incident.
67. Notwithstanding the fact that the TPS physically inputted the data and the CBP acted as the ultimate consumer of said data, the formal complaint was strategically and correctly levied against the RCMP.
68. The RCMP operates as the absolute statutory steward and supreme technological administrator of the CPIC infrastructure. Furthermore, it exercises exclusive jurisdiction over the Memorandum of Cooperation (the “MOC”) executed with the Federal Bureau of Investigation, which technically facilitates the access of United States agencies to the CPIC databanks.
69. Consequently, the RCMP is encumbered with the ultimate and inescapable legal responsibility to ensure that any intelligence disseminated to foreign state actors maintains strict adherence to the *Privacy Act*. *Ipso facto*, the RCMP is precluded from operating as a mere passive repository or “blind conduit”; rather, it is compelled by law to actively govern, monitor, and regulate the propriety and legality of any data uploaded by ancillary police forces. Invoking the foundational legal maxims authored by Herbert Broom, *qui facit per alium facit per se* (he who acts through another acts himself) and *qui non prohibet quod prohibere potest assentire videtur* (he who does not prevent what he has the power to prevent is deemed to assent), the RCMP’s failure to actively restrict unlawful data sharing renders it directly culpable for the resultant privacy breaches.

Jurisprudential Analysis and Determinations of the OPCC

70. The determinative legal issue hinged upon whether the extraterritorial transmission of the data to the CBP, absent the explicit consent of the complainant, was legally justifiable pursuant to the stringent statutory exemptions articulated within subsection 8(2) of the *Privacy Act*.

Analysis of Paragraph 8(2)(f) (Agreements with Foreign States for Law Enforcement):

71. The RCMP advanced the argument that the admissibility screening protocols executed by the CBP inherently constitute a public safety and law enforcement mandate, ostensibly designed to preemptively guard against tangible threats to property or human safety.

The Finding of the Commissioner

72. The OPCC unequivocally ruled that the immigration admissibility assessments conducted by the CBP do not satisfy the rigorous definitional thresholds of “law enforcement” or “criminal justice” within the strict purview of the MOC. The complainant had engaged in no statutory infractions and was subject to no penal sanctions; her activities were strictly limited to international transit. The OPCC firmly established that deeply sensitive health intelligence must exclusively be disseminated to border authorities in circumstances where the individual in question exhibits a demonstrable, empirical threat to public safety.

Analysis of Paragraph 8(2)(a) (The Consistent Use Doctrine):

73. The RCMP averred that leveraging the health data to evaluate transnational public safety aligned consistently with the originating purpose of its collection by the municipal constabulary.
74. The OPCC rejected this premise, finding that the primary operational intent behind the collection of such data by frontline officers is to chronicle localized incidents and ensure the immediate tactical safety of officers and the public during direct, real-time interactions. The utilization of such highly confidential health records for the facilitation of a foreign immigration assessment constitutes an application that an individual could not “reasonably

The Intransigence of the RCMP

75. The RCMP formally dissented from the OPCC’s findings and outright refused the implementation of the recommended directives. The Tribunal steadfastly maintained the position that the CBP operates as a valid law enforcement entity and that the “SHARE USA” default parameter must remain universally active to theoretically preserve public safety.
76. Notwithstanding the institutional recalcitrance regarding system defaults and the precise lexicon of the policies, the OPCC acknowledged the substantive collateral benefit: the intense scrutiny of the RCMP’s architectural administration catalyzed local agencies to unilaterally purge thousands of mental health records from the CPIC network, thereby drastically mitigating the probability of analogous privacy infractions.
77. This inherent limitation encapsulates precisely why the investigative reports generated by the OPCC are not, *ipso facto*, subject to judicial review *per se*; the OPCC operates functionally as an ombudsman, authorized to recommend remedial avenues that the impugned Government Institution possesses the discretion to disregard. This structural limitation perfectly mirrors the statutory frameworks of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 and the *Access to Information Act*, RSC 1985, c A-1.
78. The Office of the Information Commissioner has some different statutory powers but that is not at issue herein.
79. Conversely, the *Privacy Act* dictates a markedly more restrictive paradigm concerning an applicant’s right to invoke the jurisdiction of the Federal Court of Canada. Adjudicative access is narrowly circumscribed, crystallized specifically when a complainant seeks relief pursuant to section 41 of the *Privacy Act* following a formal refusal of access. Ergo, the present application for judicial review is correctly and inescapably predicated upon the egregious failure of the RCMP to conduct a requisite search for the Personal Information of the applicant (the “**Applicant**”) pursuant to his formally submitted Access Request (dated March 11, 2026), and the concomitant failure of the Head of the RCMP to execute the mandatory statutory contemplation mandated under subsection 8(2) of the *Privacy Act*.

VOLUME #3(A)(I): SUMMARY OF JURISPRUDENTIAL EFFECT REGARDING THE INPUTTING OF FALSE OR INACCURATE DATA INTO CPIC BY ANY LAW ENFORCEMENT APPARATUS

80. The OPCC’s determinations establish an irrevocable precedent: the RCMP is strictly prohibited from operating as a passive host or “blind conduit” for intelligence contributed by external police forces. Given its paramount structural and administrative role, the RCMP is legally bound to exercise an active, governing supremacy over all Personal Information transiting the national infrastructure.
81. The jurisprudential rationale underpinning the OPCC’s findings is delineated into the following determinative principles:
 - a. **The Doctrine of Sufficient Control**
 - i. The OPCC explicitly concluded that the quantum of control exercised by the RCMP over the CPIC mainframe is unequivocally sufficient to trigger the robust protections of section 8 of the *Privacy Act*. Even in circumstances where a municipal entity, such as the TPS, originated the data upload and maintained nominal carriage of their localized investigative file (denoted by an occurrence number), the Commissioner of the RCMP remains the ultimate, non-delegable authority accountable for the administration, operation, and statutory compliance of the overarching system.
 1. Herein, it is a matter of evidentiary record that at least one of the specific case identification numbers associated with the impugned records is demonstrably not attributable to the TPS; namely, Police Case ID: 457197 (visibly stamped upon the upper right-hand quadrant of the admitted False Information Package). Both the TPS and the Ontario Provincial Police (the “**OPP**”) have formally and unequivocally disclaimed any jurisdictional relation to said case identification number, a repudiation which logically and necessarily leaves the RCMP as the sole remaining institutional custodian.

82. Predicated upon the fact that the RCMP acts as the exclusive Canadian signatory to the MOC executed with the Federal Bureau of Investigation, the OPCC ruled that the RCMP bears the sole, non-transferable burden of ensuring that any cross-border intelligence dissemination strictly comports with both the MOC and the domestic imperatives of Canadian privacy legislation.

The Imperative for Active Policy and Architectural Safeguards

83. The OPCC profoundly criticized the RCMP's legally bereft posture that the onus of statutory compliance rests entirely upon the contributing municipal or provincial agencies. The OPCC firmly established that the RCMP must actively engineer the CPIC policies, user protocols, and foundational technical defaults to preemptively neutralize the potential for unauthorized data proliferation.
84. 30. By way of specific illustration, the OPCC mandated that the RCMP restructure the technical baseline of the system's "SHARE USA" feature to automatically suppress the transmission of deeply sensitive health data, rather than permitting dissemination to function as the unexamined default parameter.
85. 31. This precise conflict crystallizes the overarching precedent: while the RCMP attempts to shield itself behind the facade of a collaborative, decentralized system where localized forces "own" their respective data, the OPCC definitively ruled that supreme architectural stewardship equates inextricably to absolute legal accountability. To achieve compliance with the *Privacy Act*, the RCMP must actively audit, regulate, and restrict the manner in which both domestic and foreign agencies interface with the databanks under its sovereign control.

VOLUME #3(B): THE NOVEL LEGAL ISSUES FORMULATED FOR ADJUDICATION

86. The novel legal controversies presented for adjudication herein are robust and multifaceted. It is axiomatic that these issues fundamentally engage the broader public interest, extending far beyond the immediate evasive tactics deployed against the Applicant, and possess central, systemic importance to the integrity of the administration of justice. The resolution of these distinct, untested issues will be effortlessly achieved upon the compulsory transmission of the certified tribunal record (the "CTR") to both the Federal Court of Canada and the Applicant. The subsequent enumeration is strictly illustrative, explicitly provided to pre-empt and neutralize any unnecessary, frivolous, or meritless objections the **Respondent** may attempt to mount under *Rule 318* of the *Federal Courts Rules*, *SOR/98-106* (the "**FCR**").

The First Novel and Untested Issue

87. A primary determinative issue hinges upon whether the originating data sequence inputted into the CPIC repository—irrespective of the specific law enforcement agency acting as the originating terminal, whether acting as a principal or an agent, and under whatever alphanumeric case identification number—materially mirrored the contents of the admitted False Information Package. Should the inputted data align with said package, the Applicant is undeniably entitled to its disclosure as his proprietary Personal Information, notwithstanding the fact that the underlying data is demonstrably false and fabricated: *Lawson v. Accusearch Inc.*, 2007 FC 125.

The Second Novel and Untested Issue

88. The subsequent issue necessitates an inquiry into whether the initial data matrix entered into CPIC—specifically referencing a "warrant in the first" and the identifier "MCLEAN, Kevin"—was structurally accurate at the precise moment of inception, irrespective of the underlying, contested merits of the "Ex Parte In Camera Hearing" or the purportedly valid INTAKE COURT ENDORSEMENT (dated September 23, 2024). Crucially, the Court must determine if this data was subsequently subjected to post-hoc amendment, either prior to or immediately following

the physical arrest of the Applicant. If the metadata was technically correct at the first instance, but later strategically altered to forcefully synchronize with the relevant data points required by CPIC (specifically the Foundational Metadata, encompassing the Originating Agency Identifier (the “**ORI**”); the designated issuing authority or “court field”; the remarks/narrative field; and the System Identification Number (the “**SID**”) generated upon entry), such alterations constitute a profound abuse of process. Collectively, these elements are categorized as the foundational data elements comprising a “WANT record”.

89. It is submitted as a highly probable extrapolation that the originating law enforcement agency, designated by the initial ORI, was not the identical agency that subsequently executed the surreptitious amendments to the WANT record. These potential, unauthorized systemic alterations encompass four distinct vectors of modification:
- The deliberate modification or reassignment of the ORI, falsely transferring jurisdictional appearance to a separate police service;
 - The structural alteration of the jurisprudential authority or “court field” to legitimize an otherwise *void ab initio* warrant;
 - The substantive revision of the remarks or narrative field to retroactively justify the apprehension of the Applicant; and
 - The systemic desynchronization or reallocation of the SID, designed to obfuscate the original timestamp and audit trail of the fabricated entry.
90. The forensic veracity of these administrative maneuvers—and the exposure of the underlying malfeasance—can only be illuminated through a rigorous examination of the automated hexadecimal transaction logs and sequence trails. Consequently, this determination can solely be achieved through the unmitigated disclosure of the Applicant’s Personal Information, which is definitively housed within a Personal Information Bank (the “**PIB**”) and remains under the absolute control and constructive possession of the centralized federal repository.

VOLUME #3(C): THE JURISPRUDENTIAL DOCTRINE OF POSSESSION UNDER THE FEDERAL COURT RULES

91. A masterful comprehension of the legal doctrine of “possession” is absolutely paramount when navigating the *FCR*, specifically concerning the mandatory production of documentary evidence. This doctrine governs both the general discovery apparatus (Rules 222-223) and, crucially, the compulsory transmission of tribunal records under *Rule 317*.

The Definition of Possession in the Strict Context of Rule 317

92. *Rule 317* of the *FCR* vests an applicant in a judicial review proceeding with the absolute right to requisition material relevant to the application that resides within the possession of the impugned Tribunal.
93. 73. Within the architecture of the *FCR*, the concept of “possession” vehemently rejects the archaic limitation of mere physical custody. The appellate jurisprudence has consistently expanded “possession” to broadly encompass the legal right, authority, or institutional ability to procure the document. While the *FCR* omits a rigid definitional clause for “possession,” the overwhelming weight of document production jurisprudence establishes that it strictly incorporates:
- Actual Possession:** The immediate, physical custody of the document; and
 - Constructive Power or Control:** Vesting the entity with the absolute right or jurisdictional authority to demand and obtain the document, irrespective of its immediate physical locale.

94. Consequently, for the purposes of *Rule 317*, if a Tribunal possesses the overarching legal right or technical capacity to access relevant data, that material is definitively deemed to be in its “possession” for production purposes, even if the physical servers or archives are geographically displaced.

The Tripartite Categorization of Possession

47 In advanced civil procedure, possession is jurisprudentially categorized into three distinct operational forms:

a. **Sole Possession:**

- i. **Definition:** The most absolute iteration of possession. It manifests when a singular entity exercises exclusive physical custody and administrative dominion over a record.
 1. If the Tribunal maintains the singular physical iteration of a memorandum within its immediate administrative confines, it exercises sole possession.
 2. The Tribunal retains the exclusive, unfettered right to utilize, manipulate, and produce the material.

b. **Joint Possession**

- i. **Definition:** This formulation arises when two or more distinct entities share physical custody, administrative access, or control over a record, resulting in a shared, indivisible right to possess the material.
- ii. **Application:**
 1. In circumstances where the RCMP and an external municipal police force mutually interact with a shared digital architecture (such as CPIC), both entities may exercise Joint Possession over the underlying data matrices. In the realm of document production, shared possession with a non-party does not immunize the party from production; they remain legally compelled to produce the material or actively seek the requisite consent, as their legal right to the document remains absolute.

c. **Constructive Possession**

- i. **Definition:** This represents the most expansive and vital formulation of possession. It dictates that an entity holds possession when it lacks immediate physical containment of the material, yet wields the *de jure* legal right, institutional power, or technical authority to requisition and obtain it.
- ii. **Application:** This doctrine frequently serves as the epicenter of contentious document production litigation. If the RCMP archives its historical data utilizing external federal infrastructure but retains the sovereign right to demand the extraction of those logs at will, the RCMP is irrevocably bound by Constructive Possession. Similarly, if records are held by a delegated agent or legal counsel, the principal entity maintains Constructive Possession because it exercises the power of directive over the agent. **Rule 317 Implications:** A Tribunal is strictly legally barred from resisting a *Rule 317* request by pleading an absence of physical custody if it possesses the statutory or administrative authority to compel the retrieval of the document from its current host. The RCMP is not seeking that an independent contractor provide its backup tapes but rather it is a demand unto itself if you will.

VOLUME #3(D): A COMPARATIVE LINGUISTIC ANALYSIS OF THE RCMP'S DECISIONS (THE HALTON POLICE CASE VS. THE MCLEAN RCMP PROCEEDING)

Volume #3(D)(I): The RCMP Decision in the Halton Police FIPPA Case

96. To illuminate the institutional bad faith and strategic linguistic manipulation deployed by the RCMP herein, the Applicant heavily relies upon a comparative analysis of the strikingly similar, yet critically divergent, language utilized by the RCMP in *Halton Regional Police Services Board (Re)*, 2024 CanLII 67092 (ON IPC) (the “**Halton Police Case**”). In the Halton Police Case, Adjudicator Faughnan, presiding under the *Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M.56* (the “**MFIPPA**”), reproduced the RCMP’s formal refusal letter at paragraph four, which stated:

“This is in response to your request made under the *Privacy Act*, which was received by this office on March 2, 2015, in which you are seeking a report of all inquiries made by any officer/civilian member of any Canadian or USA police force since 1970 under your identifiers including any inquiries made on CPIC/PARAS.”

Based on the information provided, a search for records was conducted. Be advised that we can neither confirm nor deny the existence of the information requested. If the information did exist, it would be subject to exemption in its entirety pursuant to Paragraph 22(1)(b) of the *Privacy Act*...

The *Privacy Act* has established the right of applicants to access federally maintained records which contain personal information concerning themselves. If you were involved with another police department or service, they may have information that concerns you. The *Privacy Act* does not authorize the RCMP to search files or to disclose information belonging to other police forces.”

Volume #3(D)(II): The Distinctions Possessing Profound Legal Significance

Volume #3(D)(II)(a): The Execution of a “Search for Records”

97. In the Halton Police Case, the RCMP formally averred that “a search for records was conducted,” utilizing the term without limitation. The term “record” lacks a precise definition under the *Privacy Act*, contrasting sharply with the *Access to Information Act* which broadly defines it as “any documentary material, regardless of medium or form.”
98. Conversely, in the present proceeding (the “**McLean RCMP Proceeding**”), the RCMP artificially narrowed its purview, strictly representing that a search was conducted solely within “CPIC and Specialized Policing Services”—despite the Applicant explicitly demanding a search of the Foundational Metadata and Offline Historical Database.

Volume #3(D)(II)(b): The Deployment and Subsequent Waiver of the “Neither Confirm Nor Deny” Shield

99. In the Halton Police Case, the RCMP explicitly deployed the powerful statutory shield of section 16(2), stating it could “neither confirm nor deny” the existence of the requested intelligence. In stark contrast, the RCMP completely abandoned this shield in the **McLean RCMP Proceeding**.

The Legal Ramifications of Waiving Section 16(2):

100. The mechanism of Section 16(2) permits a Government Institution to completely obfuscate the existence of a record, an extraordinary measure designed to preserve the sanctity of active, highly sensitive investigations. The author of the RCMP decision in the **McLean RCMP Proceeding** explicitly chose not to invoke this provision.
101. **The Legal Import:** By declining to invoke Section 16(2) *in limine*, the RCMP legally waived its right to obfuscate the existence of the records. Because it failed to issue an NCND response, the RCMP is now irrevocably tethered to its specifically cited exemptions (Sections 19, 22, and 26).
102. Should the **Respondent** attempt to argue during these proceedings that the existence of the requested Metadata is hypothetical or that confirming its existence would compromise investigative integrity, such an objection is a strict nullity. The **Respondent** has preemptively waived this protection and cannot retroactively reconstruct a Section 16(2) shield to evade production under *Rule 317*. It chose the route it did by granting itself an extension of time and it could have amended its decision from April 27, 2026, and the record will reflect that the Applicant provided it with opportunity to do so but it declined.
103. Consequently, the RCMP is legally estopped from asserting that the Personal Information sought is immune from basic acknowledgment before this Honourable Court. It falls under the principle at least by analogy from *Turigan v. Alberta, ABCA, 1988*, involving “estoppel by record”.

Volume #3(D)(II)(c): The Strategic Erasure of “Concerning Themselves”

104. In the Halton Police Case, the RCMP stated, “The *Privacy Act* has established the right of applicants to access federally maintained records *which contain personal information concerning themselves*.” Alarmingly, in the **McLean RCMP Proceeding**, the RCMP deliberately truncated this sentence, stating merely, “The *Privacy Act*

has established the right of applicants to access federally maintained records,” entirely deleting the reference to Personal Information.

105. This surgical erasure is not benign; it perfectly substantiates the Applicant’s assertion regarding the Foundational Metadata. Under Section 3 of the *Privacy Act*, “personal information” unequivocally encompasses transaction histories and assigned identifying numbers. By deliberately removing the qualifier “concerning themselves,” the RCMP attempted to linguistically sever its statutory duty to track biographical metadata logs, unlawfully recharacterizing the underlying server operations as mere “federal administrative records” exempt from the Applicant’s reach.

Volume #3(D)(II)(d): Misinterpretations Regarding Authorization and Ownership

106. In the Halton Police Case, the RCMP hypothesized, “If you were involved with another police department... they may have information that concerns you.” In the **McLean RCMP Proceeding**, the RCMP shifted to an operative past-tense certainty: “If this matter *concerned* another police department... The *Privacy Act* does not authorize the RCMP to search files or to disclose information belonging to other police forces.”

107. 99. The hypothetical “If” in the Halton matter was logical, as the requestor sought fifty years of generalized data. Herein, the Applicant demanded highly specific, targeted access to Personal Information directly indexed under Police Case ID: 457197—an identifier formally disavowed by both the TPS and the OPP. The RCMP’s assertion that it lacks “authorization” to search its own sovereign database for records that do not “belong” to other forces is a profound misstatement of law.

VOLUME #4: WITHOUT A SEARCH, CORRECTION RIGHTS CEASE TO EXIST AS LEGISLATED BY PARLIAMENT

VOLUME #4(A): PERSONAL INFORMATION IS AKIN TO ONE’S OWNERSHIP

108. It is a well-settled jurisprudential axiom that *Rule 317* of the *FCR* does not demand that the requested material be legally “owned” by the administrative Tribunal, nor does it require exclusive, physical geographic custody. The singular, uncompromising statutory threshold is that the material resides within the “possession” of the Tribunal.

109. Furthermore, relying upon established jurisprudence (such as the determinations of Mr. Justice Tysoe in the Supreme Court of British Columbia in *Mazhero*), the Personal Information of an applicant is inherently “owned” by the applicant themselves—it emphatically does not legally “belong” to other police forces, regardless of their status as the originating agency.

110. In *Atlantic Prudence Maritime Inc. v. Canada (Minister of Transport)*, 1983 2 FC 183 (FCA) (the “**Atlantic Prudence Decision**”), the Federal Court of Appeal conclusively established that possession within the context of administrative record production must be subjected to a highly practical, functional interpretation, firmly rejecting the archaic constraints of narrow property concepts. The appellate court unequivocally ruled that a Tribunal is strictly prohibited from evading its production obligations by advancing the specious claim that records are “owned” by third parties, provided those records were relied upon, hosted, or technically accessible by the Tribunal in the execution of its administrative mandate.

111. 103. This overarching principle was subsequently codified and expanded in *Canada (Attorney General) v. Cloutier*, 2008 FC 322 (the “**Cloutier Decision**”). The Federal Court definitively held that material housed within an electronic database accessible by a government institution constitutes absolute possession for the strict purposes of a *Rule 317* request. The Court forcefully rejected the obsolete notion that electronic data must be physically manifested in print or localized within a specific geographic office to be “possessed,” holding that technological accessibility acts as the absolute functional and legal equivalent of possession.

112. Under the doctrine of Constructive Possession, an entity holds possession of material whenever it exercises the legal right, administrative power, or technological capacity to command its retrieval, completely independent of physical containment. In the modern administrative apparatus, data is perpetually decentralized across complex virtual architectures. To restrict the definition of possession to physical, paper-based custody would render the operation of *Rule 317* an archaic and absolute nullity (the “**Nullity**”).
113. 105. The CPIC database represents a colossal, centralized national infrastructure. While municipal entities input localized intelligence via their discrete ORIs, the foundational technological mainframe, the database schema, and the physical server arrays are owned, operated, and exclusively maintained by the RCMP. The interaction between the RCMP and external police forces does not constitute total operational separation; rather, it manifests as a textbook paradigm of Joint Possession over the transactional metadata.
114. 106. When an external law enforcement agency instantiates a WANT Record into CPIC, that specific data matrix is instantly ingested into a database strictly hosted upon federal servers. The corresponding transactional logs, sequence trails, and hexadecimal dumps are automatically and autonomously generated by the federal system architecture itself. The RCMP holds the supreme administrative credentials, the systemic audit tools, and the absolute physical dominion over the server farms required to extract this intelligence. Consequently, the raw forensic mainframe ledger records sought by the Applicant reside indisputably within the Constructive Possession of the RCMP.

VOLUME #4(C): THE RCMP AS THE PARAMOUNT CUSTODIAN AND SOVEREIGN ADMINISTRATIVE STEWARD

115. In *Canada (Information Commissioner) v. Minister of National Defence*, 2011 SCC 25 (the “**National Defence Decision**”), the Supreme Court of Canada formulated a rigid bipartite test to determine whether a government institution exercises control over records for statutory production purposes:
- First, does the record relate to a substantive departmental matter?
 - Second, could the institution reasonably expect to obtain a copy of the record upon executing a request?
116. Although the *National Defence Decision* was adjudicated under the *Access to Information Act*, its foundational logic applies *a fortiori* to the legal concept of possession encapsulated within *Rule 317*. The administration, forensic auditing, and structural security of the CPIC infrastructure are indisputably departmental matters under the exclusive purview of the RCMP. As the sovereign national steward of CPIC, the RCMP possesses the absolute, unassailable legal and technical right to obtain, audit, and extract any record residing within its own database.
117. 109. This conclusion is explicitly supported by provincial adjudicative bodies. As noted in the Halton Police Case, the Information and Privacy Commissioner of Ontario definitively ruled that municipal police boards possess neither custody nor control over the CPIC Offline Historical Database. Because these offline archives are managed with absolute exclusivity by the RCMP, any legal demand for historical transaction logs must be directed solely to the federal institution.

VOLUME #4(D): THE ABSOLUTE NULLITY OF THE “THIRD-PARTY OWNERSHIP” DEFENSE

118. Any anticipated attempt by the **Respondent** to resist the compulsory production mandates of *Rule 317* by falsely characterizing the requested transaction logs and hexadecimal dumps as “belonging” to other police forces is a profound legal absurdity. A transaction log is emphatically not an investigative narrative report, nor does it encompass proprietary, third-party tactical intelligence. It is purely administrative Metadata—an automated, machine-generated chronicle of the systemic operations (*acta*) of the federal mainframe itself. The unique system identification numbers, the ORIs, the hardware terminal addresses, and the microsecond timestamps are intrinsic, systemic properties belonging exclusively to the CPIC platform. They constitute the indisputable administrative footprint of state action. If an arrest warrant was subjected to illicit, post-hoc digital modification—specifically via

the unauthorized exploitation of the GrapeCity SDK API—the transaction logs represent the singular, immutable evidentiary matrix proving that alteration. The deliberate suppression of this critical Metadata by the **Respondent**, disguised beneath the specious veil of inter-agency confidentiality, constitutes an administrative omission that is an absolute Nullity *ab initio*, emphatically not a curable irregularity (the “**Irregularity**”). This obstruction directly and fatally contravenes the statutory purpose of subsection 12(1) of the *Privacy Act* and fundamentally frustrates the compulsory production mechanics of *Rule 317*. The state is strictly prohibited from deploying the complexity of its own decentralized database architecture as a jurisprudential shield to conceal administrative malfeasance or *ultra vires* jurisdictional overreach.

VOLUME #4(E): THE STATUTORY ABSURDITY AND THE FRUSTRATION OF CORRECTION RIGHTS UNDER SUBSECTION 12(2) OF THE PRIVACY ACT

119. Pursuant to subsection 12(2) of the *Privacy Act*, an individual granted access to personal information utilized for an administrative purpose is statutorily vested with the affirmative right to request a correction of said information, mandate the attachment of a formal notation if the correction is refused, and compel the notification of these amendments to any entity that received the data within the preceding two years.
120. The posture adopted by the **Respondent** herein—specifically, the legally specious assertion that it lacks the authorization to search, retrieve, or disclose data inputted into its sovereign infrastructure by ancillary police forces—engineers a profound statutory absurdity (the “**Statutory Absurdity**”).
121. If the RCMP is legally permitted to abdicate its overarching search obligations beneath the guise of “third-party ownership,” it *ipso facto* obliterates the Applicant’s fundamental statutory right to subsequently request the correction of admittedly false or materially inaccurate intelligence housed within the CPIC database. A requestor cannot correct that which the paramount custodian outright refuses to locate.
122. This administrative sleight of hand effectively insulates both the centralized repository and the originating municipal police forces from statutory accountability. Should this Honourable Court validate the RCMP’s restrictive interpretation, an individual maliciously targeted by the fabrication of a False Information Package would be permanently saddled with fraudulent data operating actively within the nation’s premier law enforcement repository. This permanent taint constitutes an ongoing, egregious violation of fundamental justice.
123. It is a foundational tenet of statutory interpretation that the law does not permit a party to benefit from its own administrative malfeasance (*nullus commodum capere potest de injuria sua propria*). Furthermore, jurisprudential doctrine strictly forbids a reading of a statute that renders a remedial provision—such as the correction rights enshrined in subsection 12(2)—meaningless or illusory (*interpretatio fienda est ut res magis valeat quam pereat*, an interpretation must be adopted so that the provision may have effect rather than fail). The RCMP cannot strategically interpret section 12(1) (access) in a manner that entirely nullifies section 12(2) (correction).
124. **Nota Bene:** Should the **Respondent** attempt to argue that any correction request must instead be directed to the originating municipal or provincial agency, such an argument is fundamentally and irreparably flawed *ab initio*. Municipal police boards are explicitly excluded from the purview of the federal *Privacy Act*. More critically, a municipal entity does not possess the sovereign administrative credentials, the requisite system-wide database access, or the structural authority to execute CPIC metadata notations or mandate downstream notifications across the federal infrastructure. The RCMP, functioning as the supreme technological custodian, remains the sole entity legally and technically capable of executing the statutory mandate commanded by subsection 12(2).

Volume #4(E)(I): The Paramountcy of the Initial Search and the “Meaningful Exercise” of Subsection 12(2)

125. It is a foundational legal axiom that the invocation of the remedial correction rights enshrined within subsection 12(2) of the *Privacy Act* is strictly predicated upon the antecedent execution of a comprehensive search. Stated with stark precision: the realization of statutory rights initiates exclusively with a search. By refusing to proactively interrogate the Foundational Metadata and the Offline Historical Database—repositories over which

the RCMP exercises absolute constructive possession—the RCMP Tribunal entirely and structurally paralyzes the Applicant’s capacity to exercise his statutory entitlements.

126. In *Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration)*, 2002 FCA 270 (CanLII), 2003 1 FC 219 (the “**Information Commissioner Decision**”), the Federal Court of Appeal conclusively established the parameters safeguarding the effective operation of subsection 12(2). The appellate court ruled that the excessive severance or redaction of records, which renders the resulting disclosure incomprehensible, fundamentally undermines the “meaningful exercise” of the correction rights granted under subsection 12(2) (at para 10).
127. Applying the deductive logic of the *Information Commissioner Decision* a fortiori to the present factual matrix: if the provision of severely redacted information illegally frustrates the meaningful exercise of subsection 12(2), then the **Respondent’s** outright, institutional refusal to even conduct a preliminary search constitutes an absolute evisceration of those identical rights *ab initio*.

Volume #4(E)(II): The Competing Interests and the Disclosure of Authorizing Identities (Paragraphs 3(g) and 3(i))

128. A central determination in the *Information Commissioner Decision* was the resolution of competing statutory interests concerning the disclosure of third-party identities under paragraphs 3(g) and 3(i) of the *Privacy Act*. The Federal Court of Appeal explicitly ruled that a requester’s significant private interest in clearing their name in the public domain invariably supersedes a third party’s minimal interest in anonymity (at paras 31 and 33). Fairness in administrative inquiries dictates that adverse actions or unfavourable views cannot remain secret and strictly unchallengeable (at para 34).
129. The Applicant herein maintains a profound, legally cognizable interest in clearing his name across the national law enforcement infrastructure, an objective partially realized but requiring further unmitigated disclosure. The singular avenue to definitively establish the falsity of the CPIC data requires the disclosure of the specific authorizing entities—namely, the issuing judicial officers—embedded within the WANT record.
130. Pursuant to the *Information Commissioner Decision*, the names of the authorizing or issuing jurists fall squarely within the purview of paragraph 3(i) of the *Privacy Act* (the name of an individual where it appears with other personal information relating to the individual, or where the disclosure of the name itself would reveal information about the individual).
131. Crucially, this disclosure imperative strictly encompasses the name of the ostensibly fictitious Justice of the Peace, “George Jiri,” irrespective of the fact that said individual did not physically execute the data upload. The identities of the actors (real or fabricated) authorizing the state’s action against the Applicant constitute “views or opinions about the individual” under paragraph 3(g) and are thus inextricably embedded within the Applicant’s own Personal Information.
132. **Nota Bene:** The **Respondent** is pre-emptively estopped from asserting that a refusal to search is justified to protect the privacy interests of the municipal officers or jurists named within the CPIC warrant metadata. As the Federal Court of Appeal unequivocally held, a generalized “chilling effect” or a promise of confidentiality cannot override the statutory duty to disclose, particularly when the requester seeks to challenge fundamentally flawed or unchallengeable state actions (at paras 11-12, 34).
133. Finally, given the high probability that the False Information Package was disseminated to ancillary government institutions—potentially both domestic and foreign—the Applicant possesses an unassailable statutory right to ascertain the precise nature of the uploaded data. This knowledge is an absolute requisite to compelling the downstream notifications mandated by clause 12(2)(c). The RCMP Tribunal’s refusal to search acts as a deliberate blockade, shielding downstream consumers of fabricated intelligence from statutory correction.

VOLUME #4(F): THE OPERATIONAL EXCLUSIVITY OF “OFF-LINE SEARCHES” AND THE REDUCTIO AD ABSURDUM OF DELEGATED CONTROL

134. It is a matter of established administrative record and judicial notice that municipal and provincial law enforcement apparatuses are strictly precluded from independently executing “off-line searches” within the CPIC

infrastructure. This systemic limitation was explicitly chronicled by the Information and Privacy Commissioner of Ontario in *Halton Regional Police Services Board (Re)*, 2024 CanLII 67092 (ON IPC), relying upon the foundational analysis articulated within *Order MO-1446*.

135. As delineated within *Order MO-1446*, while ancillary police departments may possess terminal access for standard queries, an “off-line search”—a forensic mechanism utilized to process and extract deep-archive computer records—mandates the explicit submission of a formal request to the RCMP. It is only subsequent to the RCMP’s unilateral approval and physical execution of said search that the generated results are formally transmitted to the requesting agency.
136. Crucially, the adjudicator determined that the extracted search results crystallize into a record within the custody and control of the municipal police department *strictly upon their receipt* of the finalized data from the federal repository.
137. Utilizing an advanced legal syllogism, this operational architecture yields an incontrovertible conclusion: if municipal police forces are themselves entirely reliant upon the RCMP to physically access and extract data from the Offline Historical Database, then the RCMP inherently possesses absolute, unassailable custody and control over the foundational archival intelligence. To countenance the **Respondent’s** prevailing posture—that the Applicant is legally barred from requisitioning his own Personal Information directly from the RCMP because said data ostensibly “belongs” to external police forces—engineers a profound *reductio ad absurdum*. It is a legal impossibility for an external police force to “own” or exercise paramount control over a historical dataset to which they lack direct, independent access.
138. **Nota Bene:** Consequently, the RCMP remains the singular, inescapable statutory custodian capable of discharging the search and production obligations mandated by the *Privacy Act* and *Rule 317*. Any assertion by the **Respondent** that the Applicant must uniquely pursue municipal agencies to secure off-line CPIC logs is a deceptive administrative deflection, entirely devoid of operational reality and legal merit.

VOLUME #4(G): THE JURISPRUDENCE OF “CONTROL”: THE RIGHT OF DEMAND AND THE PURPOSIVE INTERPRETATION OF ACCESS LEGISLATION

Volume #4(G)(I): The Broad, Liberal, and Purposive Interpretation of Control

139. The jurisprudential conception of “control” under federal access to information legislation commands a remarkably broad, liberal, and purposive interpretation, strictly divorced from archaic notions of physical property or immediate custody.
140. In *Canada Post Corp. v. Canada (Minister of Public Works)*, 1995 CanLII 3574 (FCA) (the “**Canada Post Decision**”), the Federal Court of Appeal definitively rejected restrictive, proprietary constraints upon the statutory definition of control. Articulating the binding precedent on behalf of the appellate court, Létourneau J.A. held at page 245:

“The notion of control referred to in the Act is left undefined and unlimited. Parliament did not see fit to distinguish between ultimate and immediate, full and partial, transient and lasting, or ‘de jure’ and ‘de facto’ control. Had Parliament intended to qualify and restrict the notion of control to the power to dispose of the information, as suggested by the appellant, it could certainly have done so by limiting the citizen’s right of access only to those documents that the government can dispose of or which are under the lasting or ultimate control of the government.”

Volume #4(G)(II): The Binding Precedent of Hale v. Ontario (Criminal Code Review Board)

141. This expansive interpretive doctrine formulated by the Federal Court of Appeal was explicitly adopted and fortified by the Court of Appeal for Ontario in *Ontario (Criminal Code Review Board) v. Hale*, 1999 CanLII 3805 (ON CA) (the “**Hale Decision**”).
142. The *Hale Decision* concerned a highly analogous statutory access request. The requesters sought access to backup audio tapes created and physically retained by a court reporter. Crucially, the court reporter was not an employee, but an independent contractor engaged on a fee-for-service basis by the Ontario Criminal Code Review

Board (the “**Review Board**”). The Review Board and the court reporter formally resisted production, vehemently arguing that the backup tapes were created strictly as a personal *aide-mémoire* for the reporter, remained within the exclusive physical custody of the contractor, and were therefore not under the “control” of the Review Board.

143. The Court of Appeal for Ontario fundamentally rejected this evasion. Justice O’Connor, writing for the unanimous court, ruled that control is not contingent upon immediate physical possession or strict ownership. Rather, because the Review Board operated under a statutory mandate to keep an accurate record of its proceedings, it inherently possessed the *right to demand* access to the independent contractor’s backup tapes to verify accuracy. The appellate court unequivocally held that the institutional legal right to make a future demand for the records satisfies the statutory threshold of “control,” thereby compelling production.

Volume #4(G)(III): Application to the Present Factual Matrix: Offline Historical Data and Amended, Purged Records

144. Applying the binding jurisprudential logic of both the *Canada Post Decision* and the *Hale Decision a fortiori* to the present factual matrix yields an unassailable legal conclusion. The Applicant herein seeks access to off-line historical data, encompassing the original iterations of the inputted CPIC intelligence, alongside any subsequent unauthorized amendments, systemic purging, or operational alterations executed upon the WANT record.
145. If an administrative tribunal (such as the Review Board) is deemed by an appellate court to exercise absolute control over the independently created and personally housed backup tapes of an arm’s-length private contractor—predicated exclusively upon the tribunal’s right to demand those records for verification—the conclusion regarding the RCMP is infinitely stronger.
146. The RCMP is not interacting with an arm’s-length contractor; it is the sovereign administrator of its own technological infrastructure. The offline historical metadata resides within the RCMP’s own proprietary server arrays. The RCMP possesses the supreme, unmitigated statutory and administrative *right to demand*, extract, and audit the historical and purged data matrices generated within its own systems.
147. **Nota Bene:** Should the **Respondent** attempt to artificially distinguish between active terminal data “belonging” to local police and offline historical data, such a distinction is a jurisprudential nullity. The RCMP’s unquestionable authority to demand and extract the offline historical data establishes immediate, incontrovertible control. To suggest that the paramount federal law enforcement agency lacks control over the historical audit logs generated entirely within its own sovereign database is a legal absurdity that offends the liberal and purposive interpretative mandate established by the Federal Court of Appeal.

VOLUME #4(H): THE JURISPRUDENTIAL SIGNIFICANCE OF THE UNSOLICITED INQUIRY INTO SPECIALIZED POLICING SERVICES AND THE INVOLUNTARY INSTITUTIONAL ADMISSION OF CENTRALIZED SYSTEMIC MANIPULATION

Volume #4(H)(I): The Inference and the “Data Trigger”

148. The explicit and unsolicited inclusion of the Specialized Policing Services (the “**SPS**”) within the formal decision letter executed by the **Respondent**—specifically, via Mr. Jeff Ball—notwithstanding the absolute absence of any such request by the Applicant, precipitates a jurisprudential inference of monumental proportion. This unsolicited inclusion functions as an involuntary institutional admission that the Applicant’s dossier migrated entirely beyond the jurisdictional boundaries of standard divisional detachments, becoming inextricably embedded within the RCMP’s paramount national operational and technological command.
149. Pursuant to the strict operational strictures governing the *Privacy Act*, an Access to Information and Privacy (the “**ATIP**”) directorate is strictly prohibited from executing arbitrary or exploratory searches within branches fundamentally disconnected from the parameters of a specific request. The federal ATIP apparatus exclusively interrogates specific Personal Information Banks (the “**PIBs**”) when an initial intake assessment or an automated algorithmic database query affirmatively flags the existence of records within that distinct repository.

150. Consequently, the explicit institutional declaration that an SPS search was effectuated unambiguously exposes the **Respondent**'s internal evidentiary trail. It constitutes an irrefutable "Data Trigger": upon querying the Applicant's initial identifiers, the centralized mainframe did not merely isolate a routine, localized police occurrence. Rather, the systemic query unequivocally triggered a definitive hit tethered directly to an elite program or high-level database administered under the sovereign, national umbrella of the SPS

Volume #4(H)(II): The Proverbial "Pandora's Box" and the MESCIUS / GrapeCity SDK Software Connection

151. The jurisprudential ramifications of this involuntary institutional admission operate akin to the opening of a proverbial Pandora's Box, fundamentally fortifying and entirely legitimizing the Applicant's parallel requests instituted under the *Access to Information Act* concerning the deployment and unauthorized manipulation of MESCIUS and GrapeCity SDK software architectures.

152. As meticulously chronicled within the RCMP National System Architecture and Specialized Operational Support Manuals, the SPS is precisely the paramount federal directorate entrusted with the ownership, administration, and architectural construction of the RCMP's centralized, high-technology infrastructure. This sprawling mandate explicitly encompasses the CPIC mainframe itself, the Canadian Firearms Program, and the National Cybercrime Coordination center (the "NC3").

153. Therefore, the ATIP directorate was compelled to search the SPS for a singular, inescapable administrative reason: the SPS serves as the exclusive federal locus where the server-side document compilation logs and the forensic metadata manipulation sequence trails physically and electronically reside

Volume #4(H)(III): The Statutory Validation via the Treasury Board of Canada

154. This operational reality is further cemented by the Treasury Board of Canada's official Info Source publication, which formally registers and delineates the legal parameters of PIB RCMP PPU 005. This registration operates as the definitive, unassailable legal proof that the Offline Historical Database is inextricably bound to the federal statutory jurisdiction exercised by the SPS, rendering any overarching claim of "third-party ownership" over these specific architectural logs a strictly *ultra vires* proposition

155. Relying upon the foundational evidentiary maxim *habemus optimum testem, confitentem reum* (we have the best witness, a confessing defendant), the **Respondent**'s own unsolicited admission that it searched the SPS stands as the highest form of evidentiary proof that the federal apparatus was actively engaged in the architectural processing of the Applicant's data.

156. **Nota Bene:** Should the **Respondent** attempt to mitigate this admission by characterizing the unsolicited SPS search as a mere "routine administrative courtesy" or an over-inclusive clerical error, such an argument must be summarily dismissed *in limine* as an absolute nullity. The federal ATIP apparatus operates within a perpetual state of resource scarcity; it inherently does not expend computational or administrative capital to execute exhaustive forensic searches within the nation's most secure cyber-directorate absent a definitive, algorithmically generated directive necessitating that specific jurisdictional inquiry.

Volume #4(H)(IV): The Indispensable Role of Regional Communications as Cross-Jurisdictional Intermediaries and the Implication of Mr. Matt Peggs

157. Furthermore, the operational architecture of the SPS heavily implicates the substantive involvement of the Regional Communications (the "**Regional COM**") apparatus and specialized operational managers, specifically including Mr. Matt Peggs.

158. Within the highly stratified command structures of the RCMP's National Capital Region and allied specialized frameworks, Regional COM operates as the vital intermediary bridging localized municipal operations (such as the TPS or Peel Regional Police) and the paramount federal mainframe. When an investigative dossier manifests a profound jurisdictional paradox—such as the irreconcilable geographic conflict observed herein between the Toronto Courthouse and the fabricated authority of Brampton-based Justice of the Peace "George

Jiri”—routine frontline detachment channels are inherently bypassed. Such complex, multi-jurisdictional matters are statutorily escalated and routed directly through specialized Regional Command elements.

Because the SPS houses the Covert Operations, Cyber, and Protective Policing units any coordination of multi-jurisdictional information packages, covert data intercepts, or specialized tracking records executed by regional managers such as Mr. Peggs would automatically and inescapably be catalogued within the Specialized Investigative and Support Services repositories

Volume #4(H)(V): The Crystallization of the Rule 317 Mandate Regarding Regional Communication Logs

160. By explicitly admitting to the execution of a search within the SPS, the **Respondent** has crystallized the exact jurisdictional authority required for the Applicant to mandate the compulsory production of the comprehensive communication logs of Mr. Matt Peggs pursuant to *Rule 317*.
161. The **Respondent** is now strictly estopped from advancing the specious defense that the Regional COM office, or the communications of its managers, resides “outside the scope” of the proceeding. By formally placing the entirety of the SPS operational branch into the administrative record of its decision, the **Respondent** has voluntarily subjected the operational metadata generated by its regional managers to the transparency mechanisms of the *Federal Courts Rules*.

Volume #4(H)(VI): The Evidentiary “Smoking Gun” and the Absurdity of the Delegated Deflection

162. This explicit reference to the SPS functions as an evidentiary “Smoking Gun”—an incontrovertible admission against interest. It validates, with absolute administrative certainty, that the Applicant’s Personal Information triggered elite operational files, confirming the mobilization of national cyber-infrastructure rather than mere localized municipal records
163. Finally, this admission exposes a fatal, irreconcilable administrative contradiction within the RCMP’s prevailing posture. It highlights the profound legal absurdity of the ATIP Director formally advising the Applicant to blindly pursue records from a “municipal police force” while his own correspondence concurrently admits that the RCMP was internally compelled to interrogate its most elite, national Specialized Operational Support and Cyber branches to process the dossier
164. The **Respondent**’s attempt to obfuscate this admission beneath the guise of a “routine thorough search.” The state is legally prohibited from simultaneously asserting that a file is a mundane municipal matter while actively deploying its highest echelon of federal cyber-infrastructure to interrogate it. The **Respondent** is bound by the contradiction within its own administrative template.

VOLUME #5: CONCLUSION

I. THE TACTICAL AVOIDANCE OF PARAGRAPH 22(1)(A) AND THE UNMET BURDEN UNDER PARAGRAPH 22(1)(B)

165. The deliberate non-reliance by the **Respondent** upon *paragraph 22(1)(a)* of the *Privacy Act* represents a fatal strategic and legal error. Had the **Respondent** relied upon *paragraph 22(1)(a)* of the *Privacy Act*, it would have been inextricably compelled to demonstrate that the personal information was obtained or prepared by a specified investigative body in the course of a lawful investigation.
166. Instead, by retreating to the generalized, harm-based exemption articulated within *paragraph 22(1)(b)* of the *Privacy Act*, the **Respondent** must satisfy a rigorous and elevated evidentiary threshold. It must substantiate, with compelling exactitude, that disclosure “could reasonably be expected to be injurious to the enforcement of any law of Canada... or the conduct of lawful investigations.” The established jurisprudence of this Honourable Court emphatically dictates that “injury” under *paragraph 22(1)(b)* of the *Privacy Act* cannot be established by

mere speculation, boilerplate assertions, or administrative trepidation. The **Respondent** has effectively cornered itself: it has invoked an exemption necessitating clear, convincing, and objective evidence of harm to state operations, an evidentiary burden it is fundamentally incapable of discharging in relation to historical system transaction logs (the “**System Transaction Logs**”) and metadata.

II. THE HIGH THRESHOLD OF “INJURY TO THE ENFORCEMENT OF LAW” AND THE RULE OF LAW

167. Far from inflicting injury upon the administration of justice, the disclosure of the requested foundational metadata (the “**Foundational Metadata**”), the aforementioned System Transaction Logs, and the offline historical data residing within the Canadian Police Information Centre (the “**Canadian Police Information Centre**”) is absolutely indispensable to the preservation of the rule of law.
168. It is precisely the non-disclosure, withholding, or retroactive purging of audit trails and system metadata that profoundly threatens the integrity of both the *Privacy Act* and the *Criminal Code*. System logs operate as the primary and incorruptible mechanism by which state accountability and data integrity are forensically verified.
169. *Paragraph 22(1)(b)* of the *Privacy Act* cannot be improperly weaponized as an impenetrable shield to preclude the discovery of administrative malfeasance, unlawful data retention, or procedural non-compliance. The “injury” contemplated by Parliament is exclusively an injury to lawful law enforcement operations, not the exposure of systemic administrative deviations, fraudulent record manipulations, or the intentional evasion of statutory purging requirements.

III. THE TEMPORAL CEILING OF INVESTIGATIVE EXEMPTIONS AND THE IMPACT OF *R. V. JORDAN*

170. Records maintained within the Canadian Police Information Centre are fundamentally transactional in their legal character; they memorialize the administrative execution of legal process (for instance, the lodging, modification, or cancellation of a warrant). Once a legal process is completed, executed, or rendered legally defunct, it immediately loses any active investigative character.
171. In the present matter, the underlying proceedings are unequivocally stale-dated, having comfortably and substantially exceeded the presumptive constitutional ceilings promulgated in *R. v. Jordan*, [2016] 1 S.C.R. 631. Where an investigation is legally deceased, irrevocably inactive, or barred from prosecution by the constitutional effluxion of time, the **Respondent** cannot legitimately posit that the disclosure of transactional metadata relates to an active or ongoing investigation.
172. Furthermore, the disclosure of metadata pertaining to a concluded or non-existent matter cannot logically precipitate “injury” to an investigative process that lacks legal vitality. As famously articulated by Lord Denning in *MacFoy v. United Africa Co. Ltd.*, [1961] 3 All E.R. 1169 (P.C.), an act that is void is an absolute nullity; one cannot put something on nothing and expect it to stand, for something on nothing remains nothing.
173. To the extent that it could ever be suggested a valid criminal proceeding existed (namely, a properly constructed arrest warrant, even one ostensibly issued orally), there was not, at law, a valid criminal prosecution (the “**Criminal Prosecution**”). The factual reality that numerous hearings were attended, culminating in an order dismissing the frivolous and meritless charge predicated upon a non-informant within a fabricated information package (the “**False Information Package**”), is indisputable. However, as a matter of strict legal classification, the entire apparatus was void *ab initio* from the precise temporal moment the False Information Package was filed. The contravention of strict statutory dictates mandates that such actions be classified as an absolute nullity rather than a mere procedural irregularity.

IV. THE FALLACY OF INFORMANT PRIVILEGE IN RELATION TO PUBLIC COURT RECORDS AND METADATA

174. The **Respondent** endeavours to improperly conflate the identity of a confidential informant—who is traditionally safeguarded by the near-absolute evidentiary shield of informer privilege—with the identity of a

complainant or a swearing officer executing a form 2 information (the “**Form 2 Information**”) pursuant to the *Criminal Code*. This constitutes a profound and fatal legal error.

175. Firstly, upon the issuance of legal process or the execution of an arrest, a Form 2 Information is instantaneously transmuted into a public court record. The identity of the informant contained therein is rendered unequivocally public as an inextricable function of constitutional open court principles.
176. Secondly, the specific metadata requested—encompassing originating agency identifier codes (the “**Originating Agency Identifier**”), issuing court locations, judicial officer identities, and system identification numbers (the “**System Identification Numbers**”)—contains absolutely no identifying information concerning legitimately confidential informants.
177. The **Respondent**’s strategic contortion of *paragraph 22(1)(b)(ii)* of the *Privacy Act* to encompass non-identifying, ministerial court metadata represents an impermissible and *ultra vires* expansion of the confidential source exemption, a proposition that is wholly unsupported by the statutory text or established common law principles.

V. ULTRA VIRES CONDUCT, FRAUDULENT MANIPULATION, AND THE LIMITS OF “LAWFUL INVESTIGATIONS”

178. The doctrine of the indivisibility of the Crown, as elucidated in *Benedict v. Ontario (2000)*, 51 O.R. (3d) 147 (C.A.), dictates that the state cannot act in a fractured or divided capacity. The state is legally precluded from claiming the benefits of statutory protections while its agents simultaneously act in direct, deliberate contravention of the law.
179. The existence of a “lawful investigation” operates as a strict, unyielding condition precedent to the application of any exemption enumerated under *subsection 22(1)* of the *Privacy Act*. State action that is birthed from bad faith, systemic fraud, or the deliberate, calculated manipulation of institutional records is *ultra vires* and void *ab initio*.
180. Just as criminal misconduct perpetrated by an individual officer operating under the colour of authority can never be shielded under the guise of “law enforcement and investigation,” institutional acts of record manipulation or the compilation of a False Information Package cannot, under any legal fiction, be characterized as a “lawful investigation.”
181. To hold otherwise would establish a perilous precedent, permitting the state to invoke statutory privacy exemptions to conceal its own unlawful conduct—a consequence that is profoundly offensive to the principles of fundamental justice, equitable doctrines, and the explicit statutory architecture of the *Privacy Act*.

VI. THE JURISDICTIONAL LEGERDEMAIN: SECTION 19(1)(D) AND THE CENTRAL REGION METAMORPHOSIS

182. In a manifest attempt to orchestrate a sophisticated statutory evasion, the **Respondent** has invoked *paragraph 19(1)(d)* of the *Privacy Act*, alleging that the foundational records constitute personal information obtained in confidence from the government of a province or an institution thereof. This invocation is a jurisprudential sleight-of-hand designed to obfuscate the internal structural metamorphosis of the Royal Canadian Mounted Police.
183. It is a matter of administrative record that the federal entity formerly designated as “O” Division has been systematically restructured into an integrated, multi-jurisdictional intelligence hub now operating as central region command (the “**Central Region**”). The invocation of *paragraph 19(1)(d)* of the *Privacy Act* is predicated upon a deliberate mischaracterization: treating the highly integrated Central Region infrastructure—which is fundamentally federal in its apex control—as an independent “provincial institution” merely because it synergizes with municipal or provincial entities.
184. The refusal to disclose the Originating Agency Identifier, the issuing court level, and the identity of the presiding judicial officer is not animated by a genuine desire to protect intergovernmental confidences. Rather, it is a calculated manoeuvre to prevent the forensic tracing of the data directly back to the executive suites of the Central Region, specifically the purview of the regional commander (the “**Regional Commander**”).

- 59 185. The evidentiary record strongly supports the inference that the Regional Commander, acting as the multi-jurisdictional intermediary, ingested unverified data and uploaded it directly into the federal mainframe under police case identification number 457197 (the “**Police Case Identification Number**”). It is submitted that the immense institutional weight of the Regional Commander was utilized to bypass standard judicial scrutiny, allowing an irregular and fundamentally flawed authorization to be accepted on its face by the issuing justice.
186. *Nota Bene*: The **Respondent** may counter that the Central Region, by virtue of its joint-forces operations, functions *de facto* as a provincial entity for the purposes of *paragraph 19(1)(d)* of the *Privacy Act*. This argument is entirely devoid of merit and offends the doctrine of federal paramountcy. The Canadian Police Information Centre is a sovereign federal mainframe. The indivisibility of the Crown strictly precludes a federal institution from bifurcating its own hybrid command structure to artificially generate a “third-party” provincial shield where none exists at law. The data residing under the Police Case Identification Number is exclusively within the constructive possession and paramount control of the federal **Respondent**.
187. This structural obfuscation perfectly elucidates why the front-facing municipal police service was entirely incapable of producing a physical arrest warrant during the period of detention. The municipal constabulary was acting merely as the operational appendage for a data file generated, maintained, and entirely controlled within the Central Region infrastructure of the **Respondent**. The concealment of this reality through the misapplication of *paragraph 19(1)(d)* of the *Privacy Act* is *ultra vires* the **Respondent**’s statutory authority.

VII. THE APPLICATION OF EQUITABLE MAXIMS: FRAUD UPON THE LAW AND THE VITIATION OF ADMINISTRATIVE ACTS

188. The deliberate withholding of exculpatory system metadata and the invocation of inapplicable statutory exemptions must be scrutinized through the lens of established equitable maxims. As extensively catalogued in Herbert Broom’s seminal treatise, *A Selection of Legal Maxims*, the foundational premise remains resolute: fraud is proved when it is demonstrated that a false representation has been made knowingly, without belief in its truth, or recklessly, careless as to whether it be true or false.
189. Where systemic administrative operations are executed with reckless disregard for statutory prerequisites, producing a False Information Package that results in unlawful deprivation of liberty, an honest belief in the truth of the state’s actions is nullified. The motive of the state actor guilty of such reckless promulgation is rendered legally immaterial.
190. Furthermore, the equitable principle of fraudulent concealment forcefully applies to toll any procedural barriers. It has long been an axiom of equity that no length of time is a bar to relief in cases of fraud where there has been no laches on the part of the defrauded party. The maxim *nemo ex suo delicto meliorem suam conditionem facere potest* (no man can improve his condition by his own wrong) strictly precludes the **Respondent** from utilizing its own obfuscatory tactics—namely, hiding the Originating Agency Identifier and the Police Case Identification Number—to prevent the discovery of the underlying nullity.
191. The execution of legal process is bound by strict jealousy, designed to protect against fraud, collusion, and the resulting disgrace to the Crown and the administration of justice. The rule *necessitas quod cogit defendit* (necessity defends what it compels) cannot be invoked by the state when the “necessity” was entirely manufactured by its own creation of a False Information Package.
192. If an individual or an institutional entity, acting under colour of right or the colour of law, executes an illegal act or abuses the process of the court, transforming it into an instrument of oppression or extortion, such conduct constitutes a fraud upon the law. Consequently, the **Respondent** is strictly barred from availing itself of its own illegal acts.
193. It is an unassailable tenet of jurisprudence that fraud vitiates everything it touches (*fraud no doubt vitiates everything*). Where an administrative act or judicial authorization is procured through the reckless or intentional submission of a False Information Package, the resulting instrument is not merely tainted by irregularity; it is an absolute nullity, void *ab initio*, rendering the parties subject to the equitable restoration of the *status quo ante*.
194. The primary function of litigation, and indeed of the administrative tribunal process, is the untrammelled search for truth. Properly interpreted, privacy legislation is designed to promote, rather than hinder, that truth-seeking function. By deliberately refusing to execute a compliant search and by shielding the executive

machinations of the Central Region, the **Respondent** continues to perpetuate a fraud upon the tribunals, upon the law, and upon the administration of justice *in limine*.

VIII. THE FIDUCIARY DUTY OF DISCLOSURE AND THE EQUITABLE INTEREST IN PERSONAL INFORMATION: THE APPLICATION OF MCINERNEY V. MACDONALD

195. The jurisprudence articulated by the Supreme Court of Canada in *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 governs the incontrovertible right of an individual to access personal information held by an institutional repository. The apex Court definitively ruled that information regarding oneself, revealed to or compiled by an institution acting in a professional capacity, remains, in a fundamental and immutable sense, the property of the individual.
196. While the **Respondent** may claim structural ownership of the physical and digital architecture comprising the Canadian Police Information Centre, it must be legally emphasized that the **Respondent** acts merely as a custodian of the personal information residing therein. The Supreme Court of Canada categorically established that the subject of the records possesses a trust-like beneficial interest (the “**Beneficial Interest**”) in the substantive information itself. This equitable interest mandates that, as an unyielding general rule, the individual possesses a paramount right of access to the information, thereby imposing a corresponding obligation upon the institutional custodian to effectuate its immediate provision.
197. The relationship between the state as the repository of sensitive personal data and the individual to whom that data pertains is inextricably imbued with fiduciary obligations. A fiduciary duty (the “**Fiduciary Duty**”) inherently demands that the institutional actor conduct itself with the utmost good faith, loyalty, and transparency. To deny an individual access to their own Foundational Metadata and System Transaction Logs constitutes a profound breach of this Fiduciary Duty, effectively utilizing the confidentiality mechanisms designed to protect the individual as a clandestine shield to facilitate improper institutional conduct.
198. Furthermore, the principles of equity demand a strict reciprocity of information. The necessity for state institutions to compile sensitive, highly private data concerning an individual must be counterbalanced by a corresponding openness and full disclosure to that selfsame individual. As noted in *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, the systematic withholding of records profoundly undermines the structural integrity of the administrative system. If there has been improper conduct in the compilation or maintenance of the records—such as the reckless promulgation of a False Information Package—it is an imperative of justice that such deviations be illuminated rather than sequestered under the guise of an arbitrary statutory exemption.
199. Given the profound disparity in the evidentiary capacities of the parties, the Supreme Court of Canada explicitly mandated that the burden of proof rests entirely and exclusively upon the entity withholding the information. The onus falls squarely upon the **Respondent** to definitively justify any exception to the general rule of access. Such a denial cannot be predicated upon mere speculative administrative inconvenience or the abstract fear of subsequent litigation; it requires the demonstration of a significant likelihood of a substantial adverse effect, a threshold the **Respondent** has conspicuously failed to meet.
200. The **Respondent** possesses no unfettered discretion to arbitrarily deny access to the Originating Agency Identifier or the Police Case Identification Number. Such administrative discretion is heavily circumscribed and must be exercised upon proper equitable principles. Where the **Respondent** refuses a legitimate request for access, this Honourable Court is fundamentally empowered to exercise its superintending equitable jurisdiction, acting *in personam* to ensure the **Respondent** adheres strictly to its standard of conduct and is restrained from acting in a manner inconsistent with the applicant’s Beneficial Interest.
201. Ultimately, the deliberate obfuscation of the System Transaction Logs to insulate the machinations of the Central Region and the Regional Commander is diametrically opposed to the fiducial qualities required of a state repository. Where systemic fraud upon the law is alleged, the principles enshrined in *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 forcefully compel the immediate unsealing and production of the underlying records, affirming the paramountcy of truth-seeking over the tactical evasion of institutional accountability.
202. But it all comes back to the same issue that the **Respondent** RCMP Tribunal admitted it did not search because of its misguided understanding of the law, as scary as it is, that the *Privacy Act* does not authorize the RCMP to search files OR disclose information belongings to other police forces.

- 61 203. The RCMP Tribunal did not rely on section 18 of the *Privacy Act* so none of the Personal Information sought by the Applicant in a PIB was exempt from searching. Moreover, the RCMP Tribunal did not rely on ss. 22(1)(a) at all or even 22(1)(a)(ii) which is required in relation for reliance on an exempt bank. This was and is fatal to the RCMP Tribunal with respect to its decision that it could not search for “files”.
204. In relation to any and all Personal Information sought by the Applicant that was highly particularized as statutorily required (see: ss. 12(1)(b): under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution), the RCMP Tribunal failed to search the CPIC database, as it admitted, for Foundational Metadata and Offline Historical Database in relation to the Applicant’s Personal Information. The attached document to the April 27, 2026, decision or disposition of the Tribunal (RCMP), was not even within the spectrum of what would be produced in disclosing Foundational Metadata (i.e. the ORI; the issuing court level; the issuing court location; the name of the judicial officer; and the SID) and/or the Offline Historical Database for amended or purged originally input data including the likes of CLEAR, CANCEL, ADD, MODIFY et al type functions in relation to the Applicant’s Personal Information. It is trite that metadata is information that can be Personal Information in relation to an individual.
205. The legal test for the transmission of materials pursuant to *Rule 317* of the *Federal Courts Rules* has been comprehensively and irrefutably satisfied. The requested material was demonstrably available to the administrative tribunal in question (see: *subsection 2(1)* of the *Federal Courts Act*) at the time but nonetheless it is in its possession at the time of this *Rule 317* request:
- Relevant to the core issues on judicial review, specifically the abject failure of the **Respondent** to execute a reasonable, legally compliant search;
 - In the possession (whether actual, constructive, or joint) of the **Respondent**, acting in its capacity as the paramount administrator of the Canadian Police Information Centre; and
 - Not in the possession of the applicant.
206. As the Applicant did not include a specified request such as this in his Notice Of Application (“NOA”) it is included hereunder pursuant to *Rule 317(3)* of the *Federal Courts Rules*.

All of which is respectfully requested by Mr. Kevin A. McLean (BA, JD, CIM)



DATED at Toronto, Ontario, this 18th day of May, 2026.

Mr. Kevin A. McLean (BA, JD, CIM)

Toronto, Ontario

Applicant, Self-Represented

mclean@searchandseizure.ca

Rule 317 of the Federal Courts Rules

317 (1) A party may request anything that is relevant to the application that is in the possession of a federal board, commission or other tribunal whose order is the subject of the application and that was not when the application was made in the possession of the party.

(2) The request shall be in Form 317.

(3) The request shall be served on the tribunal and on all other parties.

(4) A request under subsection (1) may be made at any time, but if it is made after the applicant has served its record under rule 309, the request may only be made with leave of the Court.

Rule 318 of the Federal Courts Rules

318 (1) Within 20 days after being served with a request under rule 317, the tribunal shall transmit (a) the original or a certified copy of the requested material to the registry, and (b) a copy of the material to the party who requested it or a written notification that the material is not in the possession of the tribunal.

(2) Where the tribunal or a party objects to a request under rule 317, the tribunal or party shall, within 20 days after being served with the request, serve on all other parties and file a written objection stating the grounds for the objection.

(3) The Court may, on motion, examine the material and order that the material, or a portion of it, be transmitted to the registry or returned to the tribunal.

The formal transformation of the RCMP's "O" Division into the **Federal Policing Central Region** was implemented between late **2023** and **2024**. [1, 2]

Timeline Breakdown:

- **Phase 1 (2022–2023):** The RCMP initiated a broader Federal Policing transformation plan. This included preliminary steps to decommission the old National Division and consolidate its units into Ontario's framework.
- **Phase 2 (October 2023):** Assistant Commissioner Matt Peggs was originally appointed as the Commanding Officer of "O" Division.
- **Phase 3 (2024):** As the organizational structure shifted away from traditional geographic divisions into specialized federal regions, "O" Division was officially rebranded as **Central Region**, with Peggs carrying over his leadership as the newly titled Regional Commander.

- Nothing past this line -

Tab 3

e-document-é		T-2448-26 ID 6	
F	I	FEDERAL COURT	D
L	L	COUR FÉDÉRALE	É
E	E		P
D	D		O
		May 20, 2026	S
		20 mai 2026	É
		Diane Lopez	
TOR		3	

Court File No: T-2448-26

BETWEEN:

KEVIN ALEXANDER McLEAN

Applicant

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFFREY BALL, and
STEPHANE BRISSON

Respondents

NOTICE OF FILING PROOF OF SERVICE BY ANALOGY TO RULE 146(1)(b) AND IN ACCORDANCE WITH THE CURATIVE PROVISIONS OF RULE 5, Rule 55 (Varying Rule and Dispensing with Compliance) AND RULE 66 OF THE *FEDERAL COURTS RULES* in the form of an Applicant's Certificate of Service

TO THE REGISTRY AND TO THE RESPONDENTS:

TAKE NOTICE that the Applicant is filing herewith the uncontested proof of service concerning the Applicant's "**COMPREHENSIVE WRITTEN REQUEST OF THE RCMP (TRIBUNAL) PURSUANT TO RULE 317 OF THE FEDERAL COURT RULES**", dated May 19, 2026, which was previously rejected under Rule 72(2)(a) solely for an administrative absence of verification data.

I, **Mr. Kevin A. McLean (BA, JD, CIM)**, Applicant, acting in a self-represented capacity, hereby certify that I caused the Respondents and the Attorney General of Canada (on behalf of the Respondent RCMP) to be duly served with true copies of the standalone Rule 317 Request and the stamped, issued Notice of Application for Judicial Review via the following concurrent physical and electronic methodologies:

1. **Physical Personal Service:** By personally delivering true physical copies of the aforementioned documents on the morning of **May 20, 2026**, directly to the office of the Department of Justice (Attorney General of Canada), located at 120 Adelaide Street West, Suite 400, Toronto, Ontario, M5H 1T1.
2. **Electronic Service and Ingestion Verification:** Pursuant to Rule 146(1)(b), applied by analogy via the flexible variation provisions of Rule 5 and Rule 66, actual electronic service was fully executed on the morning of **May 20, 2026**. This service was routed to the validated, public-facing Department of Justice intake addresses obtained directly from the physical entrance door of the Suite 400 office.

1. Schedule "A":

1. All emails under the titled email thread, "McLean v. RCMP et al - T-2448-26 - Notice of Application" which include eight email message;
 1. A true copy of the electronic transmission log dated May 20, 2026, at 10:20 AM and 10:23 AM, demonstrating complete service of the Rule 317 Request upon the Attorney General of Canada at the corrected, validated address: AGC_PGC_Toronto.Lead-DCECJ@justice.gc.ca (Search and... pp. 1, 3, 5).
 2. A true copy of the automated confirmation receipt generated by the Department of Justice at 10:23 AM via TOR.Leadadmissions@justice.gc.ca, verifying successful server ingestion and active monitoring (Search and... p. 7).

The underlying 39-page Rule 317 Request is appended to this notice after the last page under Schedule "A".

67
DATED at Toronto, Ontario, this 20th day of May, 2026, and duly signed by the undersigned individual:

Mr. Kevin A. McLean (BA, JD, CIM)

Applicant, Self-Represented

68 Abell Street, Toronto, ON M6J 0B1

Email: mclean@searchandseizure.ca

Schedule “A”

McLean v. RCMP et al - T-2448-26 - Notice of Application

8 messages

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Tue, May 19, 2026 at 4:57 PM

To: Legal_Services@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, Robert.Borland@rcmp-grc.gc.ca

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

As promised, please find the stamped Notice of Application from the FCC Registry for service upon the Respondents. There were some changes that were required to the final version that were drawn to my attention by the FCC Registry and I made those last night and into the morning. It does not affect my Rule 317 of the FCR request.

I have included the noted emails therein including legal counsel along the Legal Services email.

You have ten days from today's date to file and serve a Notice of Appearance.

Thank you kindly.

Mr. Kevin A. McLean (BA, JD, CIM)

--

Best regards,

Mr. Kevin A. McLean (BA (MCL), JD, CIM)

Email: mclean@searchandseizure.ca

Phone: 647.370.9354

Fax: upon request

NOTA BENE: This email is for dispute resolution and litigation purposes only. Without prejudice communication so denoted invokes settlement privilege.

CONFIDENTIALITY NOTICE: This email and any attachments are confidential and may contain privileged information. It is intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution, or reliance upon the contents of this email is strictly prohibited. If you have received this communication in error, please immediately notify the sender by replying to this email and permanently delete the original message and any attachments from your system.

2 attachments

 **T-2448-26 - Kevin Alexander McLean v. Royal Canadian Mounted Police et al - Stamped Copy - May 19 - 2026.pdf**
1066K

 **Rule 317 Requist - McLean v. RCMP - Applicant - Mr McLean - 18-May-2026 - Electronically Signed - Served - Filed.pdf**
664K

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I also confirm, out of an abundance of caution, that you now have 20 days from today's to file the certified tribunal record, along with serving me with a copy of the same, based on the materials particularized in your possession that are relevant to this Application.

Kindly provide the same exclusively to this email for service purposes.

Thank you kindly.

[Quoted text hidden]

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Tue, May 19, 2026 at 10:24 PM

To: Legal_Services@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, Robert.Borland@rcmp-grc.gc.ca

Date: May 19, 2026

Classification: Private and Confidential

Sending method: Via Email

Your file number: Court File No. T-2448-26

To:

Respondents in McLean v. Royal Canadian Mounted Police et al. under Court File No. T-2448-26

Subject I: Confirmation of effectuated service concerning Court File No. T-2448-26

Subject II: Procedural notification regarding the transmission of the notice of application

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

PART 1: INTRODUCTION

1. Written correspondence is hereby initiated regarding the aforementioned matters.
2. The enumerated documentation is appended hereto for the substantive and procedural purposes delineated herein.

PART 2: CONFIRMATION OF EFFECTUATED NOTIFICATION AND SERVICE

Execution of Primary Regional Service

3. Unambiguous confirmation is hereby proffered that formal notification has been effectuated upon the Royal Canadian Mounted Police Central Region, specifically directed via electronic mail to the attention of Regional Commander Mr. Matt Peggs.
4. In conjunction with the aforementioned electronic notification, a facsimile transmission of the notice of application (the "**Notice of Application**") for judicial review was concurrently executed upon the Royal Canadian Mounted Police Toronto West Detachment (the "**Toronto West Detachment**") situated in Milton, Ontario.
5. Furthermore, it is formally certified that a congruent courtesy transmission of the requisite materials, in strict accordance with the mechanisms outlined under *Rule 317* of the *Federal Courts Rules*, has been duly conveyed *in limine*.

71 Execution of Federal Headquarters Service

6. It is additionally certified that a facsimile transmission of the Notice of Application was effectively served upon the federal headquarters of the Royal Canadian Mounted Police, located in Ottawa, Ontario, during the evening hours of the present date.

PART 3: EVIDENTIARY SUBSTANTIATION AND PROCEDURAL SAFEGUARDS

Provision of Evidentiary Substantiation

7. In the event that evidentiary substantiation of the aforementioned transmissions is necessitated by the respondents (the "**Respondents**"), prompt advisement is respectfully demanded, whereupon comprehensive documentary validation of the effectuated service shall be expeditiously produced *ipso facto*.

Preservation of the Procedural Record

8. Notwithstanding the immediate availability of absolute proof, this communication is dispatched *ex abundanti cautela* to permanently interdict any prospective obfuscation, structural manipulation, or misrepresentation of the procedural record.
9. This proactive articulation ensures that, should procedural exigencies dictate the swearing and filing of formal affidavits of service or notice, an immutable and meticulously documented foundational substratum exists upon which absolute legal reliance may be placed, thereby rendering any subsequent contrary assertions of procedural deficiency a fundamental nullity *ab initio*.

PART 4: ANTICIPATED RESPONSES FROM INDEPENDENT COUNSEL

10. Upon the requisite retention and formal designation of independent legal counsel for each respective Respondent, it is strictly anticipated that all responsive procedural correspondence shall be directed herein in accordance with established jurisprudential protocols, thereby preserving the *status quo ante*.

Thank you.

[Quoted text hidden]

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Wed, May 20, 2026 at 12:14 AM

To: Legal_Services@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, Robert.Borland@rcmp-grc.gc.ca

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I write to confirm that my Rule 317 Request has been filed with the FCC. I made two slight revisions for the date and the inclusion of the file number. Please find attached. Thank you.

[Quoted text hidden]



Rule 317 Request - T-2448-26 - McLean v. RCMP - Applicant - Mr McLean - 19-May-2026 - SIGNED - FILED - SERVED.pdf
585K

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Wed, May 20, 2026 at 10:20 AM

To: Legal_Services@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, Robert.Borland@rcmp-grc.gc.ca, AGC_PGC_Toronto.Lead-DCECG@justice.gc.ca

Date: May 20, 2026

Classification: Private and Confidential

Sending method: Via Electronic Mail

To:

The Attorney General of Canada; Royal Canadian Mounted Police; and Relevant Respondents
Subject I: *McLean v. Royal Canadian Mounted Police et al.* (Court File No. T-2448-26) before the *Federal Court of Canada* — Confirmation of Hard Copy Service of the Issued notice of application

for judicial review (the "**Notice Of Application For Judicial Review**") dated November 15, 2026
 Subject II: Service of Requisition for Material Pursuant to *Rule 317* of the *Federal Courts Rules*,
 SOR/98-106 and Ascertainment of Legal Representation

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

PART I: INTRODUCTION

1. Correspondence is hereby transmitted in relation to the aforementioned jurisprudential matters.

PART II: EFFECTUATION OF SERVICE

Section A: Physical Service of Originating Documentation

2. Formal notification is hereby provided that physical, hard-copy service of the originating document, specifically the filed iteration of the notice of application for judicial review (the "**Notice Of Application For Judicial Review**") dated May 15, 2026, alongside a duplicate of the requisition for materials pursuant to *Rule 317* of the *Federal Courts Rules* (the "**Rule 317 Request**"), was successfully consummated upon the physical premises of the respondents.

Section B: Electronic Transmission Directive

3. During the aforementioned consummation of physical service, an observation was recorded regarding a formally posted directive upon the entryway of the premises. The said directive explicitly delineated a designated electronic mailing address, specifically AGC_PGC_Toronto.Lead-DCECG@justice.gc.ca (the "**Designated Electronic Address**"), mandated for the receipt of service of documentary instruments upon the Attorney General of Canada in proceedings wherein a notice of constitutional question (the "**Notice Of Constitutional Question**") is manifestly **absent**.

PART III: PROVISION OF SUPPLEMENTARY ENCLOSURES

5. To facilitate expeditious judicial economy and out of an abundance of procedural caution, exact duplicate iterations of the previously served physical documents are appended to this electronic transmission for immediate perusal and referential convenience.

PART IV: ASCERTAINMENT OF RESPONDENT REPRESENTATION

6. A formal inquiry is hereby advanced to ascertain whether the named respondents, individually or collectively, shall be represented by duly appointed legal counsel or, in the alternative, whether said entities shall be proceeding *in propria persona* throughout the adjudication of the aforementioned judicial review. Should any of the particulars of the material requested be unclear, please advise me forthwith. Otherwise, I will presume that all is sufficiently clear and particularized. I anticipate that I will have my current motion and application records to you in short order with the proviso that additional documents and records will be included where applicable (i.e. not in my possession).

7. Thank you kindly in advance for your anticipated compliance.

Yours truly,
 Mr. Kevin A. McLean (BA, JD, CIM)
 Enclosures

[Quoted text hidden]

2 attachments

 **Rule 317 Request - T-2448-26 - McLean v. RCMP - Applicant - Mr McLean - 19-May-2026 - SIGNED - FILED - SERVED.pdf**
 585K

 **T-2448-26 - Kevin Alexander McLean v. Royal Canadian Mounted Police et al - Stamped Copy - May 19 - 2026.pdf**
 1066K

Mail Delivery Subsystem <mailer-daemon@googlemail.com>
To: mclean@searchandseizure.ca

Wed, May 20, 2026 at 10:20 AM



Address not found

Your message wasn't delivered to **AGC_PGC_Toronto.Lead-DCECG@justice.gc.ca** because the address couldn't be found, or is unable to receive mail.

LEARN MORE

▲ This link will take you to a third-party site

The response from the remote server was:

550 5.4.1 Recipient address rejected: Access denied. For more information see <https://aka.ms/EXOSmtpErrors> [QB1PEPF00004E09.CANPRD01.PROD.OUTLOOK.COM 2026-05-20T14:20:23.271Z 08DEB324FB54CC87]

Final-Recipient: rfc822; AGC_PGC_Toronto.Lead-DCECG@justice.gc.ca

Action: failed

Status: 5.4.1

Remote-MTA: dns; [justice-gc-ca.mail.protection.outlook.com](https://aka.ms/EXOSmtpErrors). (52.101.192.0, the server for the domain [justice.gc.ca](https://aka.ms/EXOSmtpErrors).)

Diagnostic-Code: smtp; 550 5.4.1 Recipient address rejected: Access denied. For more information see <https://aka.ms/EXOSmtpErrors> [QB1PEPF00004E09.CANPRD01.PROD.OUTLOOK.COM 2026-05-20T14:20:23.271Z 08DEB324FB54CC87]

Last-Attempt-Date: Wed, 20 May 2026 07:20:23 -0700 (PDT)

noname
5K

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Wed, May 20, 2026 at 10:23 AM

To: Legal_Services@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, Robert.Borland@rcmp-grc.gc.ca, AGC_PGC_Toronto.Lead-DCECJ@justice.gc.ca

AGC_PGC_Toronto.Lead-DCECJ@justice.gc.ca

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns: I apologize as I input a "G" as opposed to a "J" where the letter before the @ was required. Thank you.

Date: May 20, 2026

Classification: Private and Confidential

Sending method: Via Electronic Mail

To:

The Attorney General of Canada; Royal Canadian Mounted Police; and Relevant Respondents
Subject I: *McLean v. Royal Canadian Mounted Police et al.* (Court File No. T-2448-26) before the *Federal Court of Canada* — Confirmation of Hard Copy Service of the Issued notice of application for judicial review (the "**Notice Of Application For Judicial Review**") dated November 15, 2026

Subject II: Service of Requisition for Material Pursuant to *Rule 317* of the *Federal Courts Rules*, SOR/98-106 and Ascertainment of Legal Representation

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

PART I: INTRODUCTION

1. Correspondence is hereby transmitted in relation to the aforementioned jurisprudential matters.

PART II: EFFECTUATION OF SERVICE

Section A: Physical Service of Originating Documentation

2. Formal notification is hereby provided that physical, hard-copy service of the originating document, specifically the filed iteration of the notice of application for judicial review (the "**Notice Of Application For Judicial Review**") dated May 15, 2026, alongside a duplicate of the requisition for materials pursuant to *Rule 317* of the *Federal Courts Rules* (the "**Rule 317 Request**"), was successfully consummated upon the physical premises of the respondents.

Section B: Electronic Transmission Directive

3. During the aforementioned consummation of physical service, an observation was recorded regarding a formally posted directive upon the entryway of the premises. The said directive explicitly delineated a designated electronic mailing address, specifically AGC_PGC_Toronto.Lead-DCECG@justice.gc.ca (the "**Designated Electronic Address**"), mandated for the receipt of service of documentary instruments upon the Attorney General of Canada in proceedings wherein a notice of constitutional question (the "**Notice Of Constitutional Question**") is manifestly **absent**.

PART III: PROVISION OF SUPPLEMENTARY ENCLOSURES

5. To facilitate expeditious judicial economy and out of an abundance of procedural caution, exact duplicate iterations of the previously served physical documents are appended to this electronic transmission for immediate perusal and referential convenience.

PART IV: ASCERTAINMENT OF RESPONDENT REPRESENTATION

6. A formal inquiry is hereby advanced to ascertain whether the named respondents, individually or collectively, shall be represented by duly appointed legal counsel or, in the alternative, whether said entities shall be proceeding *in propria persona* throughout the adjudication of the aforementioned judicial review. **Should any of the particulars of the material requested be unclear, please advise me forthwith. Otherwise, I will presume that all is sufficiently clear and particularized. I anticipate that I will have my current motion and application records to you in short order with the proviso that additional documents and records will be included where applicable (i.e. not in my possession).**
7. Thank you kindly in advance for your anticipated compliance.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)

TOR - Lead Admissions <TOR.Leadadmissions@justice.gc.ca>
To: "Mr. Kevin Alexander McLean" <mclean@searchandseizure.ca>

Wed, May 20, 2026 at 10:23 AM

This message is automatically generated, and confirms receipt of your email. Please do not respond to this message. The email box is monitored from 8:00am to 5:00pm weekdays, excluding statutory holidays. Any materials received after 5:00 pm will be treated as if received on the following business day.

Ce message est généré automatiquement et confirme la réception de votre courriel. Veuillez ne pas répondre à ce message. La boîte courriel est surveillée de 8 h à 17 h en semaine, à l'exception des jours fériés. Tout matériel reçu après 17 h sera traité comme s'il avait été reçu le jour ouvrable suivant.

Party: Applicant
Document type: PDF signed request pursuant to Rule 317 of the FCR
Short title: *McLean v. RCMP et al*
Court Level: Federal Court of Canada
Court Office: City of Toronto (180 Queen Street West, Suite 200)

COURT FILE NUMBER: T-2448-26

May 19, 2026

COMPREHENSIVE WRITTEN REQUEST OF THE RCMP (TRIBUNAL)
PURSUANT TO RULE 317 OF THE *FEDERAL COURT RULES*, WHICH IS
TITLED “MATERIAL IN THE POSSESSION OF THE TRIBUNAL” (AS
DEFINED UNDER *FCR*, S. 317 AND *FCA*, S. 2)

Served on the RCMP in its capacity as a “Tribunal” as defined under *Federal Court Rules*, section 2, where *tribunal* has the same meaning as *federal board, commission or other tribunal* under section 2(1) of the *Federal Courts Act*) on May 18, 2026.

Table of Contents

WRITTEN REQUEST OF THE RCMP (TRIBUNAL) PURSUANT TO RULE 317 OF THE *FEDERAL COURT RULES*, WHICH IS TITLED “MATERIAL IN THE POSSESSION OF THE TRIBUNAL” (AS DEFINED UNDER *FCR*, S. 317 AND *FCA*, S. 2) 1

PART 1: statement of rule 317 request and overview of seminal principles under rule 317 to 319 of the *FCR* 4

 Part 1(A): schedule of materials requested from the Applicant to the RCMP (tribunal) 5

 Volume #1(C): Rule 317 Jurisprudence: the requirement of certified tribunal record (the “CTR”).....6

 Volume #1(C)(I): Unsearched Repositories; and the RCMP Tribunal (through Mr. Ball) did not rely on any exemption under s. 18 7

 Volume #1(C)(II): For sake of completeness: Review of Exempt PIB’s 8

 Volume #1(C)(I)(a): Conclusion on the inapplicability of Exempt Banks to the PII Access Request (March 11 2026) and this NOA for Judicial Review 8

 Volume #1(D): The Failure to Search by the RCMP 9

 VOLUME #1(D)(I): THE LEGAL TEST FOR RELEVANCE 11

 VOLUME #1(D)(II): APPLICATION OF *DOUZE V. CANADA* (CITIZENSHIP AND IMMIGRATION), 2010 FC 1086..... 11

 VOLUME #1(E): WHY NOTICES OF APPLICATION FOR MANDAMUS NECESSITATE AN EXPANDED INTERPRETATION OF THE CTR..... 11

VOLUME #1(F): JUDICIAL REVIEWS ARE DISTINCT FROM APPEALS – RULE 317 EXCLUSIVELY INVOKED WITHIN APPLICATIONS	12
VOLUME #1(G): THE PRECAUTIONARY PRINCIPLE AND THE RULE OF LAW PRECLUDE SPECULATION	12
VOLUME #1(H): THE DISCOVERY OF IMPROPER MOTIVE FACILITATES MEANINGFUL JUDICIAL REVIEW	12
VOLUME #1(I): THE DIFFERENTIAL LEGAL TEST FOR PROHIBITION UNDER RULE 317	13
Volume #1(H)(ii): Judicial Treatment of Air Passenger Rights	13
VOLUME #1(I): THE IMPERATIVE OF A FORMAL REQUEST	14
VOLUME #1(J): AUTHORITY FOR THE APPLICABILITY OF RULE 317 UNDER AN ATIA REVIEW	14
VOLUME #2: STATEMENT OF ISSUES	14
VOLUME #3: Legal Bases	17
VOLUME #3(A): THE OFFICE OF THE PRIVACY COMMISSIONER DETERMINES THE EXTENT OF THE RCMP’S STATUTORY DUTY AND PARAMOUNTCY OF CONTROL OVER MULTI-JURISDICTIONAL ENTRIES WITHIN THE CANADIAN POLICE INFORMATION CENTRE (THE “CPIC”).....	17
The Genesis of the Disclosed Intelligence:	17
Jurisprudential Analysis and Determinations of the OPCC	18
Analysis of Paragraph 8(2)(f) (Agreements with Foreign States for Law Enforcement):	18
The Finding of the Commissioner.....	18
Analysis of Paragraph 8(2)(a) (The Consistent Use Doctrine):	18
The Intransigence of the RCMP.....	19
Volume #3(A)(I): Summary of Jurisprudential Effect Regarding the Inputting of False or Inaccurate Data into CPIC by any Law Enforcement Apparatus	19
Paramount Stewardship of the Bilateral Agreement	20
The Imperative for Active Policy and Architectural Safeguards	20
Volume #3(B): The Novel Legal Issues Formulated for Adjudication	20
The First Novel and Untested Issue	20
The Second Novel and Untested Issue.....	20
Volume #3(C): The Jurisprudential Doctrine of Possession under the Federal Court Rules	21
The Definition of Possession in the Strict Context of Rule 317	21
The Tripartite Categorization of Possession	21
Volume #3(D): A Comparative Linguistic Analysis of the RCMP’s Decisions (The Halton Police Case vs. The McLean RCMP Proceeding).....	22
Volume #3(D)(I): The RCMP Decision in the Halton Police FIPPA Case	22
Volume #3(D)(II): The Distinctions Possessing Profound Legal Significance.....	23
VOLUME #4: without a search, correction rights cease to exist as legislated by parliament	24
Volume #4(A): Personal Information is akin to one’s ownership	24
Volume #4(B): Constructive and Joint Possession within Decentralized Database Architectures	25
Volume #4(C): The RCMP as the Paramount Custodian and Sovereign Administrative Steward	25
Volume #4(D): The Absolute Nullity of the “Third-Party Ownership” Defense	25

78 Volume #4(E): The Statutory Absurdity and the Frustration of Correction Rights under Subsection 12(2) of the Privacy Act.....	26
Volume #4(E)(I): The Paramountcy of the Initial Search and the “Meaningful Exercise” of Subsection 12(2)	26
Volume #4(E)(II): The Competing Interests and the Disclosure of Authorizing Identities (Paragraphs 3(g) and 3(i))	27
Volume #4(F): The Operational Exclusivity of “Off-Line Searches” and the Reductio ad Absurdum of Delegated Control.....	27
Volume #4(G): The Jurisprudence of “Control”: The Right of Demand and the Purposive Interpretation of Access Legislation.....	28
Volume #4(G)(I): The Broad, Liberal, and Purposive Interpretation of Control	28
Volume #4(G)(II): The Binding Precedent of Hale v. Ontario (Criminal Code Review Board)	28
Volume #4(G)(III): Application to the Present Factual Matrix: Offline Historical Data and Amended, Purged Records.....	29
Volume #4(H): The Jurisprudential Significance of the Unsolicited Inquiry into Specialized Policing Services and the Involuntary Institutional Admission of Centralized Systemic Manipulation.....	29
Volume #4(H)(I): The Inference and the “Data Trigger”	29
Volume #4(H)(II): The Proverbial “Pandora’s Box” and the MESCIUS / GrapeCity SDK Software Connection	30
Volume #4(H)(III): The Statutory Validation via the Treasury Board of Canada	30
Volume #4(H)(IV): The Indispensable Role of Regional Communications as Cross-Jurisdictional Intermediaries and the Implication of Mr. Matt Peggs	30
Volume #4(H)(V): The Crystallization of the Rule 317 Mandate Regarding Regional Communication Logs	31
Volume #4(H)(VI): The Evidentiary “Smoking Gun” and the Absurdity of the Delegated Deflection	31
Volume #5: Conclusion	31
I. The Tactical Avoidance of Paragraph 22(1)(a) and the Unmet Burden under Paragraph 22(1)(b).....	31
II. The High Threshold of “Injury to the Enforcement of Law” and the Rule of Law	32
III. The Temporal Ceiling of Investigative Exemptions and the Impact of R. v. Jordan	32
IV. The Fallacy of Informant Privilege in Relation to Public Court Records and Metadata.....	32
V. Ultra Vires Conduct, Fraudulent Manipulation, and the Limits of “Lawful Investigations”	33
VI. The Jurisdictional Legerdemain: Section 19(1)(d) and the Central Region Metamorphosis	33
VII. The Application of Equitable Maxims: Fraud Upon the Law and the Vitiating of Administrative Acts.....	34
VIII. The Fiduciary Duty of Disclosure and the Equitable Interest in Personal Information: The Application of McInerney v. MacDonald.....	35
Appendices	37
Appendix #1	38
Appendix #2:	39

PART 1: STATEMENT OF RULE 317 REQUEST AND OVERVIEW OF SEMINAL PRINCIPLES UNDER RULE 317 TO 319 OF THE *FCR*

1. Rule 317 of the *Federal Courts Rules* is titled “**Material from Tribunal**” and it authorizes a party to request material relevant to an “Application” (see: section 2 of the FCR, which means a proceeding referred to in rule 300) that is in the possession of a “Tribunal” (see: section 2 of the FCA and section 2 of the FCR) whose “Order” (see: section 2 of the FCR) is subject of the Application and not in possession of the party by serving on the Tribunal and filing a written request, identifying the material requested.
2. “Material” is not defined under the FCA or FCR, and the Interpretation Act is not of assistance in this regard but based on statutory interpretation principles, “Material” including that which can be reproduced and where it cannot, the original “Materials” to the Registry. The FCC Registry holds that “Original Material” in trust and it is returned to the Tribunal after the Applicant has been heard subject to the Court’s directions. In essence, it is entire collective body of documents, physical items, data, papers, things, records, information, Personal Information et al that are in the possession of the Tribunal.
3. Document discovery in our country varies from province to province and has varied over time with respect to whether the test is “materiality” or “relevance”. The latter is a much broader and lower standard for the threshold as to whether the “materials” must be disclosed to the other party(ies). In the context of an Application to the FCC, a document is relevant to an application for judicial review if it may affect the decision that the Court will make on the application. the relevance of the documents requested must necessarily be determined in relation to the grounds of review set forth in the originating notice and evidence filed by a moving party (see: *infra*, Douze, the Honourable Madam Justice Tremblay-Lamer explicitly adopted the instruction provided by the Court of Appeal in Canada (Human Rights Commission) v. Pathak, 1995 CanLII 3591 (FCA), [1995] 2 F.C. 455, 54 A.C.W.S. (3d) 1344 (C.A.) (Pathak), regarding the parameters of relevance under Rule 317). The reason for the finding as to evidence filed by the Applicant, along with the grounds in the Application, is encompassed by the 20 days after service of the Rule 317 request.
4. “Possession” is not defined under the FCA or FCR, and the Interpretation Act (Federal) does not assist either. This is much like the *Privacy Act*, along with the likes of the provincial privacy protection statutes that do not define the word “control”.
5. “Control” has been interpreted by the FCC and FCA since 1995 to encompass the following wherein Letourneau J.A., writing for the court, held as follows, at p. 245:

“The notion of control referred to in [the Act] is left undefined and unlimited. Parliament did not see fit to distinguish between ultimate and immediate, full and partial, transient and lasting, or “de jure” and “de facto” control. Had Parliament intended to qualify and restrict the notion of control to the power to dispose of the information, as suggested by the appellant, it could certainly have done so by limiting the citizen's right of access only to those documents that the government can dispose of or which are under the lasting or ultimate control of the government.”

(see: *Canada Post Corp. v. Canada (Minister of Public Works)* (1995), 1995 CanLII 3574 (FCA), 30 Admin. L.R. (2d) 242, [1995] 2 F.C. 110, cited with approval by the ONCA *Ontario Criminal Code Review Board v. Hale*, 1999 CanLII 3805 (ON CA)).

6. In Ontario Criminal Review Board, the tribunal therein was found to have control of backup audio tapes created by an independent contractor as the tribunal itself had the power to make a demand for those tapes. It was irrelevant whether they existed or not or what state they were in. The lack of a contractual provision compelling the court reporter to deliver the tapes does not negate the Board's control over them (para 35).
7. However, are “control” and “possession” ‘one and the same’? That question need not be answered herein.
8. Nonetheless, the types of possession include all the various types of possession including:
 - a. De facto;

- b. De jure;
 - c. Actual;
 - d. Constructive;
 - e. Sole;
 - f. Joint; and
 - g. Others (denoted *infra*).
9. As the Respondent RCMP Tribunal is required to transmit all material (which may not be Personal Information of the Applicant) to the FCC that is in its possession whose “Orders” (which include decisions or dispositions by the Tribunal) and that is not in the possession of the Applicant, the issue of whether the Respondent RCMP Tribunal has control of requested Personal Information becomes somewhat moot. Nonetheless, the RCMP’s constructive possession is unique herein because it is the custodian, controller and operator of the CPIC architecture so it has constructive possession, at the very least, of materials therein that are relevant to this JR Application before the FCC.
10. While certain decisions have and continue to focus on what was before or available to the Tribunal at the time of the decision, the scope of disclosure broadens significantly when an applicant has sought writs of mandamus, writs of prohibition and alleged conflicts of interest and bias (individual and institutional) et al (see: *infra* for the authorities in this regard).

PART 1(A): SCHEDULE OF MATERIALS REQUESTED FROM THE APPLICANT TO THE RCMP (TRIBUNAL)

11. With that segue, the Applicant is and has requested, upon service of this written request pursuant to Rule 317 of the Federal Courts Rules, SOR/98-106, Part -1 (the “*Federal Courts Rules*” or the “*FCR*”), materials, particularized *infra*, in possession of the RCMP tribunal (the “Tribunal”). The schedule of material sought herein is as follows:

SCHEDULE OF REQUESTED MATERIALS

Item Number	Category of Material	Specific Records and Metadata Requested
1	Access Request Administrative Files	The complete internal administrative file, tracking sheets, and analyst worksheets concerning <i>Privacy Act</i> file P-2025-16999 .
2	System Initialization Logs	The complete, unredacted system entry logs from the automated sequential registry system detailing the exact date, millisecond timestamp, and file initialization sequence that generated the prefix year “ 2025 ” for an access request delivered to the Respondent on March 11, 2026.
3	Executive and Inter-Directorate Communications	All electronic communications, emails, instant messages, memorandum chains, and briefing notes concerning the Applicant or file P-2025-16999 exchanged between Director Jeff Ball, Delegate Melissa Simpson, Director General Stéphane Brisson, Regional Commander Matt Peggs, or their authorized agents, and Chief of Staff Tanya Mirsky spanning April 1, 2026, to the present.
4	Internal Legal and Operational Advice	All legal or operational advice solicited or received internally regarding the Applicant’s statutory demand for access to the Canadian Police Information Centre (“ CPIC ”) Offline Historical Database metadata, including the Foundational Metadata Request and the Offline Historical Database Request.
5	Raw Forensic Mainframe Ledger Records	The raw, unredacted transaction logs, audit trails, and hexadecimal dumps residing within the secure CPIC Offline Historical Database associated with Personal Information Bank RCMP PPU 005 tied to the Applicant’s name, identifiers, or cross-referenced occurrence numbers (2024-2028093, 24-2082035, and Court File/Case ID 457197) spanning September 15, 2024, to December 31, 2024, inclusive.
6	Cryptographic Audit Trails	The complete cryptographic audit trails capturing all ADD , MODIFY , CLEAR , and CANCEL command strings, along with terminal identifiers, physical hardware addresses, Originating Agency Identifiers (“ ORIs ”), and unstructured narrative fields for each sequential transaction executed during the aforementioned temporal window.

	Forensic Metadata of Search Methodology	The complete electronic system logs generated by Operator NBOISVERT on April 14, 2026, at 07:35:43, detailing the complete input syntax, query parameters, and system constraints utilized to execute the front-facing “Q PERS+” and “Q CNP” live database queries.
8	Internal Directives and Exclusion Policies	Any internal directives, policy documents, or operational notes instructing the Access to Information and Privacy (“ATIP”) Branch analysts to omit an interrogation of the Offline Historical Database in response to the Applicant’s explicit, specialized request for historical data.
9	Trans-Directorate Processing Records	The complete, unredacted administrative processing file, tracking timelines, and internal analyst notes concerning the concurrent <i>Access to Information Act</i> (“ATIA”) request submitted by the Applicant, explicitly targeting the procurement, enterprise licensing, and National Technology Onboarding Program (“NTOP”) integration logs of the Mescius SDK / GrapeCity.Documents.PDF.6.0.2.0 developer engines within the CPIC infrastructure.
10	Automated File Linking Records	All internal processing records showing any administrative coordination, automated file linking, or database cross-referencing executed between the privacy division handling <i>Privacy Act</i> request P-2025-16999 and the information access branch processing the parallel ATIA files.
11	Software Exception Logs	Any software error tracking logs, system exception reports, or developer audit alerts generated by the core CPIC mainframe database management system involving database inquiries or structural PDF modifications tied to the Applicant’s biographical identifiers or transaction history.
12	Executive Suite Briefing Notes and Action Logs	All briefing notes, corporate risk assessments, institutional action logs, and communications generated by or sent to Commissioner Michael Duheme and Director General Stéphane Brisson regarding the Applicant’s personal information or file P-2025-16999.
13	Central Region Command Communications	All emails, letters, instant messages, and administrative directives sent or received by Assistant Commissioner Matthew Peggs (Central Region Command) concerning Police Case ID: 457197, the “Adult Common Information Package,” or the collection and retention of the Applicant’s property from September 15, 2024, to the present.
14	Third-Party Data Transfer Ingestion Ledgers	All cross-jurisdictional system logs showing the electronic receipt, intake vetting, and cryptographic mapping of data transferred from the Toronto Police Service (TPS) or Ontario Court of Justice (OCJ) to the RCMP infrastructure involving the Applicant’s biographical profiles.
15	Primary Statutory Charging Instruments	A certified copy of the Criminal Code Form 2 “Information” and/or Criminal Code Form 4 “Indictment” purportedly generated, indexed, or uploaded into federal tracking streams regarding the Applicant’s underlying file.
16	Core Courthouse Intake Endorsements	A certified copy of the Intake Court Endorsement represented on Page 3 of 5 within the disputed “False Information Package,” capturing any handwriting, initials, or automated metadata strings applied during processing.
17	Originating Judicial Authorizations	A certified copy of the alleged warrant in the first instance executed, tracked, or registered within the CPIC network in relation to the Applicant’s identifiers.
18	Comprehensive Judicial and Executive Orders	Any and all ancillary orders, determinations, statutory authorizations, variances, or judicial directions issued by a Court of competent jurisdiction or a federal board concerning the collection, retrieval, manipulation, or preservation of the Applicant’s personal information or physical property.

VOLUME #1(C): RULE 317 JURISPRUDENCE: THE REQUIREMENT OF CERTIFIED TRIBUNAL RECORD (THE “CTR”)

12. Consistent with settled jurisprudence regarding the open court principle (the “**Open Court Principle**”) entrenched within section 2(b) of the *Canadian Charter of Rights and Freedoms* (the “**Charter**”), informations and indictments (the “**Informations**” and “**Indictments**”) are unequivocally treated as public court documents upon the issuance of a process and/or the service of a Criminal Code Summons or the execution of a Criminal Code Form 7 Arrest Warrant. Furthermore, any corresponding endorsements by a judicial officer (“**Endorsements**”) thereto are to be made available upon formal request by an accused party (devoid of prescribed fees) or the public writ large, subject to the prescribed fee schedule delineated within *Regulation 158/03*.
13. Analogously, within the taxation context, it has been established that the Canada Revenue Agency, pursuant to a request under *Rule 317* of the *FCR*, forwarded a certified copy of an information (the “**Information**”) to the

82 Registry. Said document was subsequently treated by the Registry as a public document, with a copy concurrently remitted to the applicant's counsel: *Rémillard v. Canada (National Revenue)*, 2020 FC 1061 at para 5.

14. Documentation transmitted pursuant to *Rule 318* of the *FCR* is strictly incorporated into the receiving Court's official records and is governed *ipso facto* by the **Open Court Principle** (see: *Rémillard*, at paras 25–26 and 37–38). Sections 23 and 26 of the *FCR* mandate that the Court file and its annexes be treated as publicly accessible, subject exclusively to statutory confidentiality or specific judicial sealing orders.
15. The procedural mechanism outlined in *Rules 317* and *318* of the *FCR* is strictly operational and non-exploratory; its function is solely to transition relevant materials into the possession of the Registry, distinguishable from private discoveries which are executed beyond the purview of the Court file (see: *Rémillard*, at paras 57–59 and 65–66). Private discoveries are governed by the implied undertaking rule subject to questions from discovery being read into the court record by affidavit or at a hearing.
16. Should the **Respondent RCMP Tribunal** argue that the applicant is utilizing *Rule 317* as an impermissible exploratory discovery mechanism, such an assertion is preemptively defeated by the fact that the requested records constitute foundational administrative documents that inherently form the basis of the tribunal's jurisdiction and subsequent (or omitted) actions.
17. The protections afforded under section 8 of the *Charter* are rendered inapplicable *in limine*, as no reasonable expectation of privacy ("REOP") can legally persist subsequent to an applicant requisitioning transmission pursuant to *Rule 317* of the *FCR* (see: *Rémillard*, at paras 163–165).
18. Generally, *Rule 317* of the *FCR* encompasses exclusively the material that was available to the administrative decision-maker at the time the decision was rendered (at paras 23, 39, and 41–42). However, a substantially broader scope of disclosure is mandated in circumstances where procedural fairness, reasonable apprehension of bias, or analogous equitable grounds are explicitly contained within the Notice of Application and supported by a cogent evidentiary foundation: *Lill v. Canada*, 2023 FC 1364. Such grounds are unequivocally established herein by the notice of application (the "**JR NOA**") filed by the applicant (the "**Applicant**").

Volume #1(C)(I): Unsearched Repositories; and the RCMP Tribunal (through Mr. Ball) did not rely on any exemption under s. 18

19. The circumstances present herein ostensibly construct a paradox; however, a rigorous legal examination reveals that such a paradox is illusory, even if it is averred that the Royal Canadian Mounted Police (the "**RCMP**") neglected to search the requisite repositories for foundational metadata (the "**Foundational Metadata**") and the offline historical database (the "**Offline Historical Database**") (collectively, the "**Unsearched Repositories**"). The jurisprudential test dictates that the determination rests upon what material was legally available to the decision-maker at the material time.

Volume #1(C)(I)(a): The Misstatement of Law in the RCMP Tribunal Decision: "Privacy Act does not authorize search of files...belonging to other police forces"

20. The failure of the RCMP, as admitted predicated upon its representation in the April 27, 2026, letter communicated to the Applicant that the "The *Privacy Act* does not authorize the RCMP to search files....belonging to other police forces" (see: page 1 of 6, paragraph three).
21. "Files" is not defined under the *Privacy Act* but it is mentioned six (6) times under the *Privacy Act* which are:
 - a. EXEMPTIONS
 - i. Exempt Banks
 1. Governor in Council may designate exempt banks
 - a. Subsection 18(1): The Governor in Council may, by order, designate as exempt banks certain personal information banks that contain **files** all of which consist predominantly of personal information described in section 21 or 22.
 2. Contents of order
 - a. Clause 18(3)(b): (3) An order made under subsection (1) shall specify

- i. (b) where a personal information bank is designated that contains files that consist predominantly of personal information described in subparagraph 22(1)(a)(ii), the law concerned.
- b. The auto population of “files” (three to six) involve the review of exempt banks by the Privacy Commissioner of Canada into those exempt banks.

Volume #1(C)(I)(a)(i): Conclusion on the misstatement of law in this context

22. The Respondent RCMP did NOT claim an exemption under section 18(2) of the *Privacy Act* which states for sake of convenience:

“Disclosure may be refused

(2) The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that is contained in a personal information bank designated as an exempt bank under subsection (1).”

23. The Head of the Government Institution is that of Commissioner Mr. Michael Duheme.

Volume #1(C)(II): For sake of completeness: Review of Exempt PIB's

24. Nonetheless, the exempt PIB's are:

a. Department of National Defence Exempt Bank:

- i. Exempt Personal Information Bank Order, No. 5 (ND), SOR/85-38, Part -1: The personal information bank under the control of the Department of National Defence containing the Security and Intelligence Information files No. ND-P70 is hereby designated as an exempt bank on the basis of section 21 of the *Privacy Act*;

b. Criminal Operational Intelligence Records (tied to Personal Information contained at subparagraph 22(1)(a)(ii))

- i. Exempt Personal Information Bank Order, No. 13 (RCMP), SOR/90-149, Part -1: Criminal Operational Intelligence Records, No. CMP/P-PU-015, a personal information bank under the control of the Royal Canadian Mounted Police, is hereby designated as an exempt bank on the basis of section 22 of the *Privacy Act*.
 - 1. or the purposes of paragraph 18(3)(b) of the *Privacy Act*, the laws concerned, in relation to those files that are contained in the exempt bank referred to in section 2 that consist predominantly of personal information described in subparagraph 22(1)(a)(ii) of that Act, are the Criminal Code, the Customs Act, the Excise Act, the Food and Drugs Act, the Immigration and Refugee Protection Act, the Income Tax Act, the Controlled Drugs and Substances Act and the Foreign Interference and Security of Information Act.

c. CSIS Exempt Bank:

- i. Exempt Personal Information Bank Order, No. 14 (CSIS), SOR/92-688, Part -1

d. Exempt Personal Information Bank Order, No. 25 (RCMP), SOR/93-272, Part -1,

- i. For the purposes of paragraph 18(3)(b) of the *Privacy Act*, the laws concerned, in relation to those files that are contained in the exempt bank referred to in section 2 that consist predominantly of personal information described in subparagraph 22(1)(a)(ii) of that Act, are the Criminal Code, the Foreign Interference and Security of Information Act, the Security Offences Act, the Royal Canadian Mounted Police Act and the Canadian Security Intelligence Service Act.

Volume #1(C)(I)(a): Conclusion on the inapplicability of Exempt Banks to the PII Access Request (March 11 2026) and this NOA for Judicial Review

84 25. Leaving aside that the RCMP solely focused on “information” and not “Personal Information”, it explicitly relied in its decision on April 27, 2026, wherein it stated:

“Enclosed is a copy of all of the information to which you are entitled. Please note that some of the information has been exempted pursuant to sections 19(1)(d), 22(1)(b) and 26 of the Act”

26. There is not a single solitary mention of section 18 therein. Ergo, the RCMP Tribunal was not relying on “files contained in a PIB being exempt from disclosure let alone searching.
27. For completeness purposes and to avoid unnecessary and frivolous objections by the RCMP regarding its obligation to transmit a complete, accurate, and full CTR to the FCC and the Applicant, there is also not a single mention of n subparagraph 22(1)(a)(ii). Ergo, any reliance by the RCMP Tribunal on not being able to search files or disclose information (sic) belonging to other police forces is not relevant herein.
28. Hence, the Applicant’s judicial review Notice of Application (Form 301) seeking writs of mandamus and prohibition as the relevant Personal Information sought, of which the Applicant did not seek that which was produced in the three page heavily redacted document accompanying the April 27 decision, has not been searched for.
29. Irrespective of the same, there would remain a judicial review independent of that aforementioned mandamus issue, predicated on the requirement (statutory and common law) for the Head of the Government Institution to consider whether to make a public interest disclosure regarding the manipulation of a “Criminal Code Information Package” into a False Information Package which is unprecedented in Canadian legal history (see: R. v. Scherzer and R. v. Hamilton did not contained falsification of the Criminal Code Information Packages but the falsification of underlying legal bases and notes per se; and R. v. Silva (Quebec) involved the stealing of a Justice of the Peace’s stamp on account of “noble cause corruption” by a young Police Officer in Mr. Jolly as the public was in a state of terror with a notorious gang connected hitman in Mr. Silva).

VOLUME #1(D): THE FAILURE TO SEARCH BY THE RCMP

30. In light of the above uncontroverted syllogism and the sophisms by the RCMP, the *Privacy Act* not only authorizes but obligates the Government Institution to search for Personal Information requested (not “files”) within the scope of an access request whether it is in a Personal Information Bank (a “PIB”) and has been used, is being used or is available for use for an administrative purpose or is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual (see: section 10 of the *Privacy Act*).
31. However, the word “files” is utilized under some of the attendant regulations under the *Privacy Act* where certain PIB’s, pursuant to ss. 18(1) of the *Privacy Act*, making certain PIB’s exempt from search and disclosure.
32. The Applicant requested access to the PIB known as PPU 005 and it is not an exempt PIB. Moreover, the PII Access Request (March 11 2026) was not a request for “files” per se but for Personal Information contained in the PIB (PPU 005) and searches of Foundational Metadata and Offline Historical Database with respect to an executed arrest warrant including any original and amended data therein contained his Personal Information. But for the name of the judicial officer who in fact issued an endorsement including an Arrest Warrant (Criminal Code Form 7) all of the Personal Information therein would be on its face and de facto only involving him per se. In relation to the name of the judicial officer who issued the endorsement (dubbed an “Intake Court Endorsement”) “warrant in the first”, the federal statutory Personal Information definition under section 3(i) (see: means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing...(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual). This is also consistent with the judicial interpretation of Personal Information, and the required interpretation as follows:
 - a. Drawing from jurisprudence in the federal public sector, the definition of personal information must be given a broad and expansive interpretation (Dagg v. Canada (Minister of Finance), [1997] 2 S.C.R., dissenting, 403 at para 68; Canada (Information Commissioner) v. Canada (Transportation Accident

Investigation and Safety Board), 2006 FCA 157; Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police), [2003] 1 S.C.R. 66, 2003 SCC 8, at para 23).

- b. Personal information is information “about” an identifiable individual. “About” means that the information is not just the subject of something but also relates to or concerns the subject (Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157).
- c. Information will be about an “identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information (Gordon v. Canada (Health), 2008 FC 258 (CanLII)).Footnote1 Information need not be recorded for it to constitute personal information. It is sufficient that the information be about an identifiable individual even if the information is not in a recorded form, such as oral conversations, biological samples and real time video surveillance. While the absence of a recording may go to the issue of collection, it does not change the fact that the information is personal information (Morgan v. Alta Flights Inc. (2006) FCA 121, affirming (2005) FC 421).
- d. The same information can be personal to more than one individual, where, for example, it contains the views of one individual about another individual, or where the same information reveals something about two identifiable individuals (Wyndowe v. Rousseau, 2008 FCA 39 (CanLII)).
- e. Information will still be personal information even if it is publicly available within the meaning of the regulations,Footnote2 and is exempt from applicable consent requirements (Englander v. TELUS Communications Inc., 2004 FCA 387 (CanLII)).
- f. Subjective information about an individual may still be personal information even if it is not necessarily accurate (Lawson v. Accusearch Inc. 2007 FC 125).

33. The general principles overall are:

- a. Privacy Rights’ Purpose:
 - i. privacy rights are designed to protect the privacy of individuals with respect to Personal Information held by government institutions and to provide individuals with a right of access to that information;
- b. *Privacy Act*:
 - i. quasi-constitutional;
- c. Exceptions from an individual applicant’s access rights – interpreted narrowly:
 - i. in Lavigne v. Canada (Office of the COMMISSIONER of Official Languages), 2002 SCC 53 (CanLII), [2002] 2 S.C.R. 773, Gonthier J. observed that exceptions from the rights set out in the act should be interpreted narrowly, with any doubt resolved in favour of preserving the right;
- d. Burden of proof:
 - i. the burden of persuasion on the person asserting the exception (at paras. 30-31 of Lavigne);
- e. Privacy Rights only compromised when there is a compelling state interest for doing so:
 - i. in Dagg v. Canada (Minister of Finance), 1997 CanLII 358 (SCC), [1997] 2 S.C.R. 403, the SCC articulated the governing principles of privacy law including that protection of privacy is a fundamental value in modern democracies and is enshrined in ss. 7 and 8 of the Charter, and privacy rights are to be compromised only where there is a compelling state interest for doing so (at paras. 65, 66, 71)

34. It is axiomatic that the RCMP is also subject to the Charter pursuant to section 32 of the Charter.

35. *Lex non cogit ad impossibilia* (the law does not compel the impossible) cannot shield the RCMP where the material was, in fact, extant and obtainable.

36. Inasmuch as Informations, Indictments, and any associated endorsements—including but not limited to arrest warrants—are fundamental components governed by the Open Court Principle (which concurrently protects the rights of listeners pursuant to section 2(b) of the *Charter*), the failure of an originating courthouse or originating court office to produce said documents is immaterial. The RCMP possesses the requisite statutory authority to procure such documentation and is legally obligated to do so pursuant to *Rule 317*. From a policy perspective, the Federal Court of Canada and the RCMP are absolutely bound to discharge this requirement to preserve the integrity

of the rule of law (the “**Rule of Law**”). Invoking Herbert Broom’s maxim, *omnia praesumuntur rite et solemniter esse acta* (all acts are presumed to have been done rightly and regularly), the public is entitled to presume the RCMP will fulfill its legal duties to procure necessary records.

37. Copies of the aforementioned Informations, Indictments, and corresponding endorsements, alongside copies of arrest warrants—as represented by the Toronto Police Service (the “**TPS**” or the “**Arresting Police Division**”) to have been in their possession—are strictly relevant to the JR NOA, specifically concerning the prerogative relief sought in the nature of mandamus and prohibition.
38. Furthermore, the compulsory transmission of these documents will categorically elucidate whether the RCMP was operating *mala fides* by intentionally breaching a public legal duty, or, in the alternative, operating negligently by breaching a public legal duty in a profoundly derelict manner. This evidentiary disclosure is paramount as it directly dictates the quantum and nature of the consequential relief to be awarded.

VOLUME #1(D)(I): THE LEGAL TEST FOR RELEVANCE

39. For the strict purposes of *Rule 317* of the *FCR*, a document is deemed relevant to an application for judicial review if it possesses the capacity to affect the ultimate decision that the Court will render on the application (see: *Douze v. Canada (Citizenship and Immigration)*, 2010 FC 1086 at para 19); *Boudreau v. Canada (Revenue Agency)*, 2022 FC 792 (CanLII), at para 16.

VOLUME #1(D)(II): APPLICATION OF DOUZE V. CANADA (CITIZENSHIP AND IMMIGRATION), 2010 FC 1086

40. In *Douze*, the Honourable Madam Justice Tremblay-Lamer explicitly adopted the instruction provided by the Court of Appeal in *Canada (Human Rights Commission) v. Pathak*, 1995 CanLII 3591 (FCA), [1995] 2 F.C. 455, 54 A.C.W.S. (3d) 1344 (C.A.) (*Pathak*), regarding the parameters of relevance under *Rule 317*:

“A document is relevant to an application for judicial review if it may affect the decision that the Court will make on the application. As the decision of the Court will deal only with the grounds of review invoked by the **Respondent**, the relevance of the documents requested must necessarily be determined in relation to the grounds of review set forth in the originating notice of motion and the affidavit filed by the **Respondent**. (at para. 10)”

41. The ratio decidendi established in *Douze* has been consistently affirmed across numerous subsequent decisions, including:
 - a. *Chopra v. Canada (Public Safety and Emergency Preparedness)*, 2026 CanLII 18896 (FC), at para 10;
 - b. *John Doe I v. Canada (Attorney General)*, 2024 FC 1024, wherein Mr. Justice Diner articulated:
 - i. It is well established that the test for relevance under *Rule 17* is synonymous with that under *Rule 317* of the *FCR* (*Abu* at paras 28 and 43, citing *Douze v. Canada (Citizenship and Immigration)*, 2010 FC 1086 at para 19 and *Nguesso v. Canada (Citizenship and Immigration)*, 2015 FC 102 at para 94). Ergo, a document is classified as “relevant” in this specific context where it “may affect the decision that the Court will make on the application,” determined strictly in relation to “the grounds of review and any affidavit filed in support of the application” (*Abu* at para 43).
 - c. The relevance of the material requisitioned under *Rule 317* of the *FCR* is the determinative factor. For the purposes of *Rule 317*, a document is relevant to an application for judicial review if it may affect the decision that the Court will ultimately make on the application (see: *Douze v. Canada (Citizenship and Immigration)*, 2010 FC 1086 at para 19; *Boudreau v. Canada (Revenue Agency)*, 2022 FC 792 (CanLII), at para 16; and
 - d. Various other binding appellate and trial-level jurisprudence.

VOLUME #1(E): WHY NOTICES OF APPLICATION FOR MANDAMUS NECESSITATE AN EXPANDED INTERPRETATION OF THE CTR

42. In *Abu v. Canada (Citizenship and Immigration)*, 2021 FC 1031, Mr. Justice Norris articulated the distinguished threshold for mandamus applications as follows:
43. “I begin by noting that one of the usual indicators of relevance in the judicial review context—was the document or information before the tribunal when it made its decision?—does not apply in a mandamus application because it is the failure or refusal of the tribunal to make a decision that has prompted the application in the first place. While this is a sound indicator of relevance when a decision is being reviewed, it is not exhaustive of the concept of relevance in the judicial review context generally. It is well established that the test for relevance in the context of the production of a CTR is whether a document in the possession or control of the tribunal in question “may affect the decision that the Court will make on the application” (*Canada (Human Rights Commission) v. Pathak*, 1995 CanLII 3591 (FCA), [1995] 2 F.C. 455 [at page 460], 1995 CarswellNat 666, at paragraph 10 (WL Can.) (C.A.)).

VOLUME #1(F): JUDICIAL REVIEWS ARE DISTINCT FROM APPEALS – RULE 317 EXCLUSIVELY INVOKED WITHIN APPLICATIONS

44. Mirroring the explicit statutory language of the *FCR*, *Beniey v. Canada (Border Services Agency)*, 2024 FC 972 unequivocally affirmed that *Rule 317* applies exclusively to judicial reviews conducted pursuant to the *Federal Courts Act* (the “**FCA**”) and is inapplicable to applications instituted under separate statutory regimes, such as the *Official Languages Act*, RSC 1985, c 31 (4th supp) (the “**OLA**”). This principle was previously crystallized in *Lavigne v. Canada Post Corporation*, 2009 FC 756, wherein it was determined at paragraph 16 that *Rule 317* cannot be invoked against the Commissioner within an application commenced under section 77 of the *OLA*, as the Commissioner’s decision is not formally under review.
45. By logical extrapolation, applications commenced pursuant to section 41 of the *Privacy Act* or under the *Access to Information Act* (the “**ATIA**”) do not constitute judicial reviews under the *FCA* and therefore do not govern the specific issues herein, wherein a tribunal (the “**RCMP Tribunal**”) has explicitly conceded a failure to search delineated repositories.

VOLUME #1(G): THE PRECAUTIONARY PRINCIPLE AND THE RULE OF LAW PRECLUDE SPECULATION

46. As explicated by the Federal Court of Appeal in *Canadian Copyright Licensing Agency (Access Copyright) v. Alberta*, 2015 FCA 268 [*Access Copyright*] (per Stratas JA at para 15):

“Parties before the administrative decision maker will often have in their possession all of the material the administrative decision maker considered in making its decision. But not always. And sometimes parties may be unsure whether they do. Sometimes they wish to confirm exactly what the administrative decision maker actually considered in making its decision. Rule 317 of the Federal Courts Rules provides a means by which parties can achieve those ends

(see also: *Friends of the Earth Canada v. Canada (Attorney General)*, 2023 FC 1438 (CanLII), at para 9).

47. Herein, the Applicant less than little: he has nothing.

VOLUME #1(H): THE DISCOVERY OF IMPROPER MOTIVE FACILITATES MEANINGFUL JUDICIAL REVIEW

48. It is an accepted legal tenet that the certified record and its surrounding context may unveil whether an administrative decision was predicated upon an improper motive or driven by alternative impermissible rationales (*Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65 at para 137).

88 49. In the event that the reviewing court is deprived of the evidentiary foundation relied upon by the administrative decision-maker, the detection of a reviewable error may be rendered an impossibility (*Access Copyright* at para 14). The paramount and overarching consideration is whether the requested disclosure will permit a meaningful and substantive judicial review of the impugned decision (*GCT Canada Limited Partnership v. Vancouver Fraser Port Authority*, 2021 FC 624 at para 26).

VOLUME #1(I): THE DIFFERENTIAL LEGAL TEST FOR PROHIBITION UNDER RULE 317

50. In *Air Passenger Rights v. Canada (Attorney General)*, 2021 FCA 201, Associate Justice Gleason of the Federal Court of Appeal delineated at paragraph 21:

“[21] Turning to the first of the foregoing assertions, as the applicant rightly notes, the breadth of materials that are subject to disclosure under Rules 317 and 318 of the Federal Courts Rules is broader where bias or breach of procedural fairness is alleged, particularly where, as here, relief in the nature of prohibition is sought. In such circumstances, disclosure is not limited to the materials that were before the tribunal when an order was made. Rather, where such arguments are raised, documents in the possession, control or power of a tribunal that are relevant to the allegations of bias or breach of procedural fairness are subject to disclosure.

51. Indeed, were it otherwise, this Court would be deprived of evidence necessary for the disposition of an applicant’s claims of bias or breach of procedural fairness and the availability of relief in the nature of prohibition would be largely illusory: see, e.g., *Humane Society of Canada Foundation v. Canada (National Revenue)*, 2018 FCA 66, 289 A.C.W.S. (3d) 875 at paras. 5-6; *Gagliano v. Canada (Commission of Inquiry into the Sponsorship Program & Advertising Activities)*, 2006 FC 720, 293 F.T.R. 108 at para. 50, aff’d 2007 FCA 131; *Majeed v. Canada (Minister of Employment & Immigration)*, 1997 CarswellNat 1693, [1993] F.C.J. No. 908 (F.C.T.D.) at para. 3, aff’d [1994] F.C.J. No. 1401 (F.C.A.). Thus, the first assertion advanced by the AGC as to the scope of permitted disclosure under Rules 317 and 318 is without merit.”
52. Allegations encompassing bias and profound breaches of procedural fairness have been meticulously pleaded and are comprehensively encapsulated within the operative iteration of the application record (the “**Application Record**”).
53. Concurrently, prerogative relief in the form of a writ of prohibition (the “**Writ of Prohibition**”) is actively sought by the Applicant. Herbert Broom’s maxim *ubi jus ibi remedium* (where there is a right, there is a remedy) dictates that the Court must possess the requisite evidentiary record to formulate such a remedy.
54. *Ipso facto*, given that the remedies of mandamus and prohibition are concurrently pursued, the restrictive test evaluating solely the materials available at the precise moment of the RCMP Tribunal’s decision is fundamentally inapplicable. While the Applicant submits that this narrower threshold would nonetheless be satisfied, the prevailing appellate jurisprudence unequivocally binds the Court, by virtue of vertical *stare decisis*, to compel the RCMP Tribunal to transmit the expansive array of materials in certified format to both the Federal Court and the Applicant.
55. Should it be argued that the broader array of documents falls outside the technical “control” of the decision-maker because they were not explicitly reviewed, such an argument constitutes a logical fallacy. The jurisprudence explicitly overrides this limitation where bad faith, bias, or procedural fairness are pleaded, transferring the metric of discoverability from “what was reviewed” to “what may affect the Court’s disposition of the fairness allegations.”

Volume #1(H)(ii): Judicial Treatment of Air Passenger Rights

56. When allegations of bias or breaches of procedural fairness are advanced within a notice of application, the legally permissible scope of materials subject to mandatory disclosure under *Rules 317* and *318* is substantially broadened. This augmented scope is a jurisprudential imperative designed to guarantee that the reviewing Court is vested with the requisite evidentiary matrix to judiciously dispose of these claims (*Air Passenger Rights v. Canada (Attorney*

General), 2021 FCA 201 at para 21). Consequently, where bias or a breach of procedural fairness is averred, all documentation possessing relevance to such allegations must be subject to compulsory disclosure (*Ron W Cameron Charitable Foundation v. Canada (National Revenue)*, 2023 FCA 175 [Ron W Cameron] at para 26); *Delisle (Kannabis Shop) v. Kahnawake Cannabis Control Board*, 2026 CanLII 14519 (FC), at para 13.

57. In circumstances where an allegation of a breach of procedural fairness, a reasonable apprehension of bias, or actual bias is asserted within a notice of application or notice of appeal, the orthodox convention restricting production to relevant material physically before the decision-maker is invariably expanded. Supplemental documents demonstrating relevance to the specific allegation become subject to production: *Humane Society of Canada Foundation v. Canada (National Revenue)*, 2018 FCA 66 at para 6 (*Humane Society*); *Air Passenger Rights v. Canada (Attorney General)*, 2021 FCA 201 at para 21 (*Air Passenger Rights 2021*). The Federal Court of Appeal definitively codified this expanded obligation in *Air Passenger Rights 2021* (see: paragraph 21); *Jewish National Fund of Canada Inc. v. Canada (National Revenue)*, 2025 FCA 114 (CanLII), at para 13.
58. Furthermore, averments detailing discrimination on the basis of disability or egregious breaches of procedural fairness serve as sufficient independent catalysts to warrant expanded disclosure pursuant to *Rule 317*. When such arguments are substantively raised, documents demonstrating relevance to the allegations—irrespective of whether they were physically reviewed by the decision-maker—are strictly subject to disclosure (*Air Passenger Rights v. Canada (Attorney General)*, 2021 FCA 201 at para 21); *Ron W. Cameron Charitable Foundation v. Canada (National Revenue)*, 2023 FCA 175 (CanLII), at para 26. Application of this law dictates that the Applicant’s pleadings of specific biases mandate production of the entire foundational record to assess the veracity of the tribunal’s omissions.

VOLUME #1(I): THE IMPERATIVE OF A FORMAL REQUEST

59. In *Wheeldon v. Canada (Attorney General)*, 2012 FC 355, Mr. Justice Phelan articulated the absolute necessity of tendering a formal written request, notwithstanding the absence of a strictly prescribed statutory form. The Court observed the fatal deficiency when an applicant sought supplementary information without formalizing the requisite demand pursuant to *Rule 317* of the *FCR*. Specifically, the **Respondent** formally notified the Court that it refrained from producing the entirety of the material pertaining to the impugned decision strictly because the procedural formality of *Rule 317* was not strictly adhered to by the applicant: *Wheeldon v. Canada (Attorney General)*, 2012 FC 355 (CanLII), at para 15.

VOLUME #1(J): AUTHORITY FOR THE APPLICABILITY OF RULE 317 UNDER AN ATIA REVIEW

60. The standard of correctness is universally applicable in determining the applicability of *Rule 317* to a section 44 review under the *ATIA*, as such an inquiry constitutes a pure question of law (at para 11). A review instituted under section 44 retains the fundamental character of a judicial review, as it invariably scrutinizes the administrative decision-maker’s ultimate determination regarding the disclosure of records (at paras 14–15 and 26). The decision itself embodies “the subject of the application,” thereby satisfying the strict statutory language and threshold requirements encapsulated within *Rule 317* (at para 15): *Preventous Collaborative Health v. Canada (Health)*, 2021 FC 253. By applying this doctrine to the present facts, the failure to produce the required documents transforms the administrative inaction into the direct subject matter of the application, thereby triggering the compulsory production requirements of *Rule 317*.

VOLUME #2: STATEMENT OF ISSUES

61. The issues are provided herein to ensure that this proceeding is determined in a manner that is just, most expeditious and least expensive outcome of every proceeding with consideration being given to the principle of proportionality, including consideration of the proceeding’s complexity, the importance of the issues involved and the amount in

dispute (see: rule 3(a) and (b)) and in the event that there is an objection to some of the material requested the Court has the benefit of the relevant issues:

- a. **Definitional Parameters under the *Privacy Act*:** Predicated upon the assertion that the RCMP purported to exercise jurisdiction and powers pursuant to the *Privacy Act*, RSC 1985, c P-21—an Act of Parliament—what is the proper jurisprudential and statutory interpretation of the following operative terms within the context of the present application: i. “Order”; ii. “Material”; and iii. “Relevant”.
- b. **The Legal Doctrine of Possession:** Given the absence of an explicit statutory definition of “possession” within the *Federal Courts Act*, RSC 1985, c F-7, the *FCR*, or the *Interpretation Act*, RSC 1985, c I-21, what is the prevailing common law and jurisprudential definition of “possession” specifically as it applies to the production of records in applications before the Federal Court of Canada?
- c. **Expanded Scope of Disclosure (*Rules 317 and 318*):** To what extent is the legally permissible scope of mandatory disclosure, compelled under *Rules 317 and 318* of the *FCR*, augmented and expanded in circumstances where an applicant explicitly pleads and seeks relief based upon: i. A Writ of Mandamus; ii. A Writ of Prohibition; iii. The reasonable apprehension of bias, existence of a conflict of interest, institutional lack of independence, and/or lack of impartiality; and/or iv. Egregious breaches of the principles of procedural fairness;
- d. **Subsection 19(1)(d) misguided yet revealing reference:**
 - i. **Principal Issue for Determination:**
 1. Whether the invocation of the statutory exemption enumerated within subsection 19(1)(d) of the *Privacy Act* operates, *sub silentio*, as an admission of the originating law enforcement agency status of the federal constabulary; and furthermore, whether the totality of the circumstances encompassing the disposition of the subject chattels, the internal reorganization of the federal institution, the alleged documentary irregularities, and the anomalous remuneration of court personnel furnishes a triable inference of systemic procedural manipulation or institutional impropriety.
 - ii. **Particularized Sub-Issues:**
 1. a) **Disposition of Chattels and Warrant Protocols:** Whether the ostensibly irregular handling of the subject chattels by the municipal police service—specifically, the uncatalogued sequestration thereof within a provisional repository, compounded by ensuing contradictory representations concerning the purported transfer to the Property Evidence Management Unit, and conjoined with the failure to produce an executory warrant of arrest—furnishes sufficient evidentiary weight to support the inference that the federal constabulary, rather than the municipal entity, operated as the primary or originating agency, thereby providing the foundational rationale for the invocation of subsection 19(1)(d).
 - iii. b) **Institutional Reorganization as Statutory Circumvention:**
 1. Whether the redesignation of the federal constabulary’s “O” Division to the “Central Region,” whilst remaining under the continuous administrative authority of the presiding Regional Commander, is liable to be construed as a deliberate structural realignment executed with the specific intent of satisfying the jurisdictional phrasing contained within subsection 19(1)(d) (“regional government established by... an Institution of such a government”), thereby operating as an artifice to insulate agency records from mandatory disclosure.
 - iv. c) **Inherent Prejudice to the Governmental Institution (understandable yet non-legal justification for non-disclosure):**
 1. Whether, by invoking the aforementioned statutory exemption, it is implicitly conceded by the federal institution that the execution of a comprehensive search would invariably yield specific foundational metadata—comprising the Originating Agency Identifier (ORI),

particulars of the issuing tribunal, and the identity of the presiding judicial officer—which would conclusively establish the agency’s direct involvement, thereby occasioning inherent prejudice to the institution.

- v. d) **Alleged Documentary Alteration and Software Exploitation:**
 - 1. In consideration of the publicly documented technical vulnerabilities inherent to the software framework identified as GrapeCity.Documents.PDF 6.0.2.0, whether a balance of probabilities suggests that said framework was utilized to effectuate a systematic obfuscation or manipulation of the primary evidentiary record, thereby converting the Authentic Information Package into the False Information Package.
- vi. e) **Procedural Irregularities Indicative of Federal Agency Practices:**
 - 1. Whether the particularized errors and omissions identifiable within the False Information Package bear a greater indicia of alignment with the administrative practices of a federal agency operating within a regional framework—an entity arguably lacking the high-volume, routine process-issuing expertise characteristic of municipal police forces—than with those of the municipal police service itself.
- vii. f) **Probative Inferences Regarding Personnel Remuneration:**
 - 1. What juridical inferences may be properly drawn from the sudden and material escalation in the remuneration of the named Court Officer, propelling said individual to a publicly disclosed threshold of elevated compensation in the year 2025, in immediate sequence to the allegedly unauthorized utilization of her identity as an informant—an averment she purportedly could not traverse upon confrontation. Furthermore, whether this temporal pattern of compensation raises a triable issue as to the possibility that such financial advancement was furnished as a clandestine commission or improper inducement to secure acquiescence to the aforementioned inclusion of her identity.
- e. **Subsection 22, “Law Enforcement and Investigation”:** the absence of section 22(1)(a) but the inclusion of 22(1)(b) misguided yet enlightening, illuminating and informative reference:
 - i. The central issues in this application for judicial review concern the Royal Canadian Mounted Police’s (the “RCMP”) unlawful withholding of Foundational Metadata and Offline Historical Database records under the *Privacy Act*, R.S.C. 1985, c. P-21 (the “*Act*”). Specifically, the issues are framed as follows:
 - 1. **The Jurisdictional Misdirection:** Did the RCMP ATIP Branch err in law by declining to invoke the specific exemption under paragraph 22(1)(a) of the *Act*—which would require identifying itself as an “investigative body” under the *Privacy Regulations*—and instead relying on paragraph 22(1)(b), thereby assuming an evidentiary burden of proving “injury” that it cannot legally or factually satisfy?
 - 2. **The Failure to Establish a Reasonable Expectation of Injury:** Can the disclosure of historical, transactional, or administrative metadata (including CPIC logs, Foundational Metadata, and offline database entries) be reasonably expected to cause “injury” to the enforcement of any law or the conduct of lawful investigations under paragraph 22(1)(b), particularly where the underlying investigation is stale, inactive, or structurally concluded?
 - 3. **The Temporal and Procedural Boundaries of “Investigations”:** Can the RCMP assert an ongoing investigative character over CPIC transactions that merely log the completion of past, expired, or time-barred administrative processes (such as a summons or arrest warrant), particularly where any potential prosecution is long-concluded or barred under the constitutional ceilings established in *R. v. Jordan*?
 - 4. **The Mischaracterization of Public Court Records as Confidential Sources:** Does paragraph 22(1)(b)(ii) permit the withholding of ministerial metadata (such as Originating Agency [ORI] codes, court levels, court locations, names of judicial officers, or Source Identifiers [SID]) under the guise of protecting a “confidential source,” when the informant

on a Criminal Code Form 2 Information is a matter of public record post-arrest or post-issuance of process?

5. **The Exclusion of Ultra Vires Conduct from “Lawful Investigations”:** Applying the doctrine of the indivisibility of the Crown (*Benedict v. Ontario*), can information generated through, or corrupted by, fraudulent manipulation or the compilation of false information packages ever be characterized as “obtained” or “prepared” in the course of a “lawful investigation” under subsection 22(1)?
- f. **Pre-emptive Resolution of Anticipated Objections (The Establishment of Novel Precedent):** In the event the RCMP (the “**RCMP Tribunal**”) neglects its statutory duty to transmit all relevant material to the Registry and the applicant (the “**Applicant**”), does the present factual matrix warrant the establishment of a novel legal precedent? Specifically, where there exists an underlying allegation of fraud perpetrated by law enforcement in concert with Crown Counsel during a criminal proceeding that is strictly *void ab initio*, and where a criminal prosecution could not lawfully have been sustained due to the deliberate filing of an admittedly false information package into a transferee courthouse (the Ontario Court of Justice, 10 Armoury Street Courthouse), is the RCMP Tribunal precluded from relying upon spurious legal justifications to outright refuse a requisite search for the Personal Information of the Applicant?

VOLUME #3: LEGAL BASES

VOLUME #3(A): THE OFFICE OF THE PRIVACY COMMISSIONER DETERMINES THE EXTENT OF THE RCMP’S STATUTORY DUTY AND PARAMOUNTCY OF CONTROL OVER MULTI-JURISDICTIONAL ENTRIES WITHIN THE CANADIAN POLICE INFORMATION CENTRE (THE “CPIC”)

62. The Office of the Privacy Commissioner of Canada (the “**OPCC**”) previously initiated a comprehensive investigation pertaining to formal complaints registered against the Royal Canadian Mounted Police (the “**RCMP**”) which was titled by the OPCC, Disclosure of information about complainant’s attempted suicide to US (United States) Customs and Border Protection not authorized under the *Privacy Act* (see: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170419_rcmp/).
63. Said complaints concerned the unauthorized extraterritorial disclosure of personal information (the “**Personal Information**”) regarding an individual’s historical medical distress—specifically, a suicide attempt—to the United States Customs and Border Protection (the “**CBP**”). The impugned data, originally uploaded by the Toronto Police Service (the “**TPS**”) to the CPIC database, was subsequently weaponized by the CBP to formally deny the complainant entry into the United States. The OPCC determined the complaints to be entirely well-founded, conclusively ruling that the dissemination constituted a direct contravention of the *Privacy Act*, RSC 1985, c P-21, as it satisfied neither the rigid parameters of a valid “law enforcement” exemption nor the doctrine of “consistent use”.
64. In November 2013, the complainant was engaged in transnational travel originating from Toronto Pearson International Airport. During the preclearance protocol, CBP agents detained the individual, subjecting her to interrogatory measures predicated upon a historical medical emergency dated June 2012.
65. The complainant was formally deemed inadmissible to the United States pursuant to the *Immigration and Nationality Act* (United States), predicated strictly upon health-related statutory grounds (specifically, the categorization of a mental disorder allegedly posing a threat to public safety).

The Genesis of the Disclosed Intelligence:

- 93 66. The CBP extracted this sensitive intelligence directly via the CPIC mainframe. The TPS had previously instituted a “Caution flag” denoting “Suicidal Tendencies,” running concurrently with a “Special Interest Police” (the “SIP”) entry categorized as “Mental Health - Attempted Suicide - Drugs,” following their deployment to the complainant’s 2012 medical distress incident.
67. Notwithstanding the fact that the TPS physically inputted the data and the CBP acted as the ultimate consumer of said data, the formal complaint was strategically and correctly levied against the RCMP.
68. The RCMP operates as the absolute statutory steward and supreme technological administrator of the CPIC infrastructure. Furthermore, it exercises exclusive jurisdiction over the Memorandum of Cooperation (the “MOC”) executed with the Federal Bureau of Investigation, which technically facilitates the access of United States agencies to the CPIC databanks.
69. Consequently, the RCMP is encumbered with the ultimate and inescapable legal responsibility to ensure that any intelligence disseminated to foreign state actors maintains strict adherence to the *Privacy Act*. *Ipso facto*, the RCMP is precluded from operating as a mere passive repository or “blind conduit”; rather, it is compelled by law to actively govern, monitor, and regulate the propriety and legality of any data uploaded by ancillary police forces. Invoking the foundational legal maxims authored by Herbert Broom, *qui facit per alium facit per se* (he who acts through another acts himself) and *qui non prohibet quod prohibere potest assentire videtur* (he who does not prevent what he has the power to prevent is deemed to assent), the RCMP’s failure to actively restrict unlawful data sharing renders it directly culpable for the resultant privacy breaches.

Jurisprudential Analysis and Determinations of the OPCC

70. The determinative legal issue hinged upon whether the extraterritorial transmission of the data to the CBP, absent the explicit consent of the complainant, was legally justifiable pursuant to the stringent statutory exemptions articulated within subsection 8(2) of the *Privacy Act*.

Analysis of Paragraph 8(2)(f) (Agreements with Foreign States for Law Enforcement):

71. The RCMP advanced the argument that the admissibility screening protocols executed by the CBP inherently constitute a public safety and law enforcement mandate, ostensibly designed to preemptively guard against tangible threats to property or human safety.

The Finding of the Commissioner

72. The OPCC unequivocally ruled that the immigration admissibility assessments conducted by the CBP do not satisfy the rigorous definitional thresholds of “law enforcement” or “criminal justice” within the strict purview of the MOC. The complainant had engaged in no statutory infractions and was subject to no penal sanctions; her activities were strictly limited to international transit. The OPCC firmly established that deeply sensitive health intelligence must exclusively be disseminated to border authorities in circumstances where the individual in question exhibits a demonstrable, empirical threat to public safety.

Analysis of Paragraph 8(2)(a) (The Consistent Use Doctrine):

73. The RCMP averred that leveraging the health data to evaluate transnational public safety aligned consistently with the originating purpose of its collection by the municipal constabulary.
74. The OPCC rejected this premise, finding that the primary operational intent behind the collection of such data by frontline officers is to chronicle localized incidents and ensure the immediate tactical safety of officers and the public during direct, real-time interactions. The utilization of such highly confidential health records for the facilitation of a foreign immigration assessment constitutes an application that an individual could not “reasonably

The Intransigence of the RCMP

75. The RCMP formally dissented from the OPCC’s findings and outright refused the implementation of the recommended directives. The Tribunal steadfastly maintained the position that the CBP operates as a valid law enforcement entity and that the “SHARE USA” default parameter must remain universally active to theoretically preserve public safety.
76. Notwithstanding the institutional recalcitrance regarding system defaults and the precise lexicon of the policies, the OPCC acknowledged the substantive collateral benefit: the intense scrutiny of the RCMP’s architectural administration catalyzed local agencies to unilaterally purge thousands of mental health records from the CPIC network, thereby drastically mitigating the probability of analogous privacy infractions.
77. This inherent limitation encapsulates precisely why the investigative reports generated by the OPCC are not, *ipso facto*, subject to judicial review *per se*; the OPCC operates functionally as an ombudsman, authorized to recommend remedial avenues that the impugned Government Institution possesses the discretion to disregard. This structural limitation perfectly mirrors the statutory frameworks of the *Personal Information Protection and Electronic Documents Act, SC 2000, c 5* and the *Access to Information Act, RSC 1985, c A-1*.
78. The Office of the Information Commissioner has some different statutory powers but that is not at issue herein.
79. Conversely, the *Privacy Act* dictates a markedly more restrictive paradigm concerning an applicant’s right to invoke the jurisdiction of the Federal Court of Canada. Adjudicative access is narrowly circumscribed, crystallized specifically when a complainant seeks relief pursuant to section 41 of the *Privacy Act* following a formal refusal of access. Ergo, the present application for judicial review is correctly and inescapably predicated upon the egregious failure of the RCMP to conduct a requisite search for the Personal Information of the applicant (the “**Applicant**”) pursuant to his formally submitted Access Request (dated March 11, 2026), and the concomitant failure of the Head of the RCMP to execute the mandatory statutory contemplation mandated under subsection 8(2) of the *Privacy Act*.

VOLUME #3(A)(I): SUMMARY OF JURISPRUDENTIAL EFFECT REGARDING THE INPUTTING OF FALSE OR INACCURATE DATA INTO CPIC BY ANY LAW ENFORCEMENT APPARATUS

80. The OPCC’s determinations establish an irrevocable precedent: the RCMP is strictly prohibited from operating as a passive host or “blind conduit” for intelligence contributed by external police forces. Given its paramount structural and administrative role, the RCMP is legally bound to exercise an active, governing supremacy over all Personal Information transiting the national infrastructure.
81. The jurisprudential rationale underpinning the OPCC’s findings is delineated into the following determinative principles:
 - a. **The Doctrine of Sufficient Control**
 - i. The OPCC explicitly concluded that the quantum of control exercised by the RCMP over the CPIC mainframe is unequivocally sufficient to trigger the robust protections of section 8 of the *Privacy Act*. Even in circumstances where a municipal entity, such as the TPS, originated the data upload and maintained nominal carriage of their localized investigative file (denoted by an occurrence number), the Commissioner of the RCMP remains the ultimate, non-delegable authority accountable for the administration, operation, and statutory compliance of the overarching system.
 1. Herein, it is a matter of evidentiary record that at least one of the specific case identification numbers associated with the impugned records is demonstrably not attributable to the TPS; namely, Police Case ID: 457197 (visibly stamped upon the upper right-hand quadrant of the admitted False Information Package). Both the TPS and the Ontario Provincial Police (the “**OPP**”) have formally and unequivocally disclaimed any jurisdictional relation to said case identification number, a repudiation which logically and necessarily leaves the RCMP as the sole remaining institutional custodian.

82. Predicated upon the fact that the RCMP acts as the exclusive Canadian signatory to the MOC executed with the Federal Bureau of Investigation, the OPCC ruled that the RCMP bears the sole, non-transferable burden of ensuring that any cross-border intelligence dissemination strictly comports with both the MOC and the domestic imperatives of Canadian privacy legislation.

The Imperative for Active Policy and Architectural Safeguards

83. The OPCC profoundly criticized the RCMP's legally bereft posture that the onus of statutory compliance rests entirely upon the contributing municipal or provincial agencies. The OPCC firmly established that the RCMP must actively engineer the CPIC policies, user protocols, and foundational technical defaults to preemptively neutralize the potential for unauthorized data proliferation.
84. 30. By way of specific illustration, the OPCC mandated that the RCMP restructure the technical baseline of the system's "SHARE USA" feature to automatically suppress the transmission of deeply sensitive health data, rather than permitting dissemination to function as the unexamined default parameter.
85. 31. This precise conflict crystallizes the overarching precedent: while the RCMP attempts to shield itself behind the facade of a collaborative, decentralized system where localized forces "own" their respective data, the OPCC definitively ruled that supreme architectural stewardship equates inextricably to absolute legal accountability. To achieve compliance with the *Privacy Act*, the RCMP must actively audit, regulate, and restrict the manner in which both domestic and foreign agencies interface with the databanks under its sovereign control.

VOLUME #3(B): THE NOVEL LEGAL ISSUES FORMULATED FOR ADJUDICATION

86. The novel legal controversies presented for adjudication herein are robust and multifaceted. It is axiomatic that these issues fundamentally engage the broader public interest, extending far beyond the immediate evasive tactics deployed against the Applicant, and possess central, systemic importance to the integrity of the administration of justice. The resolution of these distinct, untested issues will be effortlessly achieved upon the compulsory transmission of the certified tribunal record (the "CTR") to both the Federal Court of Canada and the Applicant. The subsequent enumeration is strictly illustrative, explicitly provided to pre-empt and neutralize any unnecessary, frivolous, or meritless objections the **Respondent** may attempt to mount under *Rule 318* of the *Federal Courts Rules*, *SOR/98-106* (the "**FCR**").

The First Novel and Untested Issue

87. A primary determinative issue hinges upon whether the originating data sequence inputted into the CPIC repository—irrespective of the specific law enforcement agency acting as the originating terminal, whether acting as a principal or an agent, and under whatever alphanumeric case identification number—materially mirrored the contents of the admitted False Information Package. Should the inputted data align with said package, the Applicant is undeniably entitled to its disclosure as his proprietary Personal Information, notwithstanding the fact that the underlying data is demonstrably false and fabricated: *Lawson v. Accusearch Inc.*, 2007 FC 125.

The Second Novel and Untested Issue

88. The subsequent issue necessitates an inquiry into whether the initial data matrix entered into CPIC—specifically referencing a "warrant in the first" and the identifier "MCLEAN, Kevin"—was structurally accurate at the precise moment of inception, irrespective of the underlying, contested merits of the "Ex Parte In Camera Hearing" or the purportedly valid INTAKE COURT ENDORSEMENT (dated September 23, 2024). Crucially, the Court must determine if this data was subsequently subjected to post-hoc amendment, either prior to or immediately following

the physical arrest of the Applicant. If the metadata was technically correct at the first instance, but later strategically altered to forcefully synchronize with the relevant data points required by CPIC (specifically the Foundational Metadata, encompassing the Originating Agency Identifier (the “**ORI**”); the designated issuing authority or “court field”; the remarks/narrative field; and the System Identification Number (the “**SID**”) generated upon entry), such alterations constitute a profound abuse of process. Collectively, these elements are categorized as the foundational data elements comprising a “WANT record”.

89. It is submitted as a highly probable extrapolation that the originating law enforcement agency, designated by the initial ORI, was not the identical agency that subsequently executed the surreptitious amendments to the WANT record. These potential, unauthorized systemic alterations encompass four distinct vectors of modification:
 - a. The deliberate modification or reassignment of the ORI, falsely transferring jurisdictional appearance to a separate police service;
 - b. The structural alteration of the jurisprudential authority or “court field” to legitimize an otherwise *void ab initio* warrant;
 - c. The substantive revision of the remarks or narrative field to retroactively justify the apprehension of the Applicant; and
 - d. The systemic desynchronization or reallocation of the SID, designed to obfuscate the original timestamp and audit trail of the fabricated entry.
90. The forensic veracity of these administrative maneuvers—and the exposure of the underlying malfeasance—can only be illuminated through a rigorous examination of the automated hexadecimal transaction logs and sequence trails. Consequently, this determination can solely be achieved through the unmitigated disclosure of the Applicant’s Personal Information, which is definitively housed within a Personal Information Bank (the “**PIB**”) and remains under the absolute control and constructive possession of the centralized federal repository.

VOLUME #3(C): THE JURISPRUDENTIAL DOCTRINE OF POSSESSION UNDER THE FEDERAL COURT RULES

91. A masterful comprehension of the legal doctrine of “possession” is absolutely paramount when navigating the *FCR*, specifically concerning the mandatory production of documentary evidence. This doctrine governs both the general discovery apparatus (Rules 222-223) and, crucially, the compulsory transmission of tribunal records under *Rule 317*.

The Definition of Possession in the Strict Context of Rule 317

92. *Rule 317* of the *FCR* vests an applicant in a judicial review proceeding with the absolute right to requisition material relevant to the application that resides within the possession of the impugned Tribunal.
93. 73. Within the architecture of the *FCR*, the concept of “possession” vehemently rejects the archaic limitation of mere physical custody. The appellate jurisprudence has consistently expanded “possession” to broadly encompass the legal right, authority, or institutional ability to procure the document. While the *FCR* omits a rigid definitional clause for “possession,” the overwhelming weight of document production jurisprudence establishes that it strictly incorporates:
 - a. **Actual Possession:** The immediate, physical custody of the document; and
 - b. **Constructive Power or Control:** Vesting the entity with the absolute right or jurisdictional authority to demand and obtain the document, irrespective of its immediate physical locale.

94. Consequently, for the purposes of *Rule 317*, if a Tribunal possesses the overarching legal right or technical capacity to access relevant data, that material is definitively deemed to be in its “possession” for production purposes, even if the physical servers or archives are geographically displaced.

The Tripartite Categorization of Possession

97 In advanced civil procedure, possession is jurisprudentially categorized into three distinct operational forms:

a. **Sole Possession:**

- i. **Definition:** The most absolute iteration of possession. It manifests when a singular entity exercises exclusive physical custody and administrative dominion over a record.
 1. If the Tribunal maintains the singular physical iteration of a memorandum within its immediate administrative confines, it exercises sole possession.
 2. The Tribunal retains the exclusive, unfettered right to utilize, manipulate, and produce the material.

b. **Joint Possession**

- i. **Definition:** This formulation arises when two or more distinct entities share physical custody, administrative access, or control over a record, resulting in a shared, indivisible right to possess the material.
- ii. **Application:**
 1. In circumstances where the RCMP and an external municipal police force mutually interact with a shared digital architecture (such as CPIC), both entities may exercise Joint Possession over the underlying data matrices. In the realm of document production, shared possession with a non-party does not immunize the party from production; they remain legally compelled to produce the material or actively seek the requisite consent, as their legal right to the document remains absolute.

c. **Constructive Possession**

- i. **Definition:** This represents the most expansive and vital formulation of possession. It dictates that an entity holds possession when it lacks immediate physical containment of the material, yet wields the *de jure* legal right, institutional power, or technical authority to requisition and obtain it.
- ii. **Application:** This doctrine frequently serves as the epicenter of contentious document production litigation. If the RCMP archives its historical data utilizing external federal infrastructure but retains the sovereign right to demand the extraction of those logs at will, the RCMP is irrevocably bound by Constructive Possession. Similarly, if records are held by a delegated agent or legal counsel, the principal entity maintains Constructive Possession because it exercises the power of directive over the agent. **Rule 317 Implications:** A Tribunal is strictly legally barred from resisting a *Rule 317* request by pleading an absence of physical custody if it possesses the statutory or administrative authority to compel the retrieval of the document from its current host. The RCMP is not seeking that an independent contractor provide its backup tapes but rather it is a demand unto itself if you will.

VOLUME #3(D): A COMPARATIVE LINGUISTIC ANALYSIS OF THE RCMP'S DECISIONS (THE HALTON POLICE CASE VS. THE MCLEAN RCMP PROCEEDING)

Volume #3(D)(I): The RCMP Decision in the Halton Police FIPPA Case

96. To illuminate the institutional bad faith and strategic linguistic manipulation deployed by the RCMP herein, the Applicant heavily relies upon a comparative analysis of the strikingly similar, yet critically divergent, language utilized by the RCMP in *Halton Regional Police Services Board (Re)*, 2024 CanLII 67092 (ON IPC) (the “**Halton Police Case**”). In the Halton Police Case, Adjudicator Faughnan, presiding under the *Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M.56* (the “**MFIPPA**”), reproduced the RCMP’s formal refusal letter at paragraph four, which stated:

“This is in response to your request made under the *Privacy Act*, which was received by this office on March 2, 2015, in which you are seeking a report of all inquiries made by any officer/civilian member of any Canadian or USA police force since 1970 under your identifiers including any inquiries made on CPIC/PARAS.”

Based on the information provided, a search for records was conducted. Be advised that we can neither confirm nor deny the existence of the information requested. If the information did exist, it would be subject to exemption in its entirety pursuant to Paragraph 22(1)(b) of the *Privacy Act*...

The *Privacy Act* has established the right of applicants to access federally maintained records which contain personal information concerning themselves. If you were involved with another police department or service, they may have information that concerns you. The *Privacy Act* does not authorize the RCMP to search files or to disclose information belonging to other police forces.”

Volume #3(D)(II): The Distinctions Possessing Profound Legal Significance

Volume #3(D)(II)(a): The Execution of a “Search for Records”

97. In the Halton Police Case, the RCMP formally averred that “a search for records was conducted,” utilizing the term without limitation. The term “record” lacks a precise definition under the *Privacy Act*, contrasting sharply with the *Access to Information Act* which broadly defines it as “any documentary material, regardless of medium or form.”
98. Conversely, in the present proceeding (the “**McLean RCMP Proceeding**”), the RCMP artificially narrowed its purview, strictly representing that a search was conducted solely within “CPIC and Specialized Policing Services”—despite the Applicant explicitly demanding a search of the Foundational Metadata and Offline Historical Database.

Volume #3(D)(II)(b): The Deployment and Subsequent Waiver of the “Neither Confirm Nor Deny” Shield

99. In the Halton Police Case, the RCMP explicitly deployed the powerful statutory shield of section 16(2), stating it could “neither confirm nor deny” the existence of the requested intelligence. In stark contrast, the RCMP completely abandoned this shield in the **McLean RCMP Proceeding**.

The Legal Ramifications of Waiving Section 16(2):

100. The mechanism of Section 16(2) permits a Government Institution to completely obfuscate the existence of a record, an extraordinary measure designed to preserve the sanctity of active, highly sensitive investigations. The author of the RCMP decision in the **McLean RCMP Proceeding** explicitly chose not to invoke this provision.
101. **The Legal Import:** By declining to invoke Section 16(2) *in limine*, the RCMP legally waived its right to obfuscate the existence of the records. Because it failed to issue an NCND response, the RCMP is now irrevocably tethered to its specifically cited exemptions (Sections 19, 22, and 26).
102. Should the **Respondent** attempt to argue during these proceedings that the existence of the requested Metadata is hypothetical or that confirming its existence would compromise investigative integrity, such an objection is a strict nullity. The **Respondent** has preemptively waived this protection and cannot retroactively reconstruct a Section 16(2) shield to evade production under *Rule 317*. It chose the route it did by granting itself an extension of time and it could have amended its decision from April 27, 2026, and the record will reflect that the Applicant provided it with opportunity to do so but it declined.
103. Consequently, the RCMP is legally estopped from asserting that the Personal Information sought is immune from basic acknowledgment before this Honourable Court. It falls under the principle at least by analogy from *Turigan v. Alberta, ABCA, 1988*, involving “estoppel by record”.

Volume #3(D)(II)(c): The Strategic Erasure of “Concerning Themselves”

104. In the Halton Police Case, the RCMP stated, “The *Privacy Act* has established the right of applicants to access federally maintained records *which contain personal information concerning themselves*.” Alarmingly, in the **McLean RCMP Proceeding**, the RCMP deliberately truncated this sentence, stating merely, “The *Privacy Act*

has established the right of applicants to access federally maintained records,” entirely deleting the reference to Personal Information.

105. This surgical erasure is not benign; it perfectly substantiates the Applicant’s assertion regarding the Foundational Metadata. Under Section 3 of the *Privacy Act*, “personal information” unequivocally encompasses transaction histories and assigned identifying numbers. By deliberately removing the qualifier “concerning themselves,” the RCMP attempted to linguistically sever its statutory duty to track biographical metadata logs, unlawfully recharacterizing the underlying server operations as mere “federal administrative records” exempt from the Applicant’s reach.

Volume #3(D)(II)(d): Misinterpretations Regarding Authorization and Ownership

106. In the Halton Police Case, the RCMP hypothesized, “If you were involved with another police department... they may have information that concerns you.” In the **McLean RCMP Proceeding**, the RCMP shifted to an operative past-tense certainty: “If this matter *concerned* another police department... The *Privacy Act* does not authorize the RCMP to search files or to disclose information belonging to other police forces.”

107. 99. The hypothetical “If” in the Halton matter was logical, as the requestor sought fifty years of generalized data. Herein, the Applicant demanded highly specific, targeted access to Personal Information directly indexed under Police Case ID: 457197—an identifier formally disavowed by both the TPS and the OPP. The RCMP’s assertion that it lacks “authorization” to search its own sovereign database for records that do not “belong” to other forces is a profound misstatement of law.

VOLUME #4: WITHOUT A SEARCH, CORRECTION RIGHTS CEASE TO EXIST AS LEGISLATED BY PARLIAMENT

VOLUME #4(A): PERSONAL INFORMATION IS AKIN TO ONE’S OWNERSHIP

108. It is a well-settled jurisprudential axiom that *Rule 317* of the *FCR* does not demand that the requested material be legally “owned” by the administrative Tribunal, nor does it require exclusive, physical geographic custody. The singular, uncompromising statutory threshold is that the material resides within the “possession” of the Tribunal.

109. Furthermore, relying upon established jurisprudence (such as the determinations of Mr. Justice Tysoe in the Supreme Court of British Columbia in *Mazhero*), the Personal Information of an applicant is inherently “owned” by the applicant themselves—it emphatically does not legally “belong” to other police forces, regardless of their status as the originating agency.

110. In *Atlantic Prudence Maritime Inc. v. Canada (Minister of Transport)*, 1983 2 FC 183 (FCA) (the “**Atlantic Prudence Decision**”), the Federal Court of Appeal conclusively established that possession within the context of administrative record production must be subjected to a highly practical, functional interpretation, firmly rejecting the archaic constraints of narrow property concepts. The appellate court unequivocally ruled that a Tribunal is strictly prohibited from evading its production obligations by advancing the specious claim that records are “owned” by third parties, provided those records were relied upon, hosted, or technically accessible by the Tribunal in the execution of its administrative mandate.

111. 103. This overarching principle was subsequently codified and expanded in *Canada (Attorney General) v. Cloutier*, 2008 FC 322 (the “**Cloutier Decision**”). The Federal Court definitively held that material housed within an electronic database accessible by a government institution constitutes absolute possession for the strict purposes of a *Rule 317* request. The Court forcefully rejected the obsolete notion that electronic data must be physically manifested in print or localized within a specific geographic office to be “possessed,” holding that technological accessibility acts as the absolute functional and legal equivalent of possession.

112. Under the doctrine of Constructive Possession, an entity holds possession of material whenever it exercises the legal right, administrative power, or technological capacity to command its retrieval, completely independent of physical containment. In the modern administrative apparatus, data is perpetually decentralized across complex virtual architectures. To restrict the definition of possession to physical, paper-based custody would render the operation of *Rule 317* an archaic and absolute nullity (the “**Nullity**”).
113. 105. The CPIC database represents a colossal, centralized national infrastructure. While municipal entities input localized intelligence via their discrete ORIs, the foundational technological mainframe, the database schema, and the physical server arrays are owned, operated, and exclusively maintained by the RCMP. The interaction between the RCMP and external police forces does not constitute total operational separation; rather, it manifests as a textbook paradigm of Joint Possession over the transactional metadata.
114. 106. When an external law enforcement agency instantiates a WANT Record into CPIC, that specific data matrix is instantly ingested into a database strictly hosted upon federal servers. The corresponding transactional logs, sequence trails, and hexadecimal dumps are automatically and autonomously generated by the federal system architecture itself. The RCMP holds the supreme administrative credentials, the systemic audit tools, and the absolute physical dominion over the server farms required to extract this intelligence. Consequently, the raw forensic mainframe ledger records sought by the Applicant reside indisputably within the Constructive Possession of the RCMP.

VOLUME #4(C): THE RCMP AS THE PARAMOUNT CUSTODIAN AND SOVEREIGN ADMINISTRATIVE STEWARD

115. In *Canada (Information Commissioner) v. Minister of National Defence*, 2011 SCC 25 (the “**National Defence Decision**”), the Supreme Court of Canada formulated a rigid bipartite test to determine whether a government institution exercises control over records for statutory production purposes:
- First, does the record relate to a substantive departmental matter?
 - Second, could the institution reasonably expect to obtain a copy of the record upon executing a request?
116. Although the *National Defence Decision* was adjudicated under the *Access to Information Act*, its foundational logic applies *a fortiori* to the legal concept of possession encapsulated within *Rule 317*. The administration, forensic auditing, and structural security of the CPIC infrastructure are indisputably departmental matters under the exclusive purview of the RCMP. As the sovereign national steward of CPIC, the RCMP possesses the absolute, unassailable legal and technical right to obtain, audit, and extract any record residing within its own database.
117. 109. This conclusion is explicitly supported by provincial adjudicative bodies. As noted in the Halton Police Case, the Information and Privacy Commissioner of Ontario definitively ruled that municipal police boards possess neither custody nor control over the CPIC Offline Historical Database. Because these offline archives are managed with absolute exclusivity by the RCMP, any legal demand for historical transaction logs must be directed solely to the federal institution.

VOLUME #4(D): THE ABSOLUTE NULLITY OF THE “THIRD-PARTY OWNERSHIP” DEFENSE

118. Any anticipated attempt by the **Respondent** to resist the compulsory production mandates of *Rule 317* by falsely characterizing the requested transaction logs and hexadecimal dumps as “belonging” to other police forces is a profound legal absurdity. A transaction log is emphatically not an investigative narrative report, nor does it encompass proprietary, third-party tactical intelligence. It is purely administrative Metadata—an automated, machine-generated chronicle of the systemic operations (*acta*) of the federal mainframe itself. The unique system identification numbers, the ORIs, the hardware terminal addresses, and the microsecond timestamps are intrinsic, systemic properties belonging exclusively to the CPIC platform. They constitute the indisputable administrative footprint of state action. If an arrest warrant was subjected to illicit, post-hoc digital modification—specifically via

101 the unauthorized exploitation of the GrapeCity SDK API—the transaction logs represent the singular, immutable evidentiary matrix proving that alteration. The deliberate suppression of this critical Metadata by the **Respondent**, disguised beneath the specious veil of inter-agency confidentiality, constitutes an administrative omission that is an absolute Nullity *ab initio*, emphatically not a curable irregularity (the “**Irregularity**”). This obstruction directly and fatally contravenes the statutory purpose of subsection 12(1) of the *Privacy Act* and fundamentally frustrates the compulsory production mechanics of *Rule 317*. The state is strictly prohibited from deploying the complexity of its own decentralized database architecture as a jurisprudential shield to conceal administrative malfeasance or *ultra vires* jurisdictional overreach.

VOLUME #4(E): THE STATUTORY ABSURDITY AND THE FRUSTRATION OF CORRECTION RIGHTS UNDER SUBSECTION 12(2) OF THE PRIVACY ACT

119. Pursuant to subsection 12(2) of the *Privacy Act*, an individual granted access to personal information utilized for an administrative purpose is statutorily vested with the affirmative right to request a correction of said information, mandate the attachment of a formal notation if the correction is refused, and compel the notification of these amendments to any entity that received the data within the preceding two years.
120. The posture adopted by the **Respondent** herein—specifically, the legally specious assertion that it lacks the authorization to search, retrieve, or disclose data inputted into its sovereign infrastructure by ancillary police forces—engineers a profound statutory absurdity (the “**Statutory Absurdity**”).
121. If the RCMP is legally permitted to abdicate its overarching search obligations beneath the guise of “third-party ownership,” it *ipso facto* obliterates the Applicant’s fundamental statutory right to subsequently request the correction of admittedly false or materially inaccurate intelligence housed within the CPIC database. A requestor cannot correct that which the paramount custodian outright refuses to locate.
122. This administrative sleight of hand effectively insulates both the centralized repository and the originating municipal police forces from statutory accountability. Should this Honourable Court validate the RCMP’s restrictive interpretation, an individual maliciously targeted by the fabrication of a False Information Package would be permanently saddled with fraudulent data operating actively within the nation’s premier law enforcement repository. This permanent taint constitutes an ongoing, egregious violation of fundamental justice.
123. It is a foundational tenet of statutory interpretation that the law does not permit a party to benefit from its own administrative malfeasance (*nullus commodum capere potest de injuria sua propria*). Furthermore, jurisprudential doctrine strictly forbids a reading of a statute that renders a remedial provision—such as the correction rights enshrined in subsection 12(2)—meaningless or illusory (*interpretatio fienda est ut res magis valeat quam pereat*, an interpretation must be adopted so that the provision may have effect rather than fail). The RCMP cannot strategically interpret section 12(1) (access) in a manner that entirely nullifies section 12(2) (correction).
124. **Nota Bene:** Should the **Respondent** attempt to argue that any correction request must instead be directed to the originating municipal or provincial agency, such an argument is fundamentally and irreparably flawed *ab initio*. Municipal police boards are explicitly excluded from the purview of the federal *Privacy Act*. More critically, a municipal entity does not possess the sovereign administrative credentials, the requisite system-wide database access, or the structural authority to execute CPIC metadata notations or mandate downstream notifications across the federal infrastructure. The RCMP, functioning as the supreme technological custodian, remains the sole entity legally and technically capable of executing the statutory mandate commanded by subsection 12(2).

Volume #4(E)(I): The Paramountcy of the Initial Search and the “Meaningful Exercise” of Subsection 12(2)

125. It is a foundational legal axiom that the invocation of the remedial correction rights enshrined within subsection 12(2) of the *Privacy Act* is strictly predicated upon the antecedent execution of a comprehensive search. Stated with stark precision: the realization of statutory rights initiates exclusively with a search. By refusing to proactively interrogate the Foundational Metadata and the Offline Historical Database—repositories over which

the RCMP exercises absolute constructive possession—the RCMP Tribunal entirely and structurally paralyzes the Applicant’s capacity to exercise his statutory entitlements.

126. In *Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration)*, 2002 FCA 270 (CanLII), 2003 1 FC 219 (the “**Information Commissioner Decision**”), the Federal Court of Appeal conclusively established the parameters safeguarding the effective operation of subsection 12(2). The appellate court ruled that the excessive severance or redaction of records, which renders the resulting disclosure incomprehensible, fundamentally undermines the “meaningful exercise” of the correction rights granted under subsection 12(2) (at para 10).
127. Applying the deductive logic of the *Information Commissioner Decision a fortiori* to the present factual matrix: if the provision of severely redacted information illegally frustrates the meaningful exercise of subsection 12(2), then the **Respondent’s** outright, institutional refusal to even conduct a preliminary search constitutes an absolute evisceration of those identical rights *ab initio*.

Volume #4(E)(II): The Competing Interests and the Disclosure of Authorizing Identities (Paragraphs 3(g) and 3(i))

128. A central determination in the *Information Commissioner Decision* was the resolution of competing statutory interests concerning the disclosure of third-party identities under paragraphs 3(g) and 3(i) of the *Privacy Act*. The Federal Court of Appeal explicitly ruled that a requester’s significant private interest in clearing their name in the public domain invariably supersedes a third party’s minimal interest in anonymity (at paras 31 and 33). Fairness in administrative inquiries dictates that adverse actions or unfavourable views cannot remain secret and strictly unchallengeable (at para 34).
129. The Applicant herein maintains a profound, legally cognizable interest in clearing his name across the national law enforcement infrastructure, an objective partially realized but requiring further unmitigated disclosure. The singular avenue to definitively establish the falsity of the CPIC data requires the disclosure of the specific authorizing entities—namely, the issuing judicial officers—embedded within the WANT record.
130. Pursuant to the *Information Commissioner Decision*, the names of the authorizing or issuing jurists fall squarely within the purview of paragraph 3(i) of the *Privacy Act* (the name of an individual where it appears with other personal information relating to the individual, or where the disclosure of the name itself would reveal information about the individual).
131. Crucially, this disclosure imperative strictly encompasses the name of the ostensibly fictitious Justice of the Peace, “George Jiri,” irrespective of the fact that said individual did not physically execute the data upload. The identities of the actors (real or fabricated) authorizing the state’s action against the Applicant constitute “views or opinions about the individual” under paragraph 3(g) and are thus inextricably embedded within the Applicant’s own Personal Information.
132. **Nota Bene:** The **Respondent** is pre-emptively estopped from asserting that a refusal to search is justified to protect the privacy interests of the municipal officers or jurists named within the CPIC warrant metadata. As the Federal Court of Appeal unequivocally held, a generalized “chilling effect” or a promise of confidentiality cannot override the statutory duty to disclose, particularly when the requester seeks to challenge fundamentally flawed or unchallengeable state actions (at paras 11-12, 34).
133. Finally, given the high probability that the False Information Package was disseminated to ancillary government institutions—potentially both domestic and foreign—the Applicant possesses an unassailable statutory right to ascertain the precise nature of the uploaded data. This knowledge is an absolute requisite to compelling the downstream notifications mandated by clause 12(2)(c). The RCMP Tribunal’s refusal to search acts as a deliberate blockade, shielding downstream consumers of fabricated intelligence from statutory correction.

VOLUME #4(F): THE OPERATIONAL EXCLUSIVITY OF “OFF-LINE SEARCHES” AND THE REDUCTIO AD ABSURDUM OF DELEGATED CONTROL

134. It is a matter of established administrative record and judicial notice that municipal and provincial law enforcement apparatuses are strictly precluded from independently executing “off-line searches” within the CPIC

infrastructure. This systemic limitation was explicitly chronicled by the Information and Privacy Commissioner of Ontario in *Halton Regional Police Services Board (Re)*, 2024 CanLII 67092 (ON IPC), relying upon the foundational analysis articulated within *Order MO-1446*.

135. As delineated within *Order MO-1446*, while ancillary police departments may possess terminal access for standard queries, an “off-line search”—a forensic mechanism utilized to process and extract deep-archive computer records—mandates the explicit submission of a formal request to the RCMP. It is only subsequent to the RCMP’s unilateral approval and physical execution of said search that the generated results are formally transmitted to the requesting agency.
136. Crucially, the adjudicator determined that the extracted search results crystallize into a record within the custody and control of the municipal police department *strictly upon their receipt* of the finalized data from the federal repository.
137. Utilizing an advanced legal syllogism, this operational architecture yields an incontrovertible conclusion: if municipal police forces are themselves entirely reliant upon the RCMP to physically access and extract data from the Offline Historical Database, then the RCMP inherently possesses absolute, unassailable custody and control over the foundational archival intelligence. To countenance the **Respondent’s** prevailing posture—that the Applicant is legally barred from requisitioning his own Personal Information directly from the RCMP because said data ostensibly “belongs” to external police forces—engineers a profound *reductio ad absurdum*. It is a legal impossibility for an external police force to “own” or exercise paramount control over a historical dataset to which they lack direct, independent access.
138. **Nota Bene:** Consequently, the RCMP remains the singular, inescapable statutory custodian capable of discharging the search and production obligations mandated by the *Privacy Act* and *Rule 317*. Any assertion by the **Respondent** that the Applicant must uniquely pursue municipal agencies to secure off-line CPIC logs is a deceptive administrative deflection, entirely devoid of operational reality and legal merit.

VOLUME #4(G): THE JURISPRUDENCE OF “CONTROL”: THE RIGHT OF DEMAND AND THE PURPOSIVE INTERPRETATION OF ACCESS LEGISLATION

Volume #4(G)(I): The Broad, Liberal, and Purposive Interpretation of Control

139. The jurisprudential conception of “control” under federal access to information legislation commands a remarkably broad, liberal, and purposive interpretation, strictly divorced from archaic notions of physical property or immediate custody.
140. In *Canada Post Corp. v. Canada (Minister of Public Works)*, 1995 CanLII 3574 (FCA) (the “**Canada Post Decision**”), the Federal Court of Appeal definitively rejected restrictive, proprietary constraints upon the statutory definition of control. Articulating the binding precedent on behalf of the appellate court, Létourneau J.A. held at page 245:

“The notion of control referred to in the Act is left undefined and unlimited. Parliament did not see fit to distinguish between ultimate and immediate, full and partial, transient and lasting, or ‘de jure’ and ‘de facto’ control. Had Parliament intended to qualify and restrict the notion of control to the power to dispose of the information, as suggested by the appellant, it could certainly have done so by limiting the citizen’s right of access only to those documents that the government can dispose of or which are under the lasting or ultimate control of the government.”

Volume #4(G)(II): The Binding Precedent of Hale v. Ontario (Criminal Code Review Board)

141. This expansive interpretive doctrine formulated by the Federal Court of Appeal was explicitly adopted and fortified by the Court of Appeal for Ontario in *Ontario (Criminal Code Review Board) v. Hale*, 1999 CanLII 3805 (ON CA) (the “**Hale Decision**”).
142. The *Hale Decision* concerned a highly analogous statutory access request. The requesters sought access to backup audio tapes created and physically retained by a court reporter. Crucially, the court reporter was not an employee, but an independent contractor engaged on a fee-for-service basis by the Ontario Criminal Code Review

Board (the “**Review Board**”). The Review Board and the court reporter formally resisted production, vehemently arguing that the backup tapes were created strictly as a personal *aide-mémoire* for the reporter, remained within the exclusive physical custody of the contractor, and were therefore not under the “control” of the Review Board.

143. The Court of Appeal for Ontario fundamentally rejected this evasion. Justice O’Connor, writing for the unanimous court, ruled that control is not contingent upon immediate physical possession or strict ownership. Rather, because the Review Board operated under a statutory mandate to keep an accurate record of its proceedings, it inherently possessed the *right to demand* access to the independent contractor’s backup tapes to verify accuracy. The appellate court unequivocally held that the institutional legal right to make a future demand for the records satisfies the statutory threshold of “control,” thereby compelling production.

Volume #4(G)(III): Application to the Present Factual Matrix: Offline Historical Data and Amended, Purged Records

144. Applying the binding jurisprudential logic of both the *Canada Post Decision* and the *Hale Decision a fortiori* to the present factual matrix yields an unassailable legal conclusion. The Applicant herein seeks access to off-line historical data, encompassing the original iterations of the inputted CPIC intelligence, alongside any subsequent unauthorized amendments, systemic purging, or operational alterations executed upon the WANT record.
145. If an administrative tribunal (such as the Review Board) is deemed by an appellate court to exercise absolute control over the independently created and personally housed backup tapes of an arm’s-length private contractor—predicated exclusively upon the tribunal’s right to demand those records for verification—the conclusion regarding the RCMP is infinitely stronger.
146. The RCMP is not interacting with an arm’s-length contractor; it is the sovereign administrator of its own technological infrastructure. The offline historical metadata resides within the RCMP’s own proprietary server arrays. The RCMP possesses the supreme, unmitigated statutory and administrative *right to demand*, extract, and audit the historical and purged data matrices generated within its own systems.
147. **Nota Bene:** Should the **Respondent** attempt to artificially distinguish between active terminal data “belonging” to local police and offline historical data, such a distinction is a jurisprudential nullity. The RCMP’s unquestionable authority to demand and extract the offline historical data establishes immediate, incontrovertible control. To suggest that the paramount federal law enforcement agency lacks control over the historical audit logs generated entirely within its own sovereign database is a legal absurdity that offends the liberal and purposive interpretative mandate established by the Federal Court of Appeal.

VOLUME #4(H): THE JURISPRUDENTIAL SIGNIFICANCE OF THE UNSOLICITED INQUIRY INTO SPECIALIZED POLICING SERVICES AND THE INVOLUNTARY INSTITUTIONAL ADMISSION OF CENTRALIZED SYSTEMIC MANIPULATION

Volume #4(H)(I): The Inference and the “Data Trigger”

148. The explicit and unsolicited inclusion of the Specialized Policing Services (the “**SPS**”) within the formal decision letter executed by the **Respondent**—specifically, via Mr. Jeff Ball—notwithstanding the absolute absence of any such request by the Applicant, precipitates a jurisprudential inference of monumental proportion. This unsolicited inclusion functions as an involuntary institutional admission that the Applicant’s dossier migrated entirely beyond the jurisdictional boundaries of standard divisional detachments, becoming inextricably embedded within the RCMP’s paramount national operational and technological command.
149. Pursuant to the strict operational strictures governing the *Privacy Act*, an Access to Information and Privacy (the “**ATIP**”) directorate is strictly prohibited from executing arbitrary or exploratory searches within branches fundamentally disconnected from the parameters of a specific request. The federal ATIP apparatus exclusively interrogates specific Personal Information Banks (the “**PIBs**”) when an initial intake assessment or an automated algorithmic database query affirmatively flags the existence of records within that distinct repository.

105 150. Consequently, the explicit institutional declaration that an SPS search was effectuated unambiguously exposes the **Respondent**'s internal evidentiary trail. It constitutes an irrefutable "Data Trigger": upon querying the Applicant's initial identifiers, the centralized mainframe did not merely isolate a routine, localized police occurrence. Rather, the systemic query unequivocally triggered a definitive hit tethered directly to an elite program or high-level database administered under the sovereign, national umbrella of the SPS

Volume #4(H)(II): The Proverbial "Pandora's Box" and the MESCIUS / GrapeCity SDK Software Connection

151. The jurisprudential ramifications of this involuntary institutional admission operate akin to the opening of a proverbial Pandora's Box, fundamentally fortifying and entirely legitimizing the Applicant's parallel requests instituted under the *Access to Information Act* concerning the deployment and unauthorized manipulation of MESCIUS and GrapeCity SDK software architectures.
152. As meticulously chronicled within the RCMP National System Architecture and Specialized Operational Support Manuals, the SPS is precisely the paramount federal directorate entrusted with the ownership, administration, and architectural construction of the RCMP's centralized, high-technology infrastructure. This sprawling mandate explicitly encompasses the CPIC mainframe itself, the Canadian Firearms Program, and the National Cybercrime Coordination center (the "NC3").
153. Therefore, the ATIP directorate was compelled to search the SPS for a singular, inescapable administrative reason: the SPS serves as the exclusive federal locus where the server-side document compilation logs and the forensic metadata manipulation sequence trails physically and electronically reside

Volume #4(H)(III): The Statutory Validation via the Treasury Board of Canada

154. This operational reality is further cemented by the Treasury Board of Canada's official Info Source publication, which formally registers and delineates the legal parameters of PIB RCMP PPU 005. This registration operates as the definitive, unassailable legal proof that the Offline Historical Database is inextricably bound to the federal statutory jurisdiction exercised by the SPS, rendering any overarching claim of "third-party ownership" over these specific architectural logs a strictly *ultra vires* proposition
155. Relying upon the foundational evidentiary maxim *habemus optimum testem, confitentem reum* (we have the best witness, a confessing defendant), the **Respondent**'s own unsolicited admission that it searched the SPS stands as the highest form of evidentiary proof that the federal apparatus was actively engaged in the architectural processing of the Applicant's data.
156. **Nota Bene:** Should the **Respondent** attempt to mitigate this admission by characterizing the unsolicited SPS search as a mere "routine administrative courtesy" or an over-inclusive clerical error, such an argument must be summarily dismissed *in limine* as an absolute nullity. The federal ATIP apparatus operates within a perpetual state of resource scarcity; it inherently does not expend computational or administrative capital to execute exhaustive forensic searches within the nation's most secure cyber-directorate absent a definitive, algorithmically generated directive necessitating that specific jurisdictional inquiry.

Volume #4(H)(IV): The Indispensable Role of Regional Communications as Cross-Jurisdictional Intermediaries and the Implication of Mr. Matt Peggs

157. Furthermore, the operational architecture of the SPS heavily implicates the substantive involvement of the Regional Communications (the "**Regional COM**") apparatus and specialized operational managers, specifically including Mr. Matt Peggs.
158. Within the highly stratified command structures of the RCMP's National Capital Region and allied specialized frameworks, Regional COM operates as the vital intermediary bridging localized municipal operations (such as the TPS or Peel Regional Police) and the paramount federal mainframe. When an investigative dossier manifests a profound jurisdictional paradox—such as the irreconcilable geographic conflict observed herein between the Toronto Courthouse and the fabricated authority of Brampton-based Justice of the Peace "George

Jiri”—routine frontline detachment channels are inherently bypassed. Such complex, multi-jurisdictional matters are statutorily escalated and routed directly through specialized Regional Command elements.

159. Because the SPS houses the Covert Operations, Cyber, and Protective Policing units any coordination of multi-jurisdictional information packages, covert data intercepts, or specialized tracking records executed by regional managers such as Mr. Peggs would automatically and inescapably be catalogued within the Specialized Investigative and Support Services repositories

Volume #4(H)(V): The Crystallization of the Rule 317 Mandate Regarding Regional Communication Logs

160. By explicitly admitting to the execution of a search within the SPS, the **Respondent** has crystallized the exact jurisdictional authority required for the Applicant to mandate the compulsory production of the comprehensive communication logs of Mr. Matt Peggs pursuant to *Rule 317*.

161. The **Respondent** is now strictly estopped from advancing the specious defense that the Regional COM office, or the communications of its managers, resides “outside the scope” of the proceeding. By formally placing the entirety of the SPS operational branch into the administrative record of its decision, the **Respondent** has voluntarily subjected the operational metadata generated by its regional managers to the transparency mechanisms of the *Federal Courts Rules*.

Volume #4(H)(VI): The Evidentiary “Smoking Gun” and the Absurdity of the Delegated Deflection

162. This explicit reference to the SPS functions as an evidentiary “Smoking Gun”—an incontrovertible admission against interest. It validates, with absolute administrative certainty, that the Applicant’s Personal Information triggered elite operational files, confirming the mobilization of national cyber-infrastructure rather than mere localized municipal records

163. Finally, this admission exposes a fatal, irreconcilable administrative contradiction within the RCMP’s prevailing posture. It highlights the profound legal absurdity of the ATIP Director formally advising the Applicant to blindly pursue records from a “municipal police force” while his own correspondence concurrently admits that the RCMP was internally compelled to interrogate its most elite, national Specialized Operational Support and Cyber branches to process the dossier

164. The **Respondent**’s attempt to obfuscate this admission beneath the guise of a “routine thorough search.” The state is legally prohibited from simultaneously asserting that a file is a mundane municipal matter while actively deploying its highest echelon of federal cyber-infrastructure to interrogate it. The **Respondent** is bound by the contradiction within its own administrative template.

VOLUME #5: CONCLUSION

I. THE TACTICAL AVOIDANCE OF PARAGRAPH 22(1)(A) AND THE UNMET BURDEN UNDER PARAGRAPH 22(1)(B)

165. The deliberate non-reliance by the **Respondent** upon *paragraph 22(1)(a)* of the *Privacy Act* represents a fatal strategic and legal error. Had the **Respondent** relied upon *paragraph 22(1)(a)* of the *Privacy Act*, it would have been inextricably compelled to demonstrate that the personal information was obtained or prepared by a specified investigative body in the course of a lawful investigation.

166. Instead, by retreating to the generalized, harm-based exemption articulated within *paragraph 22(1)(b)* of the *Privacy Act*, the **Respondent** must satisfy a rigorous and elevated evidentiary threshold. It must substantiate, with compelling exactitude, that disclosure “could reasonably be expected to be injurious to the enforcement of any law of Canada... or the conduct of lawful investigations.” The established jurisprudence of this Honourable Court emphatically dictates that “injury” under *paragraph 22(1)(b)* of the *Privacy Act* cannot be established by

107 mere speculation, boilerplate assertions, or administrative trepidation. The **Respondent** has effectively cornered itself: it has invoked an exemption necessitating clear, convincing, and objective evidence of harm to state operations, an evidentiary burden it is fundamentally incapable of discharging in relation to historical system transaction logs (the “**System Transaction Logs**”) and metadata.

II. THE HIGH THRESHOLD OF “INJURY TO THE ENFORCEMENT OF LAW” AND THE RULE OF LAW

167. Far from inflicting injury upon the administration of justice, the disclosure of the requested foundational metadata (the “**Foundational Metadata**”), the aforementioned System Transaction Logs, and the offline historical data residing within the Canadian Police Information Centre (the “**Canadian Police Information Centre**”) is absolutely indispensable to the preservation of the rule of law.
168. It is precisely the non-disclosure, withholding, or retroactive purging of audit trails and system metadata that profoundly threatens the integrity of both the *Privacy Act* and the *Criminal Code*. System logs operate as the primary and incorruptible mechanism by which state accountability and data integrity are forensically verified.
169. *Paragraph 22(1)(b)* of the *Privacy Act* cannot be improperly weaponized as an impenetrable shield to preclude the discovery of administrative malfeasance, unlawful data retention, or procedural non-compliance. The “injury” contemplated by Parliament is exclusively an injury to lawful law enforcement operations, not the exposure of systemic administrative deviations, fraudulent record manipulations, or the intentional evasion of statutory purging requirements.

III. THE TEMPORAL CEILING OF INVESTIGATIVE EXEMPTIONS AND THE IMPACT OF *R. V. JORDAN*

170. Records maintained within the Canadian Police Information Centre are fundamentally transactional in their legal character; they memorialize the administrative execution of legal process (for instance, the lodging, modification, or cancellation of a warrant). Once a legal process is completed, executed, or rendered legally defunct, it immediately loses any active investigative character.
171. In the present matter, the underlying proceedings are unequivocally stale-dated, having comfortably and substantially exceeded the presumptive constitutional ceilings promulgated in *R. v. Jordan*, [2016] 1 S.C.R. 631. Where an investigation is legally deceased, irrevocably inactive, or barred from prosecution by the constitutional effluxion of time, the **Respondent** cannot legitimately posit that the disclosure of transactional metadata relates to an active or ongoing investigation.
172. Furthermore, the disclosure of metadata pertaining to a concluded or non-existent matter cannot logically precipitate “injury” to an investigative process that lacks legal vitality. As famously articulated by Lord Denning in *MacFoy v. United Africa Co. Ltd.*, [1961] 3 All E.R. 1169 (P.C.), an act that is void is an absolute nullity; one cannot put something on nothing and expect it to stand, for something on nothing remains nothing.
173. To the extent that it could ever be suggested a valid criminal proceeding existed (namely, a properly constructed arrest warrant, even one ostensibly issued orally), there was not, at law, a valid criminal prosecution (the “**Criminal Prosecution**”). The factual reality that numerous hearings were attended, culminating in an order dismissing the frivolous and meritless charge predicated upon a non-informant within a fabricated information package (the “**False Information Package**”), is indisputable. However, as a matter of strict legal classification, the entire apparatus was void *ab initio* from the precise temporal moment the False Information Package was filed. The contravention of strict statutory dictates mandates that such actions be classified as an absolute nullity rather than a mere procedural irregularity.

IV. THE FALLACY OF INFORMANT PRIVILEGE IN RELATION TO PUBLIC COURT RECORDS AND METADATA

174. The **Respondent** endeavours to improperly conflate the identity of a confidential informant—who is traditionally safeguarded by the near-absolute evidentiary shield of informer privilege—with the identity of a

complainant or a swearing officer executing a form 2 information (the “**Form 2 Information**”) pursuant to the *Criminal Code*. This constitutes a profound and fatal legal error.

175. Firstly, upon the issuance of legal process or the execution of an arrest, a Form 2 Information is instantaneously transmuted into a public court record. The identity of the informant contained therein is rendered unequivocally public as an inextricable function of constitutional open court principles.
176. Secondly, the specific metadata requested—encompassing originating agency identifier codes (the “**Originating Agency Identifier**”), issuing court locations, judicial officer identities, and system identification numbers (the “**System Identification Numbers**”)—contains absolutely no identifying information concerning legitimately confidential informants.
177. The **Respondent**’s strategic contortion of *paragraph 22(1)(b)(ii)* of the *Privacy Act* to encompass non-identifying, ministerial court metadata represents an impermissible and *ultra vires* expansion of the confidential source exemption, a proposition that is wholly unsupported by the statutory text or established common law principles.

V. ULTRA VIRES CONDUCT, FRAUDULENT MANIPULATION, AND THE LIMITS OF “LAWFUL INVESTIGATIONS”

178. The doctrine of the indivisibility of the Crown, as elucidated in *Benedict v. Ontario (2000)*, 51 O.R. (3d) 147 (C.A.), dictates that the state cannot act in a fractured or divided capacity. The state is legally precluded from claiming the benefits of statutory protections while its agents simultaneously act in direct, deliberate contravention of the law.
179. The existence of a “lawful investigation” operates as a strict, unyielding condition precedent to the application of any exemption enumerated under *subsection 22(1)* of the *Privacy Act*. State action that is birthed from bad faith, systemic fraud, or the deliberate, calculated manipulation of institutional records is *ultra vires* and void *ab initio*.
180. Just as criminal misconduct perpetrated by an individual officer operating under the colour of authority can never be shielded under the guise of “law enforcement and investigation,” institutional acts of record manipulation or the compilation of a False Information Package cannot, under any legal fiction, be characterized as a “lawful investigation.”
181. To hold otherwise would establish a perilous precedent, permitting the state to invoke statutory privacy exemptions to conceal its own unlawful conduct—a consequence that is profoundly offensive to the principles of fundamental justice, equitable doctrines, and the explicit statutory architecture of the *Privacy Act*.

VI. THE JURISDICTIONAL LEGERDEMAIN: SECTION 19(1)(D) AND THE CENTRAL REGION METAMORPHOSIS

182. In a manifest attempt to orchestrate a sophisticated statutory evasion, the **Respondent** has invoked *paragraph 19(1)(d)* of the *Privacy Act*, alleging that the foundational records constitute personal information obtained in confidence from the government of a province or an institution thereof. This invocation is a jurisprudential sleight-of-hand designed to obfuscate the internal structural metamorphosis of the Royal Canadian Mounted Police.
183. It is a matter of administrative record that the federal entity formerly designated as “O” Division has been systematically restructured into an integrated, multi-jurisdictional intelligence hub now operating as central region command (the “**Central Region**”). The invocation of *paragraph 19(1)(d)* of the *Privacy Act* is predicated upon a deliberate mischaracterization: treating the highly integrated Central Region infrastructure—which is fundamentally federal in its apex control—as an independent “provincial institution” merely because it synergizes with municipal or provincial entities.
184. The refusal to disclose the Originating Agency Identifier, the issuing court level, and the identity of the presiding judicial officer is not animated by a genuine desire to protect intergovernmental confidences. Rather, it is a calculated manoeuvre to prevent the forensic tracing of the data directly back to the executive suites of the Central Region, specifically the purview of the regional commander (the “**Regional Commander**”).

- 109 185. The evidentiary record strongly supports the inference that the Regional Commander, acting as the multi-jurisdictional intermediary, ingested unverified data and uploaded it directly into the federal mainframe under police case identification number 457197 (the “**Police Case Identification Number**”). It is submitted that the immense institutional weight of the Regional Commander was utilized to bypass standard judicial scrutiny, allowing an irregular and fundamentally flawed authorization to be accepted on its face by the issuing justice.
186. *Nota Bene*: The **Respondent** may counter that the Central Region, by virtue of its joint-forces operations, functions *de facto* as a provincial entity for the purposes of *paragraph 19(1)(d)* of the *Privacy Act*. This argument is entirely devoid of merit and offends the doctrine of federal paramountcy. The Canadian Police Information Centre is a sovereign federal mainframe. The indivisibility of the Crown strictly precludes a federal institution from bifurcating its own hybrid command structure to artificially generate a “third-party” provincial shield where none exists at law. The data residing under the Police Case Identification Number is exclusively within the constructive possession and paramount control of the federal **Respondent**.
187. This structural obfuscation perfectly elucidates why the front-facing municipal police service was entirely incapable of producing a physical arrest warrant during the period of detention. The municipal constabulary was acting merely as the operational appendage for a data file generated, maintained, and entirely controlled within the Central Region infrastructure of the **Respondent**. The concealment of this reality through the misapplication of *paragraph 19(1)(d)* of the *Privacy Act* is *ultra vires* the **Respondent**’s statutory authority.

VII. THE APPLICATION OF EQUITABLE MAXIMS: FRAUD UPON THE LAW AND THE VITIATION OF ADMINISTRATIVE ACTS

188. The deliberate withholding of exculpatory system metadata and the invocation of inapplicable statutory exemptions must be scrutinized through the lens of established equitable maxims. As extensively catalogued in Herbert Broom’s seminal treatise, *A Selection of Legal Maxims*, the foundational premise remains resolute: fraud is proved when it is demonstrated that a false representation has been made knowingly, without belief in its truth, or recklessly, careless as to whether it be true or false.
189. Where systemic administrative operations are executed with reckless disregard for statutory prerequisites, producing a False Information Package that results in unlawful deprivation of liberty, an honest belief in the truth of the state’s actions is nullified. The motive of the state actor guilty of such reckless promulgation is rendered legally immaterial.
190. Furthermore, the equitable principle of fraudulent concealment forcefully applies to toll any procedural barriers. It has long been an axiom of equity that no length of time is a bar to relief in cases of fraud where there has been no laches on the part of the defrauded party. The maxim *nemo ex suo delicto meliorem suam conditionem facere potest* (no man can improve his condition by his own wrong) strictly precludes the **Respondent** from utilizing its own obfuscatory tactics—namely, hiding the Originating Agency Identifier and the Police Case Identification Number—to prevent the discovery of the underlying nullity.
191. The execution of legal process is bound by strict jealousy, designed to protect against fraud, collusion, and the resulting disgrace to the Crown and the administration of justice. The rule *necessitas quod cogit defendit* (necessity defends what it compels) cannot be invoked by the state when the “necessity” was entirely manufactured by its own creation of a False Information Package.
192. If an individual or an institutional entity, acting under colour of right or the colour of law, executes an illegal act or abuses the process of the court, transforming it into an instrument of oppression or extortion, such conduct constitutes a fraud upon the law. Consequently, the **Respondent** is strictly barred from availing itself of its own illegal acts.
193. It is an unassailable tenet of jurisprudence that fraud vitiates everything it touches (*fraud no doubt vitiates everything*). Where an administrative act or judicial authorization is procured through the reckless or intentional submission of a False Information Package, the resulting instrument is not merely tainted by irregularity; it is an absolute nullity, void *ab initio*, rendering the parties subject to the equitable restoration of the *status quo ante*.
194. The primary function of litigation, and indeed of the administrative tribunal process, is the untrammelled search for truth. Properly interpreted, privacy legislation is designed to promote, rather than hinder, that truth-seeking function. By deliberately refusing to execute a compliant search and by shielding the executive

VIII. THE FIDUCIARY DUTY OF DISCLOSURE AND THE EQUITABLE INTEREST IN PERSONAL INFORMATION: THE APPLICATION OF MCINERNEY V. MACDONALD

195. The jurisprudence articulated by the Supreme Court of Canada in *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 governs the incontrovertible right of an individual to access personal information held by an institutional repository. The apex Court definitively ruled that information regarding oneself, revealed to or compiled by an institution acting in a professional capacity, remains, in a fundamental and immutable sense, the property of the individual.
196. While the **Respondent** may claim structural ownership of the physical and digital architecture comprising the Canadian Police Information Centre, it must be legally emphasized that the **Respondent** acts merely as a custodian of the personal information residing therein. The Supreme Court of Canada categorically established that the subject of the records possesses a trust-like beneficial interest (the “**Beneficial Interest**”) in the substantive information itself. This equitable interest mandates that, as an unyielding general rule, the individual possesses a paramount right of access to the information, thereby imposing a corresponding obligation upon the institutional custodian to effectuate its immediate provision.
197. The relationship between the state as the repository of sensitive personal data and the individual to whom that data pertains is inextricably imbued with fiduciary obligations. A fiduciary duty (the “**Fiduciary Duty**”) inherently demands that the institutional actor conduct itself with the utmost good faith, loyalty, and transparency. To deny an individual access to their own Foundational Metadata and System Transaction Logs constitutes a profound breach of this Fiduciary Duty, effectively utilizing the confidentiality mechanisms designed to protect the individual as a clandestine shield to facilitate improper institutional conduct.
198. Furthermore, the principles of equity demand a strict reciprocity of information. The necessity for state institutions to compile sensitive, highly private data concerning an individual must be counterbalanced by a corresponding openness and full disclosure to that selfsame individual. As noted in *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, the systematic withholding of records profoundly undermines the structural integrity of the administrative system. If there has been improper conduct in the compilation or maintenance of the records—such as the reckless promulgation of a False Information Package—it is an imperative of justice that such deviations be illuminated rather than sequestered under the guise of an arbitrary statutory exemption.
199. Given the profound disparity in the evidentiary capacities of the parties, the Supreme Court of Canada explicitly mandated that the burden of proof rests entirely and exclusively upon the entity withholding the information. The onus falls squarely upon the **Respondent** to definitively justify any exception to the general rule of access. Such a denial cannot be predicated upon mere speculative administrative inconvenience or the abstract fear of subsequent litigation; it requires the demonstration of a significant likelihood of a substantial adverse effect, a threshold the **Respondent** has conspicuously failed to meet.
200. The **Respondent** possesses no unfettered discretion to arbitrarily deny access to the Originating Agency Identifier or the Police Case Identification Number. Such administrative discretion is heavily circumscribed and must be exercised upon proper equitable principles. Where the **Respondent** refuses a legitimate request for access, this Honourable Court is fundamentally empowered to exercise its superintending equitable jurisdiction, acting *in personam* to ensure the **Respondent** adheres strictly to its standard of conduct and is restrained from acting in a manner inconsistent with the applicant’s Beneficial Interest.
201. Ultimately, the deliberate obfuscation of the System Transaction Logs to insulate the machinations of the Central Region and the Regional Commander is diametrically opposed to the fiducial qualities required of a state repository. Where systemic fraud upon the law is alleged, the principles enshrined in *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 forcefully compel the immediate unsealing and production of the underlying records, affirming the paramountcy of truth-seeking over the tactical evasion of institutional accountability.
202. But it all comes back to the same issue that the **Respondent** RCMP Tribunal admitted it did not search because of its misguided understanding of the law, as scary as it is, that the *Privacy Act* does not authorize the RCMP to search files OR disclose information belongings to other police forces.

- 111 203. The RCMP Tribunal did not rely on section 18 of the *Privacy Act* so none of the Personal Information sought by the Applicant in a PIB was exempt from searching. Moreover, the RCMP Tribunal did not rely on ss. 22(1)(a) at all or even 22(1)(a)(ii) which is required in relation for reliance on an exempt bank. This was and is fatal to the RCMP Tribunal with respect to its decision that it could not search for “files”.
204. In relation to any and all Personal Information sought by the Applicant that was highly particularized as statutorily required (see: ss. 12(1)(b): under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution), the RCMP Tribunal failed to search the CPIC database, as it admitted, for Foundational Metadata and Offline Historical Database in relation to the Applicant’s Personal Information. The attached document to the April 27, 2026, decision or disposition of the Tribunal (RCMP), was not even within the spectrum of what would be produced in disclosing Foundational Metadata (i.e. the ORI; the issuing court level; the issuing court location; the name of the judicial officer; and the SID) and/or the Offline Historical Database for amended or purged originally input data including the likes of CLEAR, CANCEL, ADD, MODIFY et al type functions in relation to the Applicant’s Personal Information. It is trite that metadata is information that can be Personal Information in relation to an individual.
205. The legal test for the transmission of materials pursuant to *Rule 317* of the *Federal Courts Rules* has been comprehensively and irrefutably satisfied. The requested material was demonstrably available to the administrative tribunal in question (see: *subsection 2(1)* of the *Federal Courts Act*) at the time but nonetheless it is in its possession at the time of this *Rule 317* request:
- Relevant to the core issues on judicial review, specifically the abject failure of the **Respondent** to execute a reasonable, legally compliant search;
 - In the possession (whether actual, constructive, or joint) of the **Respondent**, acting in its capacity as the paramount administrator of the Canadian Police Information Centre; and
 - Not in the possession of the applicant.
206. As the Applicant did not include a specified request such as this in his Notice Of Application (“NOA”) it is included hereunder pursuant to *Rule 317(3)* of the *Federal Courts Rules*.

All of which is respectfully requested by Mr. Kevin A. McLean (BA, JD, CIM)



DATED at Toronto, Ontario, this 18th day of May, 2026.

Mr. Kevin A. McLean (BA, JD, CIM)

Toronto, Ontario

Applicant, Self-Represented

mclean@searchandseizure.ca

Rule 317 of the Federal Courts Rules

317 (1) A party may request anything that is relevant to the application that is in the possession of a federal board, commission or other tribunal whose order is the subject of the application and that was not when the application was made in the possession of the party.

(2) The request shall be in Form 317.

(3) The request shall be served on the tribunal and on all other parties.

(4) A request under subsection (1) may be made at any time, but if it is made after the applicant has served its record under rule 309, the request may only be made with leave of the Court.

Rule 318 of the Federal Courts Rules

318 (1) Within 20 days after being served with a request under rule 317, the tribunal shall transmit (a) the original or a certified copy of the requested material to the registry, and (b) a copy of the material to the party who requested it or a written notification that the material is not in the possession of the tribunal.

(2) Where the tribunal or a party objects to a request under rule 317, the tribunal or party shall, within 20 days after being served with the request, serve on all other parties and file a written objection stating the grounds for the objection.

(3) The Court may, on motion, examine the material and order that the material, or a portion of it, be transmitted to the registry or returned to the tribunal.

The formal transformation of the RCMP’s “O” Division into the **Federal Policing Central Region** was implemented between late **2023** and **2024**. [1, 2]

Timeline Breakdown:

- **Phase 1 (2022–2023):** The RCMP initiated a broader Federal Policing transformation plan. This included preliminary steps to decommission the old National Division and consolidate its units into Ontario’s framework.
- **Phase 2 (October 2023):** Assistant Commissioner Matt Peggs was originally appointed as the Commanding Officer of “O” Division.
- **Phase 3 (2024):** As the organizational structure shifted away from traditional geographic divisions into specialized federal regions, “O” Division was officially rebranded as **Central Region**, with Peggs carrying over his leadership as the newly titled Regional Commander.

- Nothing past this line -

Tab 4

Notice of Motion

Court File Number: T-2448-26

FEDERAL COURT

B E T W E E N:

KEVIN A. MCLEAN

Applicant

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, AND
STEPHANE BRISSON

Respondents

Notice of Motion

TAKE NOTICE THAT the Applicant, Mr. Kevin A. McLean (BA, JD, CIM), will make a motion to the Federal Court under rule 369 of the *Federal Courts Rules* “Motions in writing”, to be heard (in writing) and decided on **Wednesday, June 17, 2026 at 9:30 a.m.** or soon as thereafter.

THE MOTION IS FOR the following precise relief sought:

A. Procedural Relief

1. **Abridgment of Time:** An Order that any timelines required to be abridged are so abridged pursuant to Rule 8 of the *Federal Courts Rules*, on a *nunc pro tunc* basis where applicable;
2. **Dispensation of Compliance:** An Order varying or dispensing with strict compliance of any rule pursuant to Rule 55 of the *Federal Courts Rules*, on a *nunc pro tunc* basis where applicable;
3. **Deeming of Filing:** An Order deeming all documents submitted for filing on the day in which they were submitted to the Registry, pursuant to Rule 72.1 of the *Federal Courts Rules*;
4. **Dispensation of Proof of Service:** A Declaration and Order that the Applicant is not required to provide further proof of service upon the Respondents pursuant to Rule 73, granted *nunc pro tunc*, given the Respondents' failure to file a Notice of Appearance (Form 305).

B. Declaratory and Substantive Relief

- 117 Declaration of Contravention:** A Declaration that the Royal Canadian Mounted Police (the “RCMP Tribunal”) has contravened its mandatory statutory and procedural duties pursuant to Rule 318 of the *Federal Courts Rules*;
6. **Declaration of Disobedience:** A Declaration that the RCMP Tribunal has disobeyed a lawful process of this Honourable Court, acted in a manner that interferes with the orderly administration of justice, and impaired the authority and dignity of the Court;
7. **Mandatory Order for Compliance:** An Order compelling the RCMP Tribunal to fully comply with its duties pursuant to Rule 318 of the *Federal Courts Rules* by transmitting the complete Certified Tribunal Record to the Registry and the Applicant within twenty-four (24) hours of the issuance of this Order;
8. **Imposition of Conditions:** The imposition of such terms, conditions, and directions as this Honourable Court considers just to ensure immediate compliance, pursuant to Rule 53(1) of the *Federal Courts Rules*.

C. Leave Relating to Potential Contempt

9. **Leave for Contempt Proceedings:** An Order granting the Applicant leave to bring a motion for contempt against the RCMP Tribunal, and any specific persons facilitating the intentional breach of the orders herein, pursuant to Rule 50(1)(d) and Rules 466 and 467 of the *Federal Courts Rules*.

D. Cross-Jurisdictional Enforcement Relief

10. **Authorization for Enforcement:** An Order declaring that the Applicant is at liberty, authorized, and empowered to apply to any court, tribunal, regulatory, or administrative body, wherever located, for the recognition of this Order, and for assistance in carrying out its terms and the terms of any other order issued in these proceedings.

E. Costs and Residual Relief

11. **Costs:** Costs of this motion in favour of the Applicant on a full indemnity basis, to be assessed after this Honourable Court has rendered judgment herein;
12. **Residual Relief:** Such further and other orders of an equitable nature, predicated upon the Federal Court's equitable jurisdiction, that are fair, just, and necessary to restore the *status quo ante*.

THE GROUNDS FOR THE MOTION ARE:

A. Factual Grounds

1. The Applicant initiated this Application for Judicial Review on May 15, 2026, and it was accepted for filing on May 15, 2026 (the “Judicial Review Application”, “Statutory Application” or “Application”).
2. At its core, the **Judicial Review Application** concerns relief, *inter alia*, relating to the issues which are not subject to complaints under the Privacy Act:

- a. Failure to search for the Personal Information records in a PIB and/or within the control of the Government Institution (RCMP); and
 - b. Failure of the RCMP Commissioner (Head of the Government Institution) to discharge his duty to consider ss. 8(2)(m) in relation to the worst fraudulent manipulation of Criminal Code documents or alike under the Ontario “Information Package” in the history of our country since confederation in 1867.
3. On May 19, 2026, the Applicant served a comprehensive, formalized written request upon the RCMP Tribunal pursuant to Rule 317 of the *Federal Courts Rules* (the “Rule 317 Request”).
 4. The Respondents failed or neglected to serve, file, with proof of service, within 10 days of service of the Applicant’s Application or at all, Form 305 Notices of Appearance. As such, they are prohibited from receipt of notice of steps and service of documents in this Proceeding.
 5. The Respondents have not sought leave relating to the same.
 6. More than twenty (20) days have elapsed since the service of the **Rule 317 Request**.
 7. The RCMP Tribunal has failed, neglected, and/or refused to transmit the **Certified Tribunal Record** to the Registry and the Applicant, in direct contravention of the mandatory language of Rule 318(1).
 8. The Respondents have failed to serve and file a Notice of Appearance (Form 305) within the prescribed time, thereby forfeiting their right to notice of steps and service of documents in this proceeding.
 9. The RCMP Tribunal has a variety of undischarged, outstanding, and unfulfilled obligations under the *Privacy Act* (namely the failure in its duty to search for the Personal Information records sought) and under Rule 318.
 10. The Applicant relies on the adverse inference doctrine arising from the Respondents’ silence, default, and deliberate obfuscation.

B. Legal and Statutory Grounds

8. **The General Principle:** The motion is brought in accordance with Rule 3 of the *Federal Courts Rules* to secure the just, most expeditious, and least expensive outcome of this proceeding, with due consideration given to the principle of proportionality, the complexity of the systemic issues involved, and the overriding public interest.
9. **Statutory Interpretation (*Interpretation Act*, RSC 1985, c I-21):** The Applicant relies upon the principles of textual, contextual, and purposive construction as codified in the *Interpretation Act*, including:
 - a. **Section 10 (“Law Always Speaking”):** Statutes and regulations must be interpreted dynamically to accommodate evolving circumstances and technological realities without requiring constant legislative amendment.
 - b. **Section 12 (“Enactments Deemed Remedial”):** Enactments shall be given such fair, large, and liberal construction and interpretation as best ensures the attainment of their objects.

c. Section 25 (“Documentary Evidence”): Rebuttable presumptions regarding the admissibility and establishment of facts via documentary evidence, which stand uncontroverted due to the Respondents' default.

10. **Jurisdiction and Powers of the Federal Court (*Federal Courts Act*, RSC 1985, c F-7):** The RCMP constitutes a “federal board, commission or other tribunal” pursuant to section 2. The Court possesses concurrent original jurisdiction (ss. 17, 26), jurisdiction *in personam* (s. 43(1)), and the authority to grant extraordinary remedies, including interim orders (s. 18.2).
11. **Federal Courts Rules:** The Applicant relies upon Rules 2-8, 47, 50, 53, 55, 72.1, 73, 301, 305, 317-319, and Part 7 (Motions, specifically Rules 358-369).
12. The Applicant adopts the defined terms and relies upon the factual and legal grounds comprehensively detailed in the Notice of Application, the Rule 317 Request, and the Memorandum of Fact and Law filed in support of the Application.
13. Such further and other grounds as the Applicant may advise and this Honourable Court may permit.

THE FOLLOWING DOCUMENTARY EVIDENCE will be used at the hearing of the motion:

1. The Applicant's Notice of Application, filed on May 15, 2026;
2. The Applicant's Rule 317 Request, served May 18, 2026, and filed May 19, 2026;
3. The Applicant's Proofs of Service (dated May 19, 2026) in relation to the Notice of Application and the Rule 317 Request;
4. The Applicant's Memorandum of Fact and Law for the Application, dated June 2, 2026;
5. The Applicant's Application Record, dated June 2, 2026, and updated on June 10, 2026;
6. The Applicant's Motion Record for this Notice of Motion, including the Memorandum of Fact and Law for the Motion along with Draft Order; and
7. Such further and other documents or material that may come into the possession of the Applicant or as this Honourable Court may permit.

June 10, 2026



Digitally signed by Kevin McLean
Date: 2026.06.10 01:26:42 -04'00'
Adobe Acrobat version:
2026.001.21563

Mr. Kevin A. McLean (BA, JD, CIM)

Applicant (Self-Represented or *Pro Se* and *Pro Bono Publico*)

68 Abell Street

Toronto, Ontario

M6J 0B1

Telephone:

Fax: 416.352.0055

Email: mclean@searchandseizure.ca

120
TO:

THE REGISTRAR
Federal Court of Canada
180 Queen Street West, Suite 200
Toronto, Ontario M5V 3L6

AND TO:

(Not Applicable for service as the Respondents have failed to serve and file a Notice of Appearance in Form 305, thereby forfeiting notice of steps and service requirements pursuant to the Federal Courts Rules)

Tab 5

FEDERAL COURT

B E T W E E N:

KEVIN A. MCLEAN

Applicant / Moving Party

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, AND
STEPHANE BRISSON

Respondents

MEMORANDUM OF FACT AND LAW OF THE APPLICANT / MOVING PARTY FOR HIS NOM #1

(Motion for compliance under *rule 318 of the Federal Courts Rules*)

Table of Contents

MEMORANDUM OF FACT AND LAW OF THE APPLICANT / MOVING PARTY FOR HIS NOM #1	0
PART I — OVERVIEW AND STATEMENT OF FACTS	1
A. Overview of the Interlocutory Application and the Imperative of Judicial Review	1
I. Opening Statement	1
II. Dereliction of Statutory Duties by a creature of statute	5
B. The Procedural Default of the Institutional Respondents and the Doctrine of Waiver	6
C. The Factual Substratum and the Unprecedented Vitiating of Documentary Integrity	8
PART II — POINTS IN ISSUE	10
PART III — SUBMISSIONS (LAW AND ARGUMENT).....	11
A. The Prescriptive Mandate of rule 318 and the Absolute Nullification of Administrative Discretion	11
B. The Jurisprudential Doctrine of Constructive Possession within Decentralized Database Architectures	12
C. The Expanded Scope of the Tribunal Record in the Presence of Jurisdictional Nullities and Bias	14
D. The Repercussions of Procedural Default, Spoliation, and the Invocation of the Adverse Inference Doctrine	15

E. Dynamic Statutory Construction, the Interpretation Act and the Modernization of Evidentiary Material	16
123 F. Rule 317 Jurisprudence: The Requirement of the Certified Tribunal Record and the Open Court Principle.....	18
G. The Legal Test for Relevance Governing Compulsory Transmission.....	20
H. The Precautionary Principle and the Rule of Law Precluding Administrative Speculation	21
I. The Differential Legal Test for Prohibition Under Rule 317	21
J. Inferences Rendered Conclusive: The Discovery of Improper Motives Facilitating Meaningful Judicial Review	23
K. The Novel Legal Issues Formulated for Adjudication	23
The First Novel and Untested Issue:	23
The Second Novel and Untested Issue:.....	24
L. The Absolute Failure to Search by the Royal Canadian Mounted Police.....	25
M. Personal Information as Protected Property: The Cessation of Correction Rights Absent a Search.....	26
N. The Statutory Absurdity and the Frustration of Correction Rights under Subsection 12(2) of the Privacy Act.....	27
O. Non-Obvious Legal Theories: Institutional Complicity by Willful Blindness and the Translation Doctrine	29
PART IV — ORDERS SOUGHT	29
PART V — LIST OF AUTHORITIES.....	33
A. Statutes and Regulations	33
B. Jurisprudence (Cited and hyperlinked above)	33

PART I — OVERVIEW AND STATEMENT OF FACTS

A. OVERVIEW OF THE INTERLOCUTORY APPLICATION AND THE IMPERATIVE OF JUDICIAL REVIEW

I. Opening Statement

A. Core Issue: Failure to Search and Failure to Exercise Statutory Discretion

- The initial issue in this Application is the RCMP's, in its capacity as an Institution under the *Privacy Act* which falls on the shoulders of its Head (Commissioner Mr. Michael Duheme) **complete failure to conduct any search** for responsive records under the *Privacy Act* (and in reference to section 19 under the *ATIA* by two separate paid for by the Applicant access requests thereunder), based not on statutory criteria but on an internal, presumably emotionally but not legally justified, fear of “opening of Pandora’s box”ⁱ (with the quotation being the *idiom*) which

is known as a metaphor for a seemingly small or harmless action that ends up generating a vast, unforeseen, and unmanageable cascade of troubles (see: Merriam-Webster Online Dictionary).

2. The RCMP Commissioner, as the *Head of the Institution* under the *Privacy Act*, has **refused to consider or exercise the mandatory statutory discretion** under s. 8(2)(m) of the *Privacy Act* (and by implication s. 19 of the *ATIA*). Alternatively, his refusal to consider that clause under the *Privacy Act* is predicated upon the refusal to search for the Applicant's request **Personal Information** records in the **PII Access Request (March 11 2026)**.
3. This refusal to even *turn his mind* to the statutory duty constitutes a **jurisdictional error**, a **constructive refusal**, and a **failure to perform a public legal duty** reviewable by mandamus. Instead, the **RCMP Commissioner** was, as of May 21, 2026, away from his email "on duty" until June 19, 2026, as paradoxical as that sounds on its face (pardon the punⁱⁱ).

B. Foundational Documents as Jurisdictional Nullities

4. The Applicant's access requests arise in the context of **unequivocal jurisdictional nullities**, including the falsification and post-facto manipulation of originating criminal documents such as:
 - a. the *Criminal Code* Form 2 Information;
 - b. the Ontario "Information Package" (CCO-2-000-1...); and
 - c. a purported "Warrant for Arrest" albeit denoted on part 3 of 5 of the False Information Package as the INTAKE COURT ENDORSEMENT (SEPT 23 2024) (whatever that means in fact or at law).
5. These nullities fall squarely within the **special categories of nullity recognized by the Supreme Court of Canada in Landreville v. Boucherville (Town of) (1978)**, where the Court held that **fraud, bribery, extortion, and bad faith** constitute **exceptional forms of nullity that transcend all others and unravel everything they touch**.
6. Those **absolute nullities**, being **jurisdictional in nature**, do not—and cannot—operate to justify withholding the underlying, actual, and *de facto* **Personal Information** from the Applicant. The consequence is the opposite. As affirmed by the Supreme Court of Canada in McInerney v. MacDonald, [1992] 2 S.C.R. 138, the architecture of Canadian privacy legislation—both provincial and federal—functions in harmony with the principle that access to one's own personal information is foundational to fairness, transparency, and the avoidance of unnecessary

litigation. The statutory regimes are designed to **prevent** the very “floodgates” problem that would otherwise overwhelm provincial and federal courts (including Small Claims Courts, Superior Courts of Justice, and the Federal Court) by ensuring that requestors can obtain access to their underlying Personal Information through the statutory access mechanisms. This includes access to documents and records in their original form, as well as records that must be created pursuant to statutory definitions of “record” (for example, under the **British Columbia Freedom of Information and Protection of Privacy Act**, which expressly contemplates the creation of responsive records where necessary, along with the creation of programs, application and software to the create the original record itself or the record itself but based on the statutory and common law test, so evolving from jurisprudence interpreting the relevant statutory sections therein).

7. The **idiosyncratic and unprecedented nature** of this Proceeding is underscored by the fact that the Applicant remains, to the best of any reported judicial authority, **the only individual in Canadian legal history** who still does not know what the authentic **Criminal Code Form 2 “Information”**, the corresponding **“Information Package”**, and the **“Warrant in the First”** actually stated. This singular and anomalous deprivation of access to foundational Personal Information—information that is ordinarily available as of right to any accused person, any subject of a warrant, and any individual whose liberty or legal interests are engaged—places the Applicant in a position that is not merely irregular but **wholly foreign to the structure, purpose, and constitutional underpinnings of Canadian criminal procedure and privacy law**.
8. The subsequent **post-facto manipulation** of these documents using RCMP-owned PDF editing software — resulting in the creation of an “INTAKE COURT ENDORSEMENT (SEPT 23 2024)” unknown to the *Criminal Code*, its regulations, or any lawful judicial process — further entrenches their status as **jurisdictional nullities *ab initio***.
9. The transmission of these manipulated documents to the Ontario Court of Justice at 10 Armoury Street (the **“Transferee Courthouse”**) and thereby into the public record compounds the prejudice to the Applicant and raises profound concerns regarding **document integrity, abuse of authority, and the administration of justice**.

C. RCMP ATIP’s Responses: Compounding the Nullity and Breaching Statutory Duties

10. The RCMP ATIP Office's responses to the Applicant's *Privacy Act* request (March 11, 2026) and two *ATIA* requests have **further compounded the unlawfulness** by:

- a. refusing to search;
- b. refusing to process the requests in accordance with statutory obligations;
- c. issuing responses inconsistent with the *Privacy Act*, *ATIA*, and the *Interpretation Act*; and
- d. undermining the public trust inherent in federal access-to-information regimes.

11. These failures are not mere procedural defects — they **perpetuate and shield the underlying jurisdictional nullities**, contrary to the principles articulated in *Landreville*.

D. Federal Court Proceeding: Non-Appearance and Rule 318 Contraventions

12. In this Federal Court Proceeding, the RCMP, along with all other “Individual Respondents” has **refused to appear**, having failed to file or serve a Notice of Appearance with proof of service. This constitutes an intentional **contravention** (as defined in the Interpretation Act) of the *Federal Courts Act* and the *Federal Courts Rules*.

13. The RCMP Tribunal's refusal to transmit a **Certified Tribunal Record** under Rule 318 — a mandatory obligation in place since 2002 — represents a further **deliberate non-compliance** with the Court's procedural regime.

14. In the context of the *Landreville* principle, such conduct is not merely irregular; it is **administrative bad faith** that reinforces the Applicant's position that the underlying proceedings and documents are **void, not voidable**.

E. Public Interest and the Integrity of the Justice System

15. While the Applicant has a personal stake in the relief sought, the issues raised engage the **public interest** in:

- a. the integrity of federal law-enforcement institutions;
- b. the proper administration of the *Privacy Act* and *ATIA*;
- c. the rule of law;
- d. the accountability of federal tribunals under Rule 317 and Rule 318; and
- e. the judicial repudiation of **jurisdictional nullities arising from fraud, bad faith, and manipulation**, consistent with *Landreville*.

127 13
16. Granting leniency to a federal tribunal that has **intentionally contravened statutory duties, refused to appear, and refused to comply with mandatory procedural obligations** would undermine public confidence in the administration of justice and the stewardship of public resources.

II. *Dereliction of Statutory Duties by a creature of statute*

17. It is respectfully submitted that a profound, systemic, and egregious dereliction of statutory duty has been effectuated by the “RCMP through its deliberate, calculated, and ongoing contravention of the mandatory temporal strictures unequivocally articulated within *rule 318* of the *Federal Courts Rules*, SOR/98-106 (the “*Federal Courts Rules*”). This interlocutory motion is fundamentally necessitated to compel the immediate transmission of the **Certified Tribunal Record**.
18. The **Certified Tribunal Record** constitutes a foundational evidentiary compilation which has been unlawfully and persistently withheld by the state apparatus. This deliberate suppression obstructs the orderly administration of justice, effectively paralyzes the adjudicative function of this Honourable Court, and obfuscates the essential evidentiary matrix absolutely required for the adjudication of the underlying application for judicial review (**see: Application Record, Tab 12; page 544ⁱⁱⁱ**).
19. The compulsory production of the **Certified Tribunal Record** is by no means a mere administrative formality, nor is it a procedural nicety that may be dispensed with at the unilateral discretion of a federal board. Rather, it constitutes the very lifeblood and *sine qua non* of the judicial review mechanism. The constitutional architecture of the Canadian legal system dictates that the superior courts bear the indelible responsibility of superintending state action. Drawing upon the venerable maxims compiled by Mr. Herbert Broom, specifically *boni judicis est ampliare jurisdictionem* (it is the duty of a good judge to enlarge his jurisdiction—understood contemporaneously as amplifying the remedies of the law to achieve substantial justice), the Court must not permit administrative evasion to shrink its superintending purview. Without the untrammelled, complete, and unredacted disclosure of the materials residing within the possession of the impugned administrative body, the reviewing court is rendered effectively blind, and the constitutional imperative of superintending state action is catastrophically frustrated. The

recalcitrance demonstrated by the Royal Canadian Mounted Police in failing to adhere to *rule 318* of the *Federal Courts Rules* transcends routine procedural delay or bureaucratic inefficiency. It manifests instead as an institutional blockade, strategically designed to insulate *ultra vires* conduct from the piercing scrutiny of the Federal Court and to systematically deprive the applicant (the “**Applicant**”) of the jurisprudential tools necessary to vindicate his fundamental rights.

20. The present Motion proceeds entirely unopposed, an outcome born not of oversight, but of strategic institutional silence. The institutional and individual respondents (the “**Respondents**”) were duly, formally, and perfectly served with the originating notice of application (the “**Notice Of Application**”) and the formalized, exhaustive request pursuant to *rule 317* of the *Federal Courts Rules* (the “**Rule 317 Request**”) on May 19, 2026 (see: **Application Record, Tab 12; pages 542-580^{iv}**). A calculated administrative determination has been effectuated by the Respondents to entirely abstain from adjudicative participation, a posture manifested indisputably by their absolute failure to serve and file a notice of appearance (the “**Notice Of Appearance**”) within the statutorily prescribed temporal window. This deliberate abstention is an affront to the adversarial process and an acknowledgment of the indefensibility of their underlying administrative posture.
21. The systemic subversion of the judicial process elucidated herein is profoundly compounded and radically exacerbated by the absolute failure of the **Royal Canadian Mounted Police** to execute a constitutionally and statutorily mandated search of its offline historical database (the “**Offline Historical Database**”) and its foundational metadata (the “**Foundational Metadata**”) (see: **Application Record, Tab 1; page 12^v**). The steadfast refusal to transmit the **Certified Tribunal Record** is not merely a curable procedural irregularity or a transient defect in form; rather, it constitutes an absolute nullity, operating entirely *ultra vires* the statutory authority of the federal institution. It is demonstrably calculated to conceal an unprecedented falsification of judicial instruments that threatens not only the liberty of the Applicant but the foundational integrity, public trust, and operational veracity of the Canadian legal system collectively.

B. THE PROCEDURAL DEFAULT OF THE INSTITUTIONAL RESPONDENTS AND THE DOCTRINE OF WAIVER

22. The procedural comportment of the Respondents transcends mere administrative inadvertence, bureaucratic lethargy, or inadvertent omission. It crystallizes unequivocally into a deliberate procedural election carrying profound, irreversible legal consequences. Pursuant to the strict prescriptive language of *rule 305* of the *Federal Courts Rules*, a respondent intending to oppose an application is strictly mandated to serve and file a Notice Of Appearance utilizing the prescribed Form 305 within ten days of being served with the Notice Of Application. The architecture of the Rules does not permit ambivalence; it demands formal attornment or exacts the penalty of exclusion (see: **Application Record, Tab 12; pages 547-548^{vi}**).
23. The prescribed statutory instrument unambiguously articulates that an entity desiring to oppose the application is strictly required to file said Notice Of Appearance, failing which said entity is categorically and permanently disentitled to any future notification concerning advancing steps within the application framework. The deliberate omission by a federal institution—an entity commanding unparalleled administrative resources, backed by sophisticated internal legal directorates, and operating with a multibillion-dollar budgetary allocation—constitutes a structural default that operates *ipso facto* to nullify any participatory entitlements. The state apparatus cannot logically or legally feign ignorance of the *Federal Courts Rules*, nor can it plead resource constraints. Its silence must be construed judicially as a calculated tactical evasion, an intentional waiver of procedural rights, and a tacit admission that no viable legal defense exists to counter the Applicant’s substantive allegations.
24. Consequently, the judiciary is incontrovertibly entitled—and, it is respectfully submitted, inextricably bound by overarching equitable doctrines and the unyielding imperatives of procedural fairness owed exclusively to the Applicant—to proceed upon the uncontradicted evidentiary *acta* systematically filed before this Honourable Court. The total absence of adversarial contestation irrevocably shifts the evidentiary equilibrium. In circumstances wherein the sovereign state defaults upon its obligations to the judiciary and abandons its defense, the equitable jurisdiction of the Court demands that the requested prerogative and declaratory relief be granted *in absentia*. To do otherwise would be to reward institutional recalcitrance, prejudice the diligent Applicant, and fail to preserve the *status quo ante*, thereby permitting the perpetuation of a jurisdictional fraud without judicial consequence. The granting of such relief *nunc pro tunc* ensures that the delay engineered by the Respondents does not irreparably

prejudice the Applicant, adhering strictly to Herbert Broom's maxim *actus curiae neminem gravabit* (an act of the Court shall prejudice no man).

C. THE FACTUAL SUBSTRATUM AND THE UNPRECEDENTED VITIATION OF DOCUMENTARY INTEGRITY

25. The factual matrix underpinning this proceeding is delineated by an unprecedented, shocking, and egregious fabrication of documents purportedly authorizing severe state action and the profound deprivation of liberty. The evidentiary record demonstrates incontrovertibly that the Royal Canadian Mounted Police has never possessed, and could never have possessed at law, a validly issued warrant for arrest (the “**Warrant For Arrest**”) or a lawfully sworn information (the “**Information**”) corresponding to **Police Case ID: 457197 (see: Application Record, Tab 3; pages 74 and 325)**. The fundamental preconditions for lawful state coercion were entirely absent *ab initio*.
26. Instead of acting upon lawful authority, an entirely fabricated compilation of documents was synthetically generated, engineered, and deployed, designated herein as the false information package (the “**False Information Package**”). An authentic Information, recognized uniformly across the Province of Ontario, constitutes a meticulously structured, cryptographically secure six-page *pro forma* document generated securely within the closed-circuit integrated courts offences network (the “**ICON**”) or the modern framework for automated and networked courts (the “**FRANK**”). The False Information Package tendered herein is fatally deficient on multiple fronts: it is wholly lacking mandatory swearing attestations, entirely devoid of legitimate judicial signatures, and visibly omitting critical pages required for lawful committal (**see: Application Record, Tab 10; pages 391 and 397^{vii}**). It is a facsimile of legality designed to bypass the rigorous safeguards of the criminal justice system. As articulated in Broom's Legal Maxims, *fraus et jus nunquam cohabitant* (fraud and justice never dwell together); a document conceived in fraud cannot be permitted to vest jurisdiction in any state actor.
27. The forensic metadata deeply embedded within the **False Information Package** conclusively identifies the digital architecture utilized as the **GrapeCity Software** explicitly version 6.0.2.0 (**see: Application Record, Tab 10; pages 430-431^{viii}**). This software constitutes a commercial developer software development kit, operating entirely external to the secure, closed-circuit judicial document-generation systems utilized by the provincial and federal

131 judiciaries. The provincial judiciary does not issue 17 lawful warrants bearing commercial watermarks or third-party developer metadata tags.

28. The incontrovertible presence of this specific commercial metadata inextricably proves that the document was generated via an automated back-end script, thereby constituting a clandestine and unauthorized procedural bypass of the lawful judicial apparatus. This fabrication transcends mere subfacial deficiencies, clerical irregularities, or typographical errors; it constitutes an overt, absolute fabrication of judicial processes *ab initio*. The package engages fictitious informants (notably, a misappropriated identity of a Toronto Region Court Officer (which makes the inclusion of a fictitious judicial public officer in Justice of the Peace Mr. George Jiri, appointed to said post, in January 2024, after being a police officer with the TPS for 24 years, to Central West Region OCJ Brampton Courthouse) and falsely attributes jurisdictional authority to a fictitious judicial persona wholly devoid of any geographical or administrative nexus to the matter. It is a document engineered to deceive, rendering all subsequent state actions flowing from it absolute nullities (see: **Application Record, Tab 10; pages 391-431^{ix}**).
29. In recognition of this profound vitiation of documentary integrity, and seeking to unearth the systemic roots of this forgery, on March 11, 2026, a highly particularized demand for access to the Foundational Metadata and the Offline Historical Database was formally served upon the Royal Canadian Mounted Police. Said demand sought the precise extraction of the originating agency identifier (the “**Originating Agency Identifier**”), terminal identification protocols, system identification numbers, and the raw cryptographic audit trails reflecting any amended, overwritten, or purged data within the Canadian Police Information Centre (“**CPIC**”) (see: **Application Record, Tab 1; pages 8-15^x**). These elements constitute the irrefutable digital fingerprints of state action, the unalterable hexadecimal truth of who inputted the fraudulent data and when.
30. Following the deliberate administrative obstruction of this initial demand, on May 19, 2026, and following the lawful issuance of the Notice Of Application (Form 301), the Applicant formally served the exhaustive thirty-nine-page **Rule 317 Request** upon the Tribunal (see: **Application Record, Tab 12; page 542^{xi}**). Pursuant to the strict grammatical and statutory imperatives of *rule 318* of the *Federal Courts Rules*, the Tribunal was unequivocally compelled to transmit the requested material to the Registry within twenty days.

132 31. The temporal limitation has incontrovertibly expired¹⁸ the Tribunal has engaged in absolute and unyielding silence, failing to transmit the **Certified Tribunal Record**, failing to provide written notification that the material is absent from its possession, and failing to file any formal written objection stating grounds for refusal (see: **Application Record, Tab 12; pages 560-562^{xiii}**). Such systemic obfuscation epitomizes institutional recalcitrance, operates as a continuing fraud upon the administration of justice, and necessitates immediate, superintending judicial intervention *in limine* to aggressively restore the rule of law.

PART II — POINTS IN ISSUE

15. The present interlocutory motion necessitates the rigorous, uncompromising adjudication of the following determinative issues of law, statutory interpretation, and procedural enforcement, all of which bear heavily upon the equilibrium between state power and individual rights:
- a. **Issue 1:** Whether the deliberate, unexcused, and continuing failure of the Royal Canadian Mounted Police to transmit the **Certified Tribunal Record**, or to formally object thereto, within the mandatory twenty-day statutory period prescribed by *rule 318* of the *Federal Courts Rules* constitutes an absolute nullity, an actionable breach of public duty, and an affront to the rule of law necessitating mandatory injunctive relief.
 - b. **Issue 2:** Whether the jurisprudential doctrine of constructive possession dictates that the Offline Historical Database, the Foundational Metadata, and the encompassing CPIC digital architecture reside absolutely within the possession, oversight, and paramount control of the Royal Canadian Mounted Police for the strict purposes of compulsory documentary production, regardless of jurisdictional deflection attempts.
 - c. **Issue 3:** Whether the legally permissible scope of material mandated for transmission is substantially expanded beyond the immediate administrative record in circumstances where prerogative writs of *mandamus* and *prohibition* are actively sought concurrently with meticulously pleaded allegations of institutional bias, synthetic document fabrication, and profound procedural unfairness.
 - d. **Issue 4:** Whether the absolute procedural default of the Respondents warrants the immediate invocation of the adverse inference doctrine and the equitable principles of spoliation, thereby compelling the

immediate issuance of mandatory orders *in absentia* to rectify the jurisdictional overreach and prevent the destruction of systemic evidence.

- e. **Issue 5:** Whether the equitable jurisdiction of the Federal Court demands the piercing of administrative obfuscation to compel the revelation of digital artifacts and audit trails, ensuring that state actors are strictly precluded from leveraging their own decentralized databases and technological complexities as mechanisms for concealing *ultra vires* actions from judicial oversight.

PART III — SUBMISSIONS (LAW AND ARGUMENT)

A. THE PRESCRIPTIVE MANDATE OF RULE 318 AND THE ABSOLUTE NULLIFICATION OF ADMINISTRATIVE DISCRETION

16. The linguistic architecture of *rule 318* of the *Federal Courts Rules* is meticulously constructed upon imperative, non-discretionary, and unyielding terminology. Subsection 318(1) dictates with absolute precision that the tribunal “shall transmit” the requested material within twenty days after being served with a request under *rule 317*. It is a foundational axiom of statutory construction, codified explicitly within section 11 of the *Interpretation Act*, RSC 1985, c I-21 (the “*Interpretation Act*”), that the expression “shall” is to be construed as unconditionally imperative. It functions to entirely strip the subject administrative entity of any residual elective capacity, substituting administrative whim with binding legal duty.
17. Upon receipt of the **Rule 317 Request**, the Royal Canadian Mounted Police was entirely bereft of statutory discretion to unilaterally abstain from compliance. As exhaustively articulated within the **Rule 317 Request** itself, the framework of the *Federal Courts Rules* establishes a strict, mutually exclusive procedural dichotomy: a tribunal must either physically transmit the documentation, or it must formally file an objection (**see: Application Record, Tab 12; page 547^{xiii}**). Should an administrative tribunal ascertain that a request is ostensibly overbroad, encumbered by public interest immunity, protected by solicitor-client privilege, or technically burdensome to execute, the singular lawful trajectory available to it is to file a formal written objection pursuant to *rule 318(2)* within the identical twenty-day temporal window, stating the precise and particularized grounds for such objection. Unilateral silence is not a legally permissible response under the *Rules*.

18. The Respondents herein executed neither compliance nor formal objection; they elected to simply ignore a lawful process of the Federal Court. It is respectfully submitted that this omission does not constitute a mere curable irregularity amenable to subsequent administrative ratification or retrospective apologies. Rather, it represents an absolute nullity. A deliberate circumvention of a mandatory procedural directive designed to facilitate the constitutional function of judicial review directly subverts the administration of justice. It aggressively elevates the administrative tribunal above the sovereign authority of the judiciary, creating an intolerable paradigm where the state decides which judicial rules it will obey.

19. By failing to respond in any capacity, the Tribunal renders itself *functus officio* regarding its ability to subsequently resist the scope of the request. Having waived the statutory window to object, it cannot now be heard to complain of the breadth or complexity of the production demanded. In accordance with the venerable equitable maxim *ubi jus ibi remedium* (where there is a right, there is a remedy), the Federal Court is imbued with both the inherent jurisdiction and the explicit statutory authority to compel the strict, unmitigated execution of the Tribunal's neglected duties. This ensures that the state apparatus remains inextricably subordinate to the rule of law and accountable to the superior courts.

B. THE JURISPRUDENTIAL DOCTRINE OF CONSTRUCTIVE POSSESSION WITHIN DECENTRALIZED DATABASE ARCHITECTURES

20. A masterful, progressive, and purposive comprehension of the legal doctrine of possession is absolutely paramount when navigating the compulsory production mandates enshrined within the *Federal Courts Rules*. It is a well-settled jurisprudential axiom that the concept of possession vehemently rejects the archaic, restrictive limitations of mere physical, geographic custody, paper-based storage, or narrow proprietary ownership. The law recognizes that control transcends the physical filing cabinet.

21. In the seminal authority of *Canada Post Corp. v. Canada (Minister of Public Works)*, [1995 CanLII 3574](#) (FCA) (the “*Canada Post Decision*”), the Federal Court of Appeal conclusively established that possession within the context of federal access and production must be subjected to a highly practical, functional, and expansively modern interpretation. The appellate court definitively held that control encompasses “ultimate, immediate, full, partial, transient, lasting, *de jure*, and/or *de facto* control.” The Court reasoned logically that if Parliament had intended to

restrict the notion of control exclusively to documents over which the government exercises lasting physical and proprietary disposition, it would have explicitly legislated such a constraint. The absence of such constraint dictates a broad interpretation.

22. This expansive interpretative doctrine was further fortified, clarified, and meticulously applied by the Court of Appeal for Ontario in *Ontario (Criminal Code Review Board) v. Hale*, [1999 CanLII 3805](#) (ONCA) (the “*Hale Decision*”). In that instance, the appellate court established that an institutional entity undeniably possesses material if it wields the legal right, the administrative power, or the technological authority to command its retrieval. This holds completely independent of whether the material is physically contained within the institution’s localized administrative offices or hosted remotely by a delegated third-party contractor. In the digital age, the absolute right to demand and extract data equates incontrovertibly to constructive possession.
23. Applied *a fortiori* to the present factual matrix, and as forcefully submitted within the **Rule 317 Request**, the Canadian Police Information Centre and its underlying Offline Historical Database represent a colossal, centralized national technological infrastructure. This digital panopticon is exclusively administered, secured, governed, and physically hosted by the Royal Canadian Mounted Police (see: **Application Record, Tab 12; page 555^{xiv}**). When transactional metadata, origin identifiers, or automated hexadecimal audit trails are autonomously generated by the federal mainframe in response to a decentralized data input, the Royal Canadian Mounted Police holds the supreme administrative credentials, the overarching cryptographic keys, and the unassailable legal right to extract, audit, and produce this intelligence. They are the sovereign gatekeepers of the data.
24. As comprehensively delineated within the thirty-nine pages of the **Rule 317 Request**, the structural reorganization of the Royal Canadian Mounted Police’s ‘O’ Division into the Central Region under Regional Commander Mr. Matt Peggs inextricably links the paramount federal apparatus to the impugned systemic action (see: **Application Record, Tab 12; page 580^{xv}**). Consequently, the raw forensic mainframe ledger records, the system identification numbers, and the **Foundational Metadata** reside indisputably within the constructive, *de jure*, and *de facto* possession of the Royal Canadian Mounted Police. Any theoretical assertion or administrative deflection attempting to posit that such integral systemic data “belongs” to external municipal entities constitutes a profound legal absurdity. It is a *reductio ad absurdum* that offends the purposive interpretative mandate established by the FCC

and attempts to unlawfully weaponize the complexity of a decentralized database to evade clear statutory production obligations.

25. Lest the Respondents belatedly attempt to assert that extracting precise hexadecimal data constitutes the impermissible “creation” of a new record rather than the production of an existing one, such an anticipated counter-argument is entirely legally bankrupt. The translation of existing digital arrays into human-readable logs via established querying protocols constitutes the fundamental extraction of extant material, not the generation of novel documentation. The data exists unconditionally within their servers; formatting it for judicial consumption is a strict duty of transmission, not an act of creation).

C. THE EXPANDED SCOPE OF THE TRIBUNAL RECORD IN THE PRESENCE OF JURISDICTIONAL NULLITIES AND BIAS

25. As a matter of general procedural orthodoxy, the materials requisitioned under *rule 317* encompass exclusively the documentation that was physically before the administrative decision-maker at the precise moment the impugned decision was rendered. However, a substantially broader, highly penetrating, and investigative scope of disclosure is stringently mandated in circumstances where a breach of procedural fairness, actual institutional bias, systemic fraud, or the pursuit of prerogative relief is explicitly pleaded before the reviewing court. The standard boundaries of the record dissolve when the integrity of the process itself is the subject of the challenge.
26. In the binding appellate authority of *Air Passenger Rights v. Canada (Attorney General)*, [2021 FCA 201](#) (the “*Air Passenger Rights Decision*”), the Federal Court of Appeal comprehensively delineated the expanded evidentiary obligations of a tribunal facing such severe allegations. The Court confirmed that where equitable relief in the nature of *prohibition* is sought, or where bias and breaches of natural justice are alleged, documents in the possession or control of a tribunal that are relevant to those specific allegations are strictly subject to disclosure. This is mandated irrespective of whether they formed the immediate, formal administrative record reviewed by the decision-maker.
27. The rationale underpinning this expansion is self-evident and logically impeccable: the reviewing court cannot possibly adjudicate allegations of systemic fraud, hidden bias, or the fabrication of evidence if it is artificially restricted to reviewing only the sanitized, curated record that the biased or fraudulent decision-maker unilaterally

chose to consider and present. The fundamental tenet *nemo iudex in causa sua* (no one is judge in his own cause)

demands that the veil of administrative secrecy be forcefully pierced when the jurisdictional integrity of the tribunal itself is fundamentally impugned.

28. The underlying Application explicitly pursues prerogative writs of *mandamus* and *prohibition*, conjoined inextricably with substantive, meticulously particularized allegations of institutional fraud upon the court effectuated via the synthetic fabrication of the False Information Package (see: **Application Record, Tab 12; page 565^{xvi}**). Furthermore, as articulated consistently by Federal Court jurisprudence, an application seeking *mandamus* inherently broadens the spectrum of relevance. The very failure or refusal of the tribunal to make a lawful determination, to conduct a mandatory search, or to acknowledge the existence of fabricated evidence constitutes the underlying catalyst for the judicial review.
29. Therefore, the forensic metadata, the GrapeCity Software sequence trails, the audit logs reflecting the origin and potential post-hoc alteration of the Originating Agency Identifier, and the eighteen highly specific categories of **Offline Historical Database** entries scheduled within the **Rule 317 Request** are strictly, fundamentally, and unequivocally relevant to the disposition of the Applicant's claims (see: **Application Record, Tab 12; pages 570-572^{xvii}**). The Federal Court must not be deprived of the granular evidentiary foundation absolutely necessary to adjudicate the existence of a jurisdictional nullity and to formulate the precise terms of the requested prerogative writs designed to halt the abuse of process.

D. THE REPERCUSSIONS OF PROCEDURAL DEFAULT, SPOILIATION, AND THE INVOCATION OF THE ADVERSE INFERENCE DOCTRINE

30. The calculated dereliction exhibited by the Respondents in omitting the submission of the **Notice Of Appearance** (which is the evincing the mere intent to oppose the Application) and failing to transmit the **Certified Tribunal Record** operates to definitively substantiate the incontrovertible truth that the state apparatus is fundamentally incapable of legally justifying *its refusal to search*. The silence of a highly resourced federal institution in the face of grave allegations of document fabrication and liberty deprivation is legally deafening. It serves as an unmistakable signal of institutional culpability and an inability to produce exculpatory evidence.

31. The doctrine of spoliation and the venerable evidentiary maxim *omnia praesumuntur contra spoliatores* (every presumption is made against a wrongdoer) are inextricably engaged and highly relevant in this factual matrix. This doctrine originates in equity to prevent parties from benefiting from the destruction or concealment of vital evidence. When an entity exercises exclusive, monolithic control over the singular evidentiary repository that can definitively prove or disprove an allegation of systemic fraud, and that entity deliberately suppresses or refuses to produce the data in flagrant defiance of a mandatory court rule, the law rightfully commands the drawing of a severe adverse inference. Furthermore, as codified in Broom's Maxims, *suppression veri, expressio falsi* (the suppression of truth is equivalent to the expression of falsehood); the refusal to produce the logs is a tacit admission of the falsity of the underlying warrants.
32. The deliberate suppression of critical metadata, disguised inadequately beneath the specious veil of administrative silence and procedural default, precipitates the irrebuttable presumption that the withheld documentation would be fundamentally adverse to the Respondents' position. The self-evident conclusion extrapolated from such glaring omissions dictates that the Offline Historical Database either incontrovertibly corroborates the alleged nullities regarding the GrapeCity Software manipulations (see: **Application Record, Tab 10; pages 430-43^{xviii}1**), or proves definitively that the authentic judicial authorizations (the warrants and informations) are, and always were, entirely non-existent.
33. Where an institutional actor intentionally abstains from challenging a comprehensive evidentiary matrix demonstrating *ultra vires* statutory contravention, the scales of the balance of probabilities are tipped inexorably and permanently in favour of the Moving Party. The Applicant has exhaustively discharged his initial evidentiary burden; the state's deliberate default transforms the Applicant's meticulously pleaded allegations into established judicial facts, ripe for the issuance of declaratory and mandatory relief.

E. DYNAMIC STATUTORY CONSTRUCTION, THE INTERPRETATION ACT, AND THE MODERNIZATION OF EVIDENTIARY MATERIAL

34. The statutory obligations imposed upon the Tribunal by the *Federal Courts Rules* and the *Privacy Act* must be construed through the progressive, purposive, and modernizing lens mandated by the *Interpretation Act*. Section 10 of the *Interpretation Act* codifies the fundamental, dynamic principle that the law shall be considered as always

speaking. The Federal Court of Appeal has consistently affirmed that statutes must be interpreted dynamically to apply seamlessly to changing technological realities, evolving circumstances, and novel forms of data architecture without requiring perpetual, reactive legislative intervention.

35. The concepts of “material,” “record,” and “possession” within the *Federal Courts Rules* must not be artificially frozen in anachronistic, paper-based historical paradigms of the twentieth century. The open-textured, flexible interpretation required by Section 10 strictly demands that algorithmic sequence trails, digital artifacts, hexadecimal data arrays, cryptographic signatures, and encrypted audit logs be recognized as tangible, discoverable “material” subject to compulsory transmission under *rule 318*. Data is the modern document or the material in the format known to the RCMP Tribunal.
36. Concurrently, section 12 of the *Interpretation Act* designates all enactments as inherently remedial, necessitating a fair, large, and liberal construction that best ensures the attainment of their objects. The overarching object of *rule 318* is to ensure absolute transparency, accountability, and to facilitate the Federal Court’s essential constitutional role of judicial review over the executive branch. To permit the Royal Canadian Mounted Police to exploit the profound technological complexity of its own decentralized database architecture as a jurisprudential shield against production would violently frustrate this remedial purpose and entirely vitiate the transparency mechanisms of the Federal Court (**see:** Application Record, Tab 12; page 580^{xix}).
37. The foundational nullities embedded deeply within the orchestrated process invoke the immutable equitable doctrine of *quod ab initio non valet, in tractu temporis non convalescit* (that which is invalid from the beginning does not gain validity by the passage of time). The fabrication of the **False Information Package** was an absolute nullity at its inception wherein a “false document” was created at its time of creation but then when it was filed the Criminal Proceeding ceased to exist, and certainly no “Criminal Prosecution” could even commence. The continuing failure to transmit the **Certified Tribunal Record** constitutes an ongoing, intentional perpetuation of this original nullity. The equitable jurisdiction of this Honourable Court is thus profoundly engaged, commanding the immediate issuance of the requested mandatory orders to compel the revelation of the digital truth, dismantle the fraudulent construct, and mandate the restoration of the *status quo ante*.

38. Consistent with settled jurisprudence governing the open court principle (the “**Open Court Principle**”) entrenched within subsection 2(b) of the *Canadian Charter of Rights and Freedoms* (the “*Charter*”), informations and indictments (the “**Informations**” and “**Indictments**”) are unequivocally treated as public judicial *acta* upon the issuance of a process, the service of a *Criminal Code* Summons, or the execution of a *Criminal Code* Form 7 Arrest Warrant. The Open Court Principle serves as the bulwark of a democratic society, ensuring that the coercive powers of the state are exercised under the sanitizing light of public scrutiny. Furthermore, any corresponding endorsements promulgated by a judicial officer (the “**Endorsements**”) thereto are strictly required to be made available upon formal request by an accused party—devoid of prescribed fees—or to the public writ large, subject to the prescribed fee schedule delineated within *Regulation 158/03*. Secret warrants are anathema to the Canadian legal tradition. Even worse are constating and originating documents and “warrants for arrest” that falsified post facto. But the worst of all are those falsified originating documents and “warrants for arrest” by any other name like an INTAKE COURT ENDORSEMENT (SEPT 23 2024) that are then filed in a “Transferee Courthouse” like they were herein.
39. Analogously, within the rigorous administrative framework of taxation, it has been definitively established that the Canada Revenue Agency, pursuant to an adversarial request under *rule 317* of the *Federal Courts Rules*, forwarded a certified copy of an information (the “**Tax Information**”) directly to the Registry. Said document was subsequently and properly treated by the Registry as a public document, with a formalized copy concurrently remitted to the applicant’s counsel, as articulated clearly in *Rémillard v. Canada (National Revenue)*, [2020 FC 1061](#) at [paragraph 5](#) (the “*Rémillard Decision*”). The transmission effectively placed the document into the public domain.
40. Documentation transmitted pursuant to *rule 318* of the *Federal Courts Rules* is strictly incorporated into the receiving Court’s official records and is governed *ipso facto* by the Open Court Principle (see: [Rémillard Decision](#), at [paragraphs 25–26](#) and [37–38](#)). Rules 23 and 26 of the *Federal Courts Rules* categorically mandate that the Court file and its respective annexes be treated as fully publicly accessible. This principle remains inviolate, subject

exclusively to targeted statutory confidentiality frameworks or specific, narrowly tailored judicial sealing orders granted only upon a stringent evidentiary showing.

41. The procedural mechanism outlined in *rules 317 and 318* of the *Federal Courts Rules* is strictly operational, administrative, and non-exploratory; its foundational function is solely to transition relevant materials from the exclusive possession of the state into the neutral possession of the Registry. This process is entirely distinguishable from private civil discoveries executed beyond the purview of the Court file (see: [Remillard Decision](#), at paragraphs [57–59](#) and [65–66](#)). Private discoveries are rigidly governed by the implied undertaking rule, restricting secondary use of the information, subject only to questions from discovery being formally read into the court record by affidavit or during a public hearing. *Rule 317* suffers from no such limitations.
42. Should the Respondent Royal Canadian Mounted Police Tribunal attempt to advance the specious, deflecting argument that the Applicant is utilizing *rule 317* as an impermissible exploratory discovery mechanism or a “fishing expedition,” such an assertion is preemptively and resoundingly defeated. The incontrovertible fact remains that the requested records constitute the foundational administrative documents that inherently form the absolute basis of the tribunal’s jurisdiction and its subsequent, or maliciously omitted, actions. One cannot “fish” for the very documents that purportedly authorized one’s own arrest (see: **Application Record, Tab 3; pages 74 and 325^{xx}**).
43. The protections afforded under section 8 of the *Charter* regarding unreasonable search and seizure are rendered wholly inapplicable *in limine*, as no reasonable expectation of privacy (the “**Reasonable Expectation of Privacy**”) can legally persist subsequent to an applicant affirmatively requisitioning the transmission of his own records pursuant to *rule 317* of the *Federal Courts Rules* (see: [Remillard Decision](#), at paragraphs 163–165). The Applicant seeks his own data, effectively waiving any privacy shield the state might attempt to erect to prevent disclosure.
44. Generally, *rule 317* of the *Federal Courts Rules* encompasses exclusively the material that was available to the administrative decision-maker at the precise time the impugned decision was rendered (see: [Remillard Decision](#), at paragraphs [23](#), [39](#), and 41–42). However, as aforementioned, a substantially broader scope of disclosure is stringently mandated in circumstances where procedural fairness, reasonable apprehension of bias, systemic fabrication, or analogous equitable grounds are explicitly contained within the Notice of Application and supported by a cogent evidentiary foundation: *Lill v. Canada*, [2023 FC 1364](#). Such grounds are unequivocally established

herein by the detailed notice of application (the “**Notice of Application**”), by the very Application Record and Motion Record, which evidences another default by the RCMP ATIP Branch in ATIA Request #2 without even the pretense of an explanation, formally filed by the Applicant. ATIA Request #2 could not even demonstrate even the purported reliance on an extension of time by even citing a section under the extension of time provision of ATIA and then misled the Applicant about his complaint rights under ATIA which occur when the extension is taken not an alleged 60 days after the RCMP ATIP Branch presumably fails to meet its self-created standard. By the falsely relied upon extension of time under ATIA Request #1, the RCMP ATIP Branch has until Monday, June 14, 2026, to provided the requested “records” as per section three thereunder. This is, in part, why the Applicant has selected Wednesday, June 17, 2026, as the date of the written hearing for the NOM #1.

G. THE LEGAL TEST FOR RELEVANCE GOVERNING COMPULSORY TRANSMISSION

45. For the strict analytical purposes of *rule 317* of the *Federal Courts Rules*, a document is deemed legally relevant to an application for judicial review if it possesses the inherent capacity, logic, or evidentiary weight to affect the ultimate decision that the Court will render on the application. This threshold has been conclusively articulated in *Douze v. Canada (Citizenship and Immigration)*, [2010 FC 1086](#) at paragraph 19 (the “*Douze Decision*”), and reinforced comprehensively in *Boudreau v. Canada (Revenue Agency)*, [2022 FC 792](#) (CanLII) at paragraph 16 (the “*Boudreau Decision*”).
46. In the [Douze Decision](#), the Honourable Madam Justice Tremblay-Lamer explicitly adopted the authoritative, binding instruction provided by the Federal Court of Appeal in *Canada (Human Rights Commission) v. Pathak*, [1995 CanLII 3591 \(FCA\)](#) (the “*Pathak Decision*”), regarding the precise parameters of relevance under *rule 317*. The appellate instruction dictates that a document is relevant if it may affect the decision of the Court, determined strictly in relation to the specific grounds of review set forth in the originating notice and the supporting evidentiary affidavits.
47. The *ratio decidendi* established in the *Douze Decision* has been consistently, rigorously, and forcefully affirmed across numerous subsequent decisions, cementing the operational legal test into the bedrock of Federal Court procedure. This includes the application in *Chopra v. Canada (Public Safety and Emergency Preparedness)*, [2026](#)

Justice Diner confirmed the well-established alignment of relevance tests, stipulating that relevance is determined strictly against the grounds of review and the affidavits filed in support thereof. The relevance of the material requisitioned under *rule 317* is the singular, overriding determinative factor authorizing its compulsory transmission.

H. THE PRECAUTIONARY PRINCIPLE AND THE RULE OF LAW PRECLUDING ADMINISTRATIVE SPECULATION

48. As explicated masterfully by the Federal Court of Appeal in *Canadian Copyright Licensing Agency (Access Copyright) v. Alberta*, 2015 FCA 268 at paragraph 15 (the “*Access Copyright Decision*”), parties before an administrative decision-maker will frequently, but not universally, possess all the material that the decision-maker considered. In instances of profound uncertainty, systemic obfuscation, or suspected bad faith, *rule 317* of the *Federal Courts Rules* provides the definitive statutory mechanism by which parties can pierce the administrative veil to confirm exactly what the administrative entity considered, thereby precluding conjecture and ensuring parity of arms (see also: *Friends of the Earth Canada v. Canada (Attorney General)*, [2023 FC 1438](#) (CanLII) at paragraph 9).

49. Herein, the factual reality is stark: the Applicant possessed nothing then, and possesses nothing now; concurrently, the Court possessed nothing then, and possesses nothing now. The absolute dearth of documentary transparency perpetrated by the Respondents transforms the theoretical utility of *rule 317* into an urgent, unassailable judicial imperative. The Court cannot adjudicate in a vacuum deliberately engineered by the state.

I. THE DIFFERENTIAL LEGAL TEST FOR PROHIBITION UNDER RULE 317

50. In *Air Passenger Rights v. Canada (Attorney General)*, [2021 FCA 201](#) (the “*Air Passenger Rights Decision*”), Associate Justice Gleason of the Federal Court of Appeal delineated the profound, necessary expansion of the disclosure test at paragraph 21. The Court explicitly recognized that the breadth of materials subject to disclosure under *rules 317* and *318* is substantially broadened where institutional bias or a fundamental breach of procedural

fairness is alleged, particularly where extraordinary relief in the nature of prohibition is sought. In such grave circumstances, disclosure is not artificially limited to the immediate materials before the tribunal.

51. The appellate reasoning is flawless and constitutionally sound: were the strict limitation maintained, the reviewing Court would be systematically deprived of the evidence absolutely necessary for the disposition of an applicant's claims of bias or breaches of procedural fairness, rendering the availability of relief in the nature of prohibition a purely illusory legal fiction. A tribunal guilty of bias will rarely compile a record that openly advertises its own malfeasance. By analogy from the SCC in 1990, *MacDonald Estate v. Martin*, it is one of those things that is not only not subject to proof but disproof.
52. Allegations encompassing overt institutional bias, synthetic documentation generation, and profound breaches of procedural fairness have been meticulously pleaded and are comprehensively encapsulated within the operative iteration of the application record (the "**Application Record**") (see: **Application Record, Tab 12; pages 565-568^{xxi}**). Concurrently, prerogative relief in the form of a writ of prohibition is actively, forcefully, and necessarily sought by the Applicant to halt the ongoing abuse of process.
53. *Ipso facto*, given that the extraordinary remedies of *mandamus* and *prohibition* are concurrently pursued, the restrictive legal test evaluating solely the materials available at the precise moment of the Royal Canadian Mounted Police Tribunal's decision is fundamentally inapplicable. While the Applicant submits that even this narrower threshold would nonetheless be satisfied given the specific *Privacy Act* context, the prevailing appellate jurisprudence unequivocally binds this Honourable Court, by virtue of vertical *stare decisis*, to compel the Tribunal to transmit the expansive array of materials in certified format.
54. Should it be speculatively argued by the recalcitrant Respondents that the broader array of documents falls outside the technical "control" of the decision-maker because they were not explicitly reviewed by the specific analyst assigned to the file, such an argument constitutes a profound logical fallacy. The binding jurisprudence explicitly overrides this artificial limitation where bad faith, bias, or procedural fairness are formally pleaded, fundamentally transferring the metric of discoverability from "what was actively reviewed by a specific clerk" to "what exists within the institution that may affect the Court's disposition of the fairness allegations."

55. It is an accepted, foundational legal tenet that the certified record and its surrounding systemic context may unveil whether an administrative decision was predicated upon an improper motive, infected by bias, or driven by alternative, impermissible rationales, as established powerfully in *Canada (Minister of Citizenship and Immigration) v. Vavilov*, [2019 SCC 65](#) at paragraph 137. The record is the window into the administrative mind or, by *supra*, the “Pandora’s box”.
56. In the event that the reviewing court is maliciously deprived of the evidentiary foundation relied upon—or deliberately avoided—by the administrative decision-maker, the detection of a reviewable error may be rendered a functional impossibility (see: *Access Copyright Decision* at paragraph 14). The paramount and overarching consideration guiding this Honourable Court is whether the requested disclosure will permit a meaningful and substantive judicial review of the impugned state action, as affirmed in *GCT Canada Limited Partnership v. Vancouver Fraser Port Authority*, [2021 FC 624](#) at [paragraph 26](#). Without the metadata and the historical logs, review is reduced to a meaningless rubber-stamping exercise.

K. THE NOVEL LEGAL ISSUES FORMULATED FOR ADJUDICATION

57. The novel legal controversies presented for adjudication herein are robust, multifaceted, and entirely untested in Canadian administrative jurisprudence. It is axiomatic that these issues fundamentally engage the broader public interest, extending far beyond the immediate evasive tactics deployed against the Applicant, and possess central, systemic importance to the integrity of the administration of justice across Canada. The resolution of these distinct, untested issues will be effortlessly achieved upon the compulsory transmission of the **Certified Tribunal Record** to both the Federal Court and the Applicant. The subsequent enumeration is strictly illustrative, explicitly provided to pre-empt and neutralize any unnecessary, frivolous, or meritless objections the Respondent may attempt to resurrect *ex post facto*.

The First Novel and Untested Issue:

58. A primary determinative issue hinges upon whether the originating data sequence inputted into the CPIC repository—irrespective of the specific law enforcement agency acting as the originating terminal, whether acting as a principal or an agent, and under whatever alphanumeric case identification number—materially mirrored the contents of the admitted False Information Package (see: **Application Record, Tab 10; pages 391 and 397^{xxii}**). Should the inputted data align with said fabricated package, the Applicant is undeniably entitled to its disclosure as his proprietary **Personal Information** notwithstanding the fact that the underlying data is demonstrably false and synthesized: *Lawson v. Accusearch Inc.*, [2007 FC 125](#). Falsity of data does not negate its classification as Personal Information belonging to the subject.

The Second Novel and Untested Issue:

59. The subsequent issue necessitates an inquiry into whether the initial data matrix entered into CPIC—specifically referencing a “warrant in the first” and the identifier “MCLEAN, Kevin”—was structurally accurate at the precise moment of inception, irrespective of the underlying, contested merits of the “Ex Parte In Camera Hearing”. Crucially, the Court must determine if this data was subsequently subjected to *post-hoc* amendment, either prior to or immediately following the physical arrest of the Applicant. If the metadata was technically correct at the first instance, but later strategically altered to forcefully synchronize with the relevant data points required by CPIC (specifically the **Foundational Metadata**, encompassing the Originating Agency Identifier; the designated issuing authority; the narrative field; and the System Identification Number generated upon entry), such alterations constitute a profound, actionable abuse of process designed to retroactively validate an unlawful detention.
60. It is submitted as a highly probable extrapolation that the originating law enforcement agency, designated by the initial Originating Agency Identifier, was demonstrably not the identical agency that subsequently executed the surreptitious amendments to the WANT record. These potential, unauthorized systemic alterations encompass distinct vectors of modification, including the deliberate reassignment of the Originating Agency Identifier to falsely transfer jurisdictional appearance, and the systemic desynchronization of the System Identification Number to obfuscate the original timestamp. The forensic veracity of these administrative maneuvers can only be

illuminated through a rigorous examination of the automated hexadecimal transaction logs, compelling the unmitigated disclosure of the Applicant's Personal Information.

L. THE ABSOLUTE FAILURE TO SEARCH BY THE ROYAL CANADIAN MOUNTED POLICE

61. In light of the above uncontroverted syllogism and the administrative sophisms deployed by the Royal Canadian Mounted Police, the *Privacy Act* not only authorizes but statutorily obligates the federal institution to search for the Personal Information requested within the scope of an access request. This obligation applies unequivocally whether the data resides in a personal information bank (the “**Personal Information Bank**”) and has been used, is being used, or is available for use for an administrative purpose, or is organized or intended to be retrieved by the name of an individual or by an identifying symbol assigned to an individual, pursuant to section 10 of the *Privacy Act*.
62. While the terminology “files” is occasionally utilized within attendant regulations where certain Personal Information Banks are rendered exempt from search and disclosure pursuant to subsection 18(1) of the *Privacy Act*, the Applicant specifically requested access to the Personal Information Bank known as **PPU 005**, which operates unequivocally as a non-exempt repository open to statutory interrogation (**see: Application Record, Tab 1; pages 8-10^{xxiii}**).
63. Moreover, the access request executed on March 11, 2026, was not a generalized request for unstructured “files” *per se*, but a highly targeted demand for Personal Information contained within PPU 005 and specific searches of Foundational Metadata and the Offline Historical Database respecting an executed arrest warrant (**see: Application Record, Tab 1; pages 12-15^{xxiv}**). But for the name of the judicial officer who ostensibly issued the endorsement, all of the Personal Information therein relates *de facto* exclusively to the Applicant. Regarding the name of the judicial officer who issued the endorsement, the federal statutory definition of Personal Information under paragraph 3(i) of the *Privacy Act* explicitly encompasses the name of an individual where it appears with other personal information relating to the individual.
64. This posture is entirely consistent with the binding judicial interpretation of Personal Information. Jurisprudence from the federal public sector commands that the definition of personal information must be afforded a broad,

expansive, and highly liberal interpretation, designed to capture any data uniquely relating to an individual (see:

Dagg v. Canada (Minister of Finance), [1997 2 S.C.R. 403](#); *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, [2006 FCA 157](#); *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003 SCC 8](#)).

65. Personal information encompasses information “about” an identifiable individual, establishing that the information relates to or concerns the subject in a meaningful way. There exists a serious possibility that an individual could be identified through the use of that information, alone or in combination with other data (*Gordon v. Canada (Health)*, [2008 FC 258](#)). Crucially, information need not be recorded in a traditional, paper-based format to constitute personal information under the federal Act or statute (*Morgan v. Alta Flights Inc.*, [2006 FCA 121](#)).
66. The identical information can be classified as personal to more than one individual (*Wyndowe v. Rousseau*, [2008 FCA 39](#)), and information firmly retains its classification as personal information even if it is otherwise publicly available within the meaning of the regulations (*Englander v. TELUS Communications Inc.*, [2004 FCA 387](#)). Most pertinently, subjective information about an individual robustly retains its status as personal information even if it is demonstrably inaccurate, fabricated, or false (*Lawson v. Accusearch Inc.*, [2007 FC 125](#)).
67. The governing principles dictate that privacy rights are quasi-constitutional, designed fundamentally to protect individuals against state overreach while providing an affirmative right of access to the data utilized to govern their lives. Exceptions from an applicant’s access rights must be interpreted narrowly, strictly, and conservatively, with the burden of persuasion strictly residing upon the entity asserting the exception (*Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002 SCC 53](#)).
68. It is axiomatic that the Royal Canadian Mounted Police is subject to the *Charter* pursuant to section 32 thereof. The archaic maxim *lex non cogit ad impossibilia* (the law does not compel the impossible) cannot legally shield the Royal Canadian Mounted Police where the requested digital material was, in verifiable fact, extant, retrievable, and strictly obtainable via standard, routine administrative querying of their own centralized mainframes.

M. PERSONAL INFORMATION AS PROTECTED PROPERTY: THE CESSATION OF CORRECTION RIGHTS ABSENT A SEARCH

69. It is a well-settled jurisprudential axiom that *rule 37* of the *Federal Courts Rules* does not demand that the requested material be legally “owned” by the administrative tribunal as chattel, nor does it require exclusive, physical geographic custody. The singular, uncompromising statutory threshold is that the material resides functionally within the “possession” of the tribunal, an assessment based on the realities of power and access, not antiquated property law.
70. Furthermore, relying upon established equitable jurisprudence, the Personal Information of an applicant is inherently “owned” beneficially by the applicant themselves—it emphatically does not legally “belong” to other police forces as proprietary trade secrets, regardless of their status as the originating agency entering the data into the federal grid.

N. THE STATUTORY ABSURDITY AND THE FRUSTRATION OF CORRECTION RIGHTS UNDER SUBSECTION 12(2) OF THE PRIVACY ACT

73. Pursuant to subsection 12(2) of the *Privacy Act*, an individual granted access to personal information utilized for an administrative purpose is statutorily vested with the affirmative, actionable right to request a correction of said information, mandate the attachment of a formal notation if the correction is unlawfully refused, and compel the mandatory notification of these amendments to any entity that received the data within the preceding two years. This is a critical mechanism for individual self-determination and protection against state error.
74. The posture adopted by the Respondent herein—specifically, the legally specious assertion that it lacks the authorization to search, retrieve, or disclose data inputted into its sovereign infrastructure by ancillary police forces—engineers a profound, irreconcilable statutory absurdity that threatens to dismantle the entire framework of the *Privacy Act*.
75. If the Royal Canadian Mounted Police is legally permitted to abdicate its overarching search obligations beneath the guise and façade of “third-party ownership,” it *ipso facto* obliterates the Applicant’s fundamental statutory right to subsequently request the correction of admittedly false or materially inaccurate intelligence housed within the CPIC database. An aggrieved requestor cannot exercise the right to correct that which the paramount custodian outright refuses to locate, acknowledge, or produce. The right to correct becomes a phantom right, existing only on paper but impossible to actualize. Here, the legal maxim *cinque aliquis quid concedit concedere videtur et id sine*

quo res ipsa esse non pituita (whoever grants a thing supposed also tacitly to grant that without which the grant itself would be of no effect) is resolutely engaged; Parliament's grant of the right to correct structurally requires and commands the corresponding right to compel the antecedent search.

76. This administrative sleight of hand effectively insulates both the centralized repository and the originating municipal police forces from statutory accountability. Should this Honourable Court validate the restrictive interpretation proffered by the Royal Canadian Mounted Police, an individual maliciously targeted by the synthetic fabrication of a False Information Package would be permanently saddled with fraudulent data operating actively within the nation's premier law enforcement repository. This permanent algorithmic taint constitutes an ongoing, egregious violation of fundamental justice, leaving citizens vulnerable to perpetual harassment based on uncorrected, fraudulent inputs.
77. It is a foundational tenet of statutory interpretation that the law does not permit a party to benefit from its own administrative malfeasance (*nullus commodum capere potest de injuria sua propria*). Furthermore, jurisprudential doctrine strictly forbids a reading of a statute that renders a remedial provision—such as the correction rights enshrined in subsection 12(2)—meaningless or illusory (*interpretatio fienda est ut res magis valeat quam pereat*). The Royal Canadian Mounted Police cannot strategically interpret subsection 12(1) governing access in a manner that entirely nullifies the corrective mechanisms of subsection 12(2). The statute must be read as a cohesive whole, designed to empower the citizen, not to shield the state repository.
78. Should the Respondent attempt to argue that any correction request must instead be directed to the originating municipal or provincial agency, such an argument is fundamentally and irreparably flawed *ab initio*. Municipal police boards are explicitly excluded from the purview of the federal *Privacy Act*, leaving the applicant without a federal remedy if forced to pursue local agencies. More critically, a municipal entity does not possess the sovereign administrative credentials, the requisite system-wide database access, or the structural authority to execute CPIC metadata notations or mandate downstream notifications across the federal infrastructure. The Royal Canadian Mounted Police, functioning as the supreme technological custodian of the database, remains the sole entity legally and technically capable of executing the statutory mandate commanded by subsection 12(2).

79. The Applicant formally advances the Doctrine of Institutional Complicity by Willful Blindness. By affirmatively refusing to search the CPIC architecture after being formally notified via the March 11, 2026 PII Access Request that a fabricated, *ultra vires* warrant was operationalized through its systems, the Royal Canadian Mounted Police transcends its status as a mere passive database host (see: Application Record, Tab 1; page 12^{xxv}). The deliberate refusal to audit its own system transforms the federal institution into an active, complicit participant in the ongoing constitutional tort and jurisdictional fraud.
80. Any theoretical counter-argument positing that this motion under *rule 318* constitutes an impermissible “collateral attack” on the underlying criminal arrest is wholly structurally defeated. The Federal Court possesses exclusive supervisory jurisdiction over federal boards. The Applicant is not mounting a collateral attack on the execution of the warrant itself in this forum; rather, he is mounting a direct, meticulously targeted attack on the Royal Canadian Mounted Police’s administrative failure to discharge its independent statutory duties under the *Privacy Act* and the *Federal Courts Rules*.
81. Furthermore, the Applicant advances the Translation Doctrine respecting electronic records. An anticipated objection by the Respondents might suggest that generating hexadecimal dumps or cryptographic audit trails constitutes the impermissible “manufacturing” of new records not mandated by *rule 317*. This logic is archaic. The data presently exists as dormant binary code within the federal mainframe. Utilizing standard operator queries to compile this existing data into a legible format is legally synonymous with translating a foreign-language document already within the Tribunal’s possession; it is the translation of an existing record, not the creation of a new one.

PART IV — ORDERS SOUGHT

81. Predicated upon the uncontradicted evidentiary record, the absolute procedural default of the Respondents, and the binding jurisprudential doctrines comprehensively articulated herein, the Applicant respectfully requests that this Honourable Court exercise its original, plenary and superintending equitable jurisdiction to grant an Order for the precise relief enumerated within the Notice of Motion, including, *inter alia*:

- a. A Declaration that the Royal Canadian Mounted Police has Contravened its mandatory statutory and procedural duties pursuant to *rule 318* of the *Federal Courts Rules*;
- b. A mandatory Order compelling the Royal Canadian Mounted Police to fully comply with its duties by transmitting the complete **Certified Tribunal Record** to the Registry and the Applicant within twenty-four (24) hours of the issuance of the Order, explicitly inclusive of the schedule of materials detailed herein below (**see:** Application Record, Tab 12; pages 570-572^{xxvi}):

Item Number	Category of Material	Specific Records and Metadata Requested
1	Access Request Administrative Files	The complete internal administrative file, tracking sheets, and analyst worksheets concerning <i>Privacy Act</i> file P-2025-16999.
2	System Initialization Logs	The complete, unredacted system entry logs from the automated sequential registry system detailing the exact date, millisecond timestamp, and file initialization sequence that generated the prefix year “2025” for an access request delivered to the Respondent on March 11, 2026.
3	Executive and Inter-Directorate Communications	All electronic communications, emails, instant messages, memorandum chains, and briefing notes concerning the Applicant or file P-2025-16999 exchanged between Director Jeff Ball, Delegate Melissa Simpson, Director General Stéphane Brisson, Regional Commander Matt Peggs, or their authorized agents, and Chief of Staff Tanya Mirsky spanning April 1, 2026, to the present.
4	Internal Legal and Operational Advice	All legal or operational advice solicited or received internally regarding the Applicant’s statutory demand for access to the Canadian Police Information Centre (“CPIC”) Offline Historical Database metadata, including the Foundational Metadata Request and the Offline Historical Database Request.
5	Raw Forensic Mainframe Ledger Records	The raw, unredacted transaction logs, audit trails, and hexadecimal dumps residing within the secure CPIC Offline Historical Database associated with Personal Information Bank RCMP PPU 005 tied to the Applicant’s name, identifiers, or cross-referenced occurrence numbers (2024-2028093, 24-2082035, and Court File/Case ID 457197) spanning September 15, 2024, to December 31, 2024, inclusive.
6	Cryptographic Audit Trails	The complete cryptographic audit trails capturing all ADD, MODIFY, CLEAR, and CANCEL command strings, along with terminal identifiers, physical hardware addresses, Originating Agency Identifiers (“ORIs”), and unstructured narrative fields for each sequential transaction executed during the aforementioned temporal window.
7	Forensic Metadata of Search Methodology	The complete electronic system logs generated by Operator NBOISVERT on April 14, 2026, at 07:35:43, detailing the complete input syntax, query

parameters, and system constraints utilized to execute the front-facing “Q PERS+” and “Q CNI” live database queries.

8	Internal and Policies	Directives Exclusion	Any internal directives, policy documents, or operational notes instructing the Access to Information and Privacy (“ATIP”) Branch analysts to omit an interrogation of the Offline Historical Database in response to the Applicant’s explicit, specialized request for historical data.
9	Trans-Directorate Processing Records		The complete, unredacted administrative processing file, tracking timelines, and internal analyst notes concerning the concurrent <i>Access to Information Act</i> (“ATIA”) request submitted by the Applicant, explicitly targeting the procurement, enterprise licensing, and National Technology Onboarding Program (“NTOP”) integration logs of the Mescius SDK / GrapeCity.Documents.PDF.6.0.2.0 developer engines within the CPIC infrastructure.
10	Automated File Linking Records		All internal processing records showing any administrative coordination, automated file linking, or database cross-referencing executed between the privacy division handling <i>Privacy Act</i> request P-2025-16999 and the information access branch processing the parallel <i>ATIA</i> files.
11	Software Logs	Exception	Any software error tracking logs, system exception reports, or developer audit alerts generated by the core CPIC mainframe database management system involving database inquiries or structural PDF modifications tied to the Applicant’s biographical identifiers or transaction history.
12	Executive Briefing Notes and Action Logs	Suite	All briefing notes, corporate risk assessments, institutional action logs, and communications generated by or sent to Commissioner Michael Duheme and Director General Stéphane Brisson regarding the Applicant’s personal information or file P-2025-16999.
13	Central Command Communications	Region	All emails, letters, instant messages, and administrative directives sent or received by Assistant Commissioner Matthew Peggs (Central Region Command) concerning Police Case ID: 457197, the “Adult Common Information Package,” or the collection and retention of the Applicant’s property from September 15, 2024, to the present.
14	Third-Party Transfer Ledgers	Data Ingestion	All cross-jurisdictional system logs showing the electronic receipt, intake vetting, and cryptographic mapping of data transferred from the Toronto Police Service (TPS) or Ontario Court of Justice (OCJ) to the RCMP infrastructure involving the Applicant’s biographical profiles.
15	Primary Charging Instruments	Statutory	A certified copy of the <i>Criminal Code</i> Form 2 “Information” and/or <i>Criminal Code</i> Form 4 “Indictment” purportedly generated, indexed, or uploaded into federal tracking streams regarding the Applicant’s underlying file.
16	Core Intake Endorsements	Courthouse	A certified copy of the Intake Court Endorsement represented on Page 3 of 5 within the disputed “False Information Package,” capturing any handwriting, initials, or automated metadata strings applied during processing.

154	Originating Judicial Authorizations	A certified copy of the alleged warrant in the first instance executed, tracked, or registered within the CPIC network in relation to the Applicant's identifiers.
18	Comprehensive Judicial and Executive Orders	Any and all ancillary orders, determinations, statutory authorizations, variances, or judicial directions issued by a Court of competent jurisdiction or a federal board concerning the collection, retrieval, manipulation, or preservation of the Applicant's personal information or physical property.

(Nota bene: The requested relief does not demand the impossible of the Respondents; it strictly compels the production of digital architectures fundamentally within their sovereign administrative control. The Court must exercise its equitable discretion to refuse any attempts by the Respondents to bifurcate or dilute the transmission schedule listed above).

- c. Costs of this interlocutory motion awarded to the Applicant on a full indemnity basis, payable forthwith.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 10th day of June, 2026.



Digitally signed by Kevin McLean

Date: 2026.06.10 01:20:46 -04'00'

Adobe Acrobat version: 2026.001.21563

Mr. Kevin A. McLean (BA, JD, CIM)

68 Abell Street

Toronto, Ontario

M6J 0B1

Fax: 416.352.0055

Email: mclean@searchandseizure.ca

Applicant (Self-Represented)

PART V — LIST OF AUTHORITIES**A. STATUTES AND REGULATIONS**

1. *Access to Information Act*, RSC 1985, c A-1
2. *Canada Evidence Act*, RSC 1985, c C-5
3. *Federal Courts Act*, RSC 1985, c F-7
4. *Federal Courts Rules*, SOR/98-106
5. *Interpretation Act*, RSC 1985, c I-21
6. *Privacy Act*, RSC 1985, c P-21
7. *Criminal Code*, RSC 1985, c C-46

B. JURISPRUDENCE (CITED AND HYPERLINKED ABOVE)

8. *Air Passenger Rights v. Canada (Attorney General)*, 2021 FCA 201
9. *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65
10. *Canada Post Corp. v. Canada (Minister of Public Works)*, 1995 CanLII 3574 (FCA)
11. *Ontario (Criminal Code Review Board) v. Hale*, 1999 CanLII 3805 (ON CA)
12. *McInerney v. MacDonald*, 1992 CanLII 57 (SCC), 1992 2 SCR 138
13. *Lawson v. Accusearch Inc.*, 2007 FC 125
14. *Chitrakar v. Bell TV*, 2013 FC 1103 (CanLII)
15. *Rémillard v. Canada (National Revenue)*, 2020 FC 1061
16. *Douze v. Canada (Citizenship and Immigration)*, 2010 FC 1086
17. *Boudreau v. Canada (Revenue Agency)*, 2022 FC 792 (CanLII)
18. *Canada (Human Rights Commission) v. Pathak*, 1995 CanLII 3591 (FCA), 1995 2 F.C. 455
19. *Chopra v. Canada (Public Safety and Emergency Preparedness)*, 2026 CanLII 18896 (FC)
20. *John Doe I v. Canada (Attorney General)*, 2024 FC 1024

21. *Canadian Copyright Licensing Agency (Access Copyright) v. Alberta*, 2015 FCA 268

22. *Friends of the Earth Canada v. Canada (Attorney General)*, 2023 FC 1438 (CanLII)

23. *GCT Canada Limited Partnership v. Vancouver Fraser Port Authority*, 2021 FC 624

24. *Dagg v. Canada (Minister of Finance)*, 1997 2 S.C.R. 403

25. *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157

26. *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8

27. *Gordon v. Canada (Health)*, 2008 FC 258

28. *Morgan v. Alta Flights Inc.*, 2006 FCA 121

29. *Wyndowe v. Rousseau*, 2008 FCA 39

30. *Englander v. TELUS Communications Inc.*, 2004 FCA 387

31. *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53

32. *Atlantic Prudence Maritime Inc. v. Canada (Minister of Transport)*, 1983 2 FC 183 (FCA)

33. *Canada (Attorney General) v. Cloutier*, 2008 FC 322

ⁱ The term originates from ancient Greek mythology (specifically the poet Hesiod). According to the story, Zeus gifted Pandora—the first mortal woman—a sealed jar containing all the evils, miseries, and hardships of the world, strictly instructing her never to open it. Overcome by curiosity, Pandora opened the jar, releasing all the world's afflictions onto humanity. She managed to slam the lid shut, but only Hope remained trapped inside.

ⁱⁱ The False Information Package, specifically page 3 of 5 titled “Intake Court Endorsement” used the language of “This Information is Accepted [sic] on its face”.

ⁱⁱⁱ See: page(s) in Motion Record as hyperlinked herein

^{iv} See: page(s) in Motion Record as hyperlinked herein

^v See: page(s) in Motion Record as hyperlinked herein

^{vi} See: page(s) in Motion Record as hyperlinked herein

^{vii} See: page(s) in Motion Record as hyperlinked herein

^{viii} See: page(s) in Motion Record as hyperlinked herein

^{ix} See: page(s) in Motion Record as hyperlinked herein

^x See: page(s) in Motion Record as hyperlinked herein

^{xi} See: page(s) in Motion Record as hyperlinked herein

^{xii} See: page(s) in Motion Record as hyperlinked herein

^{xiii} See: page(s) in Motion Record as hyperlinked herein

^{xiv} See: page(s) in Motion Record as hyperlinked herein

^{xv} See: page(s) in Motion Record as hyperlinked herein

^{xvi} See: page(s) in Motion Record as hyperlinked herein

^{xvii} See: page(s) in Motion Record as hyperlinked herein

^{xviii} See: page(s) in Motion Record as hyperlinked herein

- 157**
- ^{xix} See: page(s) in Motion Record as hyperlinked herein
- ^{xx} See: page(s) in Motion Record as hyperlinked herein
- ^{xxi} See: page(s) in Motion Record as hyperlinked herein
- ^{xxii} See: page(s) in Motion Record as hyperlinked herein
- ^{xxiii} See: page(s) in Motion Record as hyperlinked herein
- ^{xxiv} See: page(s) in Motion Record as hyperlinked herein
- ^{xxv} See: page(s) in Motion Record as hyperlinked herein
- ^{xxvi} See: page(s) in Motion Record as hyperlinked herein

Tab 6

FEDERAL COURT

The Honourable ____ Justice _____

June ___, 2026

Court Seal

B E T W E E N:

KEVIN A. MCLEAN

Applicant

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, AND
STEPHANE BRISSON

Respondents

**ORDER
(AFTER MOTION)**

UPON MOTION made by the Applicant, Mr. Kevin A. McLean, in writing pursuant to Rule 369 of the *Federal Courts Rules*, for an Order compelling the Royal Canadian Mounted Police to transmit the Certified Tribunal Record pursuant to Rule 318, alongside associated procedural, declaratory, and substantive relief;

46

160

AND UPON reading the Notice of Motion dated June 10, 2026, the Applicant's Memorandum of Fact and Law, and the documentary evidence contained within the Applicant's Motion Record and Application Record;

AND UPON noting that the Respondents were duly served with the Notice of Application and the Rule 317 Request on May 19, 2026, as per the Applicant's Proof of Service accepted for filing on May 19, 2026;

AND UPON noting that the Respondents have failed to serve and file a Notice of Appearance (Form 305) within the prescribed time, have failed to file a formal objection under Rule 318(2), and are accordingly in default and prohibited from receiving further notice of steps and service of documents in this Proceeding;

AND UPON determining that the immediate intervention of this Court is necessary to ensure the orderly administration of justice, to preserve the *status quo ante*, and to compel compliance with the mandatory strictures of the *Federal Courts Rules* including its General Principle under Rule 3 therein (so amended in

THIS COURT ORDERS AND DECLARES THAT:

Procedural Relief

1. **Abridgment of Time:** Any timelines required to be abridged for the hearing and disposition of this motion are hereby abridged pursuant to Rule 8 of the *Federal Courts Rules*, on a *nunc pro tunc* basis.
2. **Dispensation of Compliance:** Strict compliance with any procedural rule is hereby varied or dispensed with pursuant to Rule 55 of the *Federal Courts Rules*, on a *nunc pro tunc* basis where applicable.
3. **Deeming of Filing:** All documents submitted by the Applicant for filing in this motion are deemed filed on the day in which they were submitted to the Registry, pursuant to Rule 72.1 of the *Federal Courts Rules*.
4. **Dispensation of Proof of Service:** The Applicant is not required to provide further proof of service upon the Respondents in respect of this motion or future steps, pursuant to Rule 73, granted *nunc pro tunc*, given the Respondents' deliberate failure to file a Notice of Appearance.

Declaratory and Substantive Relief

5. **Declaration of Contravention:** It is declared that the Royal Canadian Mounted Police (the "RCMP Tribunal") has contravened its mandatory statutory and procedural duties pursuant to Rule 318 of the *Federal Courts Rules*.

161 **47** 6. **Declaration of Disobedience:** It is declared that the RCMP Tribunal has disobeyed a lawful process of this Honourable Court, acted in a manner that interferes with the orderly administration of justice, and impaired the authority and dignity of the Court.

7. **Mandatory Order for Compliance:** The RCMP Tribunal shall, within twenty-four (24) hours of the issuance of this Order, fully comply with its duties pursuant to Rule 318 of the *Federal Courts Rules* by transmitting the complete Certified Tribunal Record to the Registry and to the Applicant. The Certified Tribunal Record shall explicitly include, but is not limited to, the following schedule of materials:

Item Number	Category of Material	Specific Records and Metadata Requested
1	Access Request Administrative Files	The complete internal administrative file, tracking sheets, and analyst worksheets concerning <i>Privacy Act</i> file P-2025-16999.
2	System Initialization Logs	The complete, unredacted system entry logs from the automated sequential registry system detailing the exact date, millisecond timestamp, and file initialization sequence that generated the prefix year “2025” for an access request delivered to the Respondent on March 11, 2026.
3	Executive and Inter-Directorate Communications	All electronic communications, emails, instant messages, memorandum chains, and briefing notes concerning the Applicant or file P-2025-16999 exchanged between Director Jeff Ball, Delegate Melissa Simpson, Director General Stéphane Brisson, Regional Commander Matt Peggs, or their authorized agents, and Chief of Staff Tanya Mirsky spanning April 1, 2026, to the present.
4	Internal Legal and Operational Advice	All legal or operational advice solicited or received internally regarding the Applicant’s statutory demand for access to the Canadian Police Information Centre (“CPIC”) Offline Historical Database metadata, including the Foundational Metadata Request and the Offline Historical Database Request.
5	Raw Forensic Mainframe Ledger Records	The raw, unredacted transaction logs, audit trails, and hexadecimal dumps residing within the secure CPIC Offline Historical Database associated with Personal Information Bank RCMP PPU 005 tied to the Applicant’s name, identifiers, or cross-referenced occurrence numbers (2024-2028093, 24-2082035, and Court File/Case ID 457197) spanning September 15, 2024, to December 31, 2024, inclusive.
6	Cryptographic Audit Trails	The complete cryptographic audit trails capturing all ADD, MODIFY, CLEAR, and CANCEL command strings, along with terminal identifiers, physical hardware addresses, Originating Agency Identifiers (“ORIs”), and

unstructured narrative fields for each sequential transaction executed during the aforementioned temporal window.

7	Forensic Metadata of Search Methodology	The complete electronic system logs generated by Operator NBOISVERT on April 14, 2026, at 07:35:43, detailing the complete input syntax, query parameters, and system constraints utilized to execute the front-facing “Q PERS+” and “Q CNI” live database queries.
8	Internal Directives and Exclusion Policies	Any internal directives, policy documents, or operational notes instructing the Access to Information and Privacy (“ATIP”) Branch analysts to omit an interrogation of the Offline Historical Database in response to the Applicant’s explicit, specialized request for historical data.
9	Trans-Directorate Processing Records	The complete, unredacted administrative processing file, tracking timelines, and internal analyst notes concerning the concurrent <i>Access to Information Act</i> (“ATIA”) request submitted by the Applicant, explicitly targeting the procurement, enterprise licensing, and National Technology Onboarding Program (“NTOP”) integration logs of the Mescius SDK / GrapeCity.Documents.PDF.6.0.2.0 developer engines within the CPIC infrastructure.
10	Automated File Linking Records	All internal processing records showing any administrative coordination, automated file linking, or database cross-referencing executed between the privacy division handling <i>Privacy Act</i> request P-2025-16999 and the information access branch processing the parallel ATIA files.
11	Software Exception Logs	Any software error tracking logs, system exception reports, or developer audit alerts generated by the core CPIC mainframe database management system involving database inquiries or structural PDF modifications tied to the Applicant’s biographical identifiers or transaction history.
12	Executive Suite Briefing Notes and Action Logs	All briefing notes, corporate risk assessments, institutional action logs, and communications generated by or sent to Commissioner Michael Duheme and Director General Stéphane Brisson regarding the Applicant’s personal information or file P-2025-16999.
13	Central Region Command Communications	All emails, letters, instant messages, and administrative directives sent or received by Assistant Commissioner Matthew Peggs (Central Region Command) concerning Police Case ID: 457197, the “Adult Common Information Package,” or the collection and retention of the Applicant’s property from September 15, 2024, to the present.
14	Third-Party Data Transfer Ingestion Ledgers	All cross-jurisdictional system logs showing the electronic receipt, intake vetting, and cryptographic mapping of data transferred from the Toronto Police Service (TPS) or Ontario Court of Justice (OCJ) to the RCMP infrastructure involving the Applicant’s biographical profiles.

Primary Statutory
Charging
Instruments

A certified copy of the *Criminal Code* Form 2 “Information” and/or *Criminal Code* Form 4 “Indictment” purportedly generated, indexed, or uploaded into federal tracking streams regarding the Applicant’s underlying file.

16

Core Courthouse
Intake Endorsements

A certified copy of the Intake Court Endorsement represented on Page 3 of 5 within the disputed “False Information Package,” capturing any handwriting, initials, or automated metadata strings applied during processing.

17

Originating Judicial
Authorizations

A certified copy of the alleged warrant in the first instance executed, tracked, or registered within the CPIC network in relation to the Applicant’s identifiers.

18

Comprehensive
Judicial and
Executive Orders

Any and all ancillary orders, determinations, statutory authorizations, variances, or judicial directions issued by a Court of competent jurisdiction or a federal board concerning the collection, retrieval, manipulation, or preservation of the Applicant’s personal information or physical property.

Leave Relating to Potential Contempt

8. **Leave for Contempt Proceedings:** The Applicant is hereby granted leave to bring a motion for contempt against the RCMP Tribunal, and any specific persons facilitating the intentional breach of the orders herein, pursuant to Rule 50(1)(d) and Rules 466 and 467 of the *Federal Courts Rules*.

Cross-Jurisdictional Enforcement Relief

9. **Authorization for Enforcement:** The Applicant is at liberty, authorized, and empowered to apply to any court, tribunal, regulatory, or administrative body, wherever located, for the recognition of this Order, and for assistance in carrying out its terms and the terms of any other order issued in these proceedings.

Costs and Residual Relief

10. **Costs:** Costs of this motion are awarded in favour of the Applicant on a full indemnity basis, payable forthwith by the Respondents.

11. **Residual Relief:** This Honourable Court remains seized of this matter for the purpose of granting such further
and other orders of an equitable nature as may be necessary to ensure compliance and restore the *status quo ante*.

Date: June _____, 2026

The Honourable _____ Justice _____

(Signature of Judge)

TAB 7

PRIVATE AND CONFIDENTIAL

DATE: February 27, 2026

DELIVERY METHOD: Via MAIL

TO: Royal Canadian Mounted Police Access to Information and Privacy Branch
73 Leikin Drive, Mail Stop #61

Ottawa, Ontario

K1A 0R2

SUBJECT I: Statutory Request for Access to Personal Information under the *Privacy Act* (Canada)

SUBJECT II: Exaction of Canadian Police Information Centre Metadata Pertaining to the Promulgation of Judicial Authorizations and Concomitant Arrest Warrants

SUBJECT III: Formal Demand for the Production of Offline Historical Database Audit Trails, Transaction Logs, Originating Agency Identifiers, and Systemic Non-Repudiation Artifacts

Dear Sirs/Mesdames:

I. INTRODUCTION, CONTEXTUAL FRAMEWORK, AND QUASI-CONSTITUTIONAL IMPERATIVES

1. Correspondence is heretofore initiated with respect to the aforementioned matters, wherein the immediate, unmitigated, and comprehensive exaction of specified forensic metadata archived within the digital and physical federal repositories is sought. The present requisition is advanced not as a routine administrative issue, nor as a peripheral, academic, or vexatious pursuit of archival data, but rather as a fundamental, paramount, and non-derogable exercise of quasi-constitutional entitlements. The exaction of these records is an indispensable prerequisite for the vindication of rights that reside at the very core of the *lex terrae*, serving as the only viable mechanism to restore the *status quo ante* in the face of systemic administrative failure, technological vitiation, and jurisdictional overreach.
2. Reliance is unequivocally placed upon the established and binding jurisprudence, notably *Dagg v Canada (Minister of Finance)*, 1997 2 SCR 403 (the "**Dagg**") at para 61, wherein the quasi-constitutional status of access rights is unambiguously affirmed by the Supreme Court of Canada. These statutory entitlements are specifically engineered, deliberately constructed, and statutorily enshrined such that the citizenry is empowered to scrutinize, challenge, and definitively rectify the purported deployment of vitiated judicial instruments—*acta* which have facilitated a profound, potentially *ultra vires* deprivation of physical liberty. The right of access is not a mere procedural adjunct; it is a substantive pillar of democratic accountability designed to prevent the state from operating in a vacuum of unreviewable discretion, thereby mitigating the profound democratic deficit inherent in clandestine law enforcement databases.
3. The contravention of these strictures constitutes an **Irremediable Nullity** which vitiates the law of the land and obviates any pretense of lawful detention, rendering the actions of the state functionally indistinguishable from arbitrary coercion and unlawful confinement. It is posited that the structural integrity, procedural fairness, and moral authority of the Canadian criminal justice system are inextricably tethered to the absolute accuracy, verifiable provenance, and jurisdictional legitimacy of the administrative records that authorize state coercion. A justice system that operates upon the basis of fraudulent or "metamorphosed" digital records is one that has abandoned the rule of law in favour of systemic expediency, effectively rendering the *Canadian Charter of Rights and Freedoms* (the "**Charter**") a series of hollow platitudes rather than a living instrument of protection.
4. The federal government, acting as the ultimate steward, architect, and host of the paramount law enforcement database, bears the ultimate, inescapable, and non-delegable burden of ensuring this requisite transparency is maintained. Consequently, the demand for absolute, unvarnished transparency regarding the systemic inception, precise digital timestamping, and exact geographical origin of these judicial authorizations constitutes a foundational democratic imperative. The state cannot wield the ultimate sword of physical arrest while simultaneously cloaking the shield of administrative accountability in bureaucratic darkness, as the lack of transparency invites the very corruption and documentary "metamorphosis" that the *Privacy Act* (the "**Privacy Act**") was designed to illuminate and rectify.

- 3 5. Furthermore, the complex intersection of federal informational control and provincial criminal administration mandates an extraordinarily rigorous standard of hygiene for all digital entries that precipitate a physical deprivation of liberty. A warrant is not merely an administrative convenience or a digital flag; it is a profound constitutional mechanism that overrides the fundamental freedom of movement. It is respectfully submitted that an arrest effectuated upon a digitally manipulated, retroactively generated, or deliberately post-dated warrant is legally and constitutionally indistinguishable from an arbitrary kidnapping perpetrated under the colour of right. The validity of such an instrument is contingent upon its temporal and jurisdictional accuracy, both of which are currently subjected to intense forensic scrutiny due to the discovery of irreconcilable internal contradictions within the municipal paper trail.
6. Appended hereto are the ensuing documents, submitted for the concomitant purposes delineated herein, and specifically calibrated to facilitate the expeditious processing of this statutory requisition while proactively circumventing any preliminary institutional requests for supplementary identity verification or procedural obfuscation:
- a. A reproduction of the Canadian passport pertaining to Kevin A. McLean (the "**Applicant**"), provided exclusively for the strict circumscription of identity verification and the absolute, preemptive satisfaction of all legislative authentication thresholds mandated by the institution's internal administrative directives. This enclosure serves to extinguish any preliminary jurisdictional or standing-based objections *in limine* and ensures that the institution cannot rely upon identity-based prevarication to delay the thirty-day statutory response window.
 - b. A reproduction of the vitiated information package and associated documentation (the "**False Information Package**"). In a spirit of profound cooperation and *bona fides*, this document is enclosed to explicitly demonstrate the imperative necessity for the exhaustive nature of the present statutory requisition. It is noted with immense legal gravity that the fraudulent character of this document has been corroborated by the Ministry of the Attorney General, specifically by counsel situated within the civil document request division. This corroboration establishes a *prima facie* case for the existence of an **Irremediable Nullity** within the municipal records that requires federal metadata for definitive resolution.
7. As heretofore noted, it is expressly confirmed via the signature appended to this requisition and the concomitant provision of identity documentation that Kevin A. McLean was subjected to a physical deprivation of liberty on October 2, 2024, purportedly pursuant to a represented arrest warrant. Notwithstanding the representation of authority, it is posited that the Toronto Police Service (the "**TPS**") failed to maintain a valid or accurate iteration of the authorizing instrument, instead relying upon a technologically corrupted version of the intake court endorsement (the "**Intake Court Endorsement**") which was factually inaccurate and fundamentally devoid of any legal or factual nexus to Kevin A. McLean. This corruption is not merely an aesthetic or clerical flaw; it is a fundamental breakdown in the chain of judicial authorization, rendering the subsequent detention a profound violation of the principles of fundamental justice and a manifestation of state action that is strictly *extrajudicial*.

II. FACTUAL MATRIX AND FORENSIC DATABASE PARTICULARS

8. It is legally necessitated that access be unequivocally granted to the specific algorithmic, structural, and foundational fields within the Canadian Police Information Centre (the "**CPIC**") database. This requisite access encompasses, but is absolutely not limited to, the exact, unredacted nomenclature of the authorizing judicial officer, the specific judicial tier and territorial jurisdiction of said officer, the precise temporal date and immutable algorithmic timestamp of initial systemic entry into the federal ledger, and the precise law enforcement divisions responsible for the primary data input and any subsequent digital modifications. The exaction must include the "Time-to-Live" (the "**TTL**") parameters and the terminal identification numbers (the "**Terminal Identification Numbers**") utilized during the primary data transmission.
9. The **CPIC** database operates as the supreme, centralized nervous system of Canadian law enforcement, dictating real-time liberty deprivations across all provincial, territorial, and municipal boundaries. It is fundamentally acknowledged that **CPIC** is a highly complex, federated system, wherein the relevant repository for active, unexecuted warrants is specifically designated as the investigative data bank (the "**Investigative Data Bank**"). The personal information housed within the

- Investigative Data Bank is legally governed, strictly regulated, and administratively audited under the formal federal designation of personal information bank rcmp ppu 005 (the "**PIB RCMP PPU 005**").
10. Because an entry within **CPIC** instantaneously transforms an individual into a subject of national state coercion, empowering every sworn officer across the dominion to effectuate a physical arrest upon mere systemic confirmation, the metadata underlying that entry transcends mere administrative trivia. It is the absolute digital *acta* upon which constitutional rights are either respected or irreparably breached. The database is the digital embodiment of the sovereign's coercive power, and its logs are the only unimpeachable evidence of its exercise, providing a "single source of truth" that remains insulated from the potential for local, municipal-level record manipulation or localized software "glitches" that conveniently obscure jurisdictional errors.
 11. The primary occurrence number is definitively recorded as Toronto Police Service occurrence number 2024-2028093 (the "**Primary Occurrence**"), established on September 15, 2024 (the "**Primary Date**"), and administratively managed by Officer Eric Tang, bearing badge number 10942 (the "**Primary Case Manager**"). This specific cipher establishes the temporal genesis of the investigatory phase, marking the initial engagement of the municipal constabulary and establishing the foundational timeline against which all subsequent digital entries must be forensically measured for chronological fidelity.
 12. The secondary occurrence number, which appears to govern the immediate custodial trajectory of the matter and the physical effectuation of the arrest itself, is recorded as Toronto Police Service occurrence number 24-2082035 (the "**TPS Occurrence Number**"), dated September 22, 2024 (the "**Secondary Date**"), and managed by Detective Constable Michael Kolankowski, bearing badge number 82239 (the "**Secondary Case Manager**"). The administrative bifurcation of the investigation into dual occurrences necessitates a highly precise temporal mapping of all judicial authorizations applied within the local municipal records management system (the "**Local RMS**"), as such fragmentation is often indicative of procedural anomalies intended to bypass the scrutiny of a single judicial oversight officer.
 13. A concomitant identification cipher, critical to the central archival indexing of the prosecution and the integration of physical court records, is noted as Toronto Police Service case identification number 457197 (the "**Police Case ID Number**"). The multiplicity of these labyrinthine tracking digits further exacerbates the necessity for a pristine, federally verified chronological timeline, as disparate occurrences frequently signify deliberate administrative compartmentalization explicitly designed to obscure jurisdictional overreach or the unauthorized "stacking" of occurrences to justify a warrantless apprehension *ex post facto*.
 14. The purported date of the formal commencement of proceedings, as explicitly indicated upon the physical face of the impugned documentation and purportedly sworn under oath, is September 23, 2024 (the "**Commencement Date**"). This date is the absolute temporal fulcrum upon which the legality of all subsequent state actions, including the physical detention, fundamentally balances. If the digital entry into **CPIC** post-dates this moment, or if the metadata reveals a "retroactive addition" transaction, the entire prosecution is infected with a fatal chronological defect that cannot be cured by the *Rules of Civil Procedure* (the "**Civil Rules**").
 15. It is further confirmed that as a result of any court or judge being **Coram Non JUDGE** or **Factum A JUDGE, Quod Ad Officium Jure Non Pertinet, Ratum Non Est** on account of the **False Information Package**, which is attached for ease of reference albeit a false document or false documents, it will also be 18 months since the time of the declaring of an Information (Criminal Code Form 2) albeit with the incorrect name involving Court Officer (Toronto Region) Christyn Frugoni-Rojas and incorrect data therein along with the **Intake Court Endorsement** not being the correct document either and presumably a problem of modern technology.
 16. In relation to the 18th month window, it is also pursuant to *R v Jordan*, 2016 SCC 27 (the "**Jordan**") that in any matter involving a matter before the Ontario Court of Justice, of which the Crown Counsel elected to proceed summarily and the arrest warrant (the correct one) that a trial must be held and concluded within 18 months. That terminal date would be March 23, 2026. As such, although every judge was **Coram Non JUDGE** and any act, step, or document was subject to **Factum A JUDGE, Quod Ad Officium Jure Non Pertinet, Ratum Non Est**, Kevin A. McLean provides that for ease of reference noting the thirty-day time window for the fulfillment of this statutory requisition.
 17. The informant of record is identified as Court Officer Christyn Frugoni-Rojas (the "**Informant**"). It is noted with profound, overarching legal significance that Christyn Frugoni-Rojas was acting not merely

- as a civilian administrative clerk, but in the highly specialized, deputized, and statutorily augmented capacity of a special constable. This designation inherently engages the coercive apparatus of the state and significantly elevates the standard of exactitude, procedural fairness, and duty of candour required in the swearing of the underlying information and the subsequent generation of any resultant arrest warrants. The sworn statements of a special constable carry the full weight of the Crown; any falsehood, temporal inaccuracy, or "technological corruption" therein constitutes a fundamental breach of the duty of *uberrima fides* (the "**Utmost Good Faith**").
18. The sworn information number, serving as the unique identifier for the specific charging document contained on the Form 2, is formally recorded as 4810 998 24 48129169 (the "**Information Number**").
 19. An intake court endorsement was purportedly effectuated on the **Commencement Date**, bearing a digital signature purportedly attributed to Justice of the Peace George Jiri (the "**Authorizing Officer**") of the Brampton Ontario Court of Justice (the "**Non-Originating Courthouse**"). It is observed with the utmost, grave concern that said endorsement is entirely devoid of the requisite geographical, territorial, and temporal indicators explicitly corresponding to the Toronto region, where the alleged offense and investigation were inextricably localized.
 20. The sterile application of a digital signature by a judicial officer stationed within the Peel Region, affixed to a strictly Toronto-based prosecution—without the explicit, recorded invocation of inter-jurisdictional transfer protocols or telewarrant provisions delineated within the *Criminal Code*—constitutes an act of **Factum A Judice, Quod Ad Officium Jure Non Pertinet, Ratum Non Est**. Because the judicial officer lacked the requisite territorial jurisdiction and the inherent authority to promulgate such an order outside their assigned venue, the resulting process is an absolute, irredeemable nullity. The exercise of judicial power outside its statutory ambit is a jurisdictional vacuum that cannot be cured by subsequent administrative action, as it strikes at the heart of the court's competence.
 21. Furthermore, as any appearance before a judicial officer lacking such authority is strictly **Coram Non Judice**, the entire procedural foundation of the arrest is structurally unsound. The fundamental common law maxim *nemo dat quod non habet* (no one gives what they do not have) dictates that a judicial officer cannot confer lawful authority over a jurisdiction to which they are not temporally or geographically assigned; thus, a Brampton justice possesses zero inherent jurisdiction to issue a Toronto warrant absent strict statutory compliance, which is entirely absent from the face of the record.
 22. The presumed originating venue as of the **Commencement Date**, dictated inflexibly by the strict territorial strictures of the alleged offense and the locus of the police investigation, is the Ontario Superior Court of Justice South Toronto Criminal Division (the "**Originating Courthouse**"). This constitutes the only proper, constitutionally sound venue for the promulgation of the *acta*.
 23. The presumed originating police division, universally vested with the primary investigatory jurisdiction and operational oversight, is the Toronto Police Service 52nd Division (the "**Originating Police Division**"). Within the highly secure architecture of **CPIC**, every single entry is inextricably tethered to a specific originating agency identifier (the "**ORI**"), which serves as the unforgeable digital signature for every transaction and irrevocably traces the exact terminal and data input back to a specific law enforcement division. The **ORI** prevents any local agency from disclaiming responsibility for a fraudulent, extra-jurisdictional, or "technologically corrupted" entry.
 24. The effectuation of the physical arrest transpired on October 2, 2024 (the "**Arrest Date**") at the Toronto Police Service 14th Division (the "**Non-Originating Police Division**"). Subsequent to the initial arrest at the **Non-Originating Police Division**, the specialized attendance, custodial transfer logistics, and interrogatory presence within the holding cells were singularly conducted by Detective Abdulhameed K. Virani (the "**Deciding Detective**"), who is operationally attached to the **Originating Police Division**.
 25. The release documentation, effectuated via a Form 10 (the "**Release Order**"), incorporated the **TPS Occurrence Number** but fundamentally and inexplicably omitted the **Police Case ID Number**. The omission of this universally required central indexing digit on a mandatory release document suggests that the document may have been generated entirely outside the primary **Local RMS** architecture, potentially as a manual, offline override deliberately utilized to bypass locked systemic safeguards that strictly require verified antecedent warrants before a formal **Release Order** can be generated by municipal software.
 26. It is fundamentally acknowledged that the removal of a WANT record from the active **CPIC** interface upon the execution of an arrest constitutes a mere functional illusion of deletion. Systemic architecture requires that operational statuses be updated via highly specific command codes, namely the

clearance transaction (the "**CLEAR Transaction**") indicating a successful execution, or the cancellation transaction (the "**CANCEL Transaction**") indicating withdrawal or profound procedural error. Execution of these terminal transactions triggers the immediate migration of the data into an insulated repository formally designated as the offline historical database (the "**Offline Historical Database**"). Any deviation whatsoever between the physical paper trail and the digital federal ledger is unconditionally indicative of institutional malfeasance, unauthorized data entry, and deliberate documentary metamorphosis intended to cure jurisdictional defects post-arrest.

III. MEMORANDUM OF LEGAL ANALYSIS: STATUTORY MANDATES FOR DISCLOSURE

The Statutory Right of Access: Section 12(1) and the Breadth of Federal Control

27. Pursuant to Section 12(1) of the **Privacy Act**, a robust, quasi-constitutional right of access is conferred upon Kevin A. McLean to acquire personal information concerning themselves that is under the control of a federal government institution (the "**Institution**"). This statutory entitlement transcends mere procedural courtesy; it operates as a substantive jurisprudential bedrock intended to ensure absolute governmental accountability and guarantee strict, unwavering adherence to the *lex terrae*. The right to know the basis of one's detention is the cornerstone of *habeas corpus*, now modernized into the digital realm via the **Privacy Act**. The ontological status of the digital warrant, being the primary vehicle for the deprivation of physical liberty, mandates that the subject of such a record possess the unmitigated ability to verify its provenance and chronological integrity.

28. The Royal Canadian Mounted Police (the "**RCMP**"), acting in its capacity as the paramount architect and supreme custodian of the **CPIC** database infrastructure, is deemed by well-established appellate authority to be in absolute legal control of the records entered into that national system. This expansive definition of "control" is utterly unaffected by the inter-agency principle of "originator control." Established jurisprudence from the Office of the Privacy Commissioner of Canada unequivocally confirms that the **RCMP** bears the ultimate, non-delegable responsibility for ensuring that all information hosted across the **CPIC** network complies strictly with federal statutes, regardless of which agency performed the initial keystrokes.

29. The Supreme Court of Canada, in *Canada (Information Commissioner) v Minister of National Defence*, 2011 SCC 25 (the "**National Defence**"), affirmed that physical possession, systemic administration, and structural integration satisfy the highest threshold for "control" under federal access legislation. The hosting institution cannot disavow the contents of its own digital ledger, nor can it outsource its strict privacy obligations to the constituent municipalities who utilize its infrastructure. Consequently, a non-derogable obligation is imposed upon the **RCMP** to provide unfettered, unredacted access to the specific **CPIC** metadata fields requested herein. The inter-jurisdictional nature of the data entry provides no legal sanctuary from the disclosure obligations imposed upon the federal host.

Systemic Audit Trails, Non-Repudiation, and the Mandate for Informational Veracity: Section 6(2)

30. The architecture of **CPIC** relies upon the principle of absolute non-repudiation. Every systemic interaction generates a permanent, immutable entry within the system's underlying transaction logs (the "**Transaction Logs**"). This includes the initial addition of data (the "**ADD Transaction**") and any subsequent alterations (the "**MODIFY Transaction**"). These logs capture forensic-level details including the exact millisecond of execution, the unique user identifier of the operator, and the internet protocol address (the "**IP Address**") of the originating terminal. The Principle of Non-Repudiation serves as a cryptographic and administrative guarantee that a digital record cannot be disowned or surreptitiously altered by its creator without leaving an indelible audit trail.

31. Section 6(2) of the **Privacy Act** stipulates that the **Institution** shall take all reasonable steps to ensure that personal information utilized for an administrative purpose is as accurate as possible. When the coercive power of the state is mobilized based upon hosted digital data, the tolerance for systemic inaccuracy is reduced to an absolute nullity. A false entry in **CPIC** is a digital loaded weapon pointed at the liberty of the citizen. Should the **Transaction Logs** reveal a **MODIFY Transaction** that inexplicably alters the judicial officer's name to an extra-territorial jurisdiction post-arrest, institutional fraud is established. The doctrine of *fraus omnia corrumpit* (fraud unravels all) dictates that a judicial process infected by deliberate fraud is void *ab initio*.

Judicial Accountability, the Functus Officio Doctrine, and the Status Quo Ante

32. The exaction of the authorizing judicial officer's nomenclature and the precise, verified tier of the authorizing court are critical, non-negotiable imperatives for establishing the substantive jurisdictional validity of an arrest *ab initio*. At the exact moment of execution, the issuing judicial officer becomes

7 entirely *functus officio* with respect to that specific warrant. Reliance is placed upon the principles articulated in *Chandler v Alberta Association of Architects*,
171 1989

2 SCR 848 (the "**Chandler**"), wherein the Court affirmed that once a judicial officer has finally decided a matter and issued their order, their jurisdiction over that specific matter is entirely exhausted.

33. Consequently, the authorization itself crystallizes into administrative, historical records of a definitively concluded judicial process (*acta*). The statutory shield of investigative privilege cannot be contorted or retrofitted to conceal procedural anomalies, jurisdictional overreaches, or the *post facto* generation of documents explicitly designed to sanitize a botched apprehension. Once the custodial phase has culminated in the issuance of a **Release Order**, the foundational details of the warrant's authorization transcend the protected realm of active law enforcement investigative techniques and must be subjected to public and judicial scrutiny to maintain the integrity of the administration of justice.

The Jordan Ceiling and the Imperative for Expedited Remediation

34. The temporal trajectory of these proceedings is governed by the strictures delineated in *R v Jordan*. As the Crown Counsel elected to proceed summarily, the presumptive ceiling for the completion of the trial is established at 18 months from the date of the commencement of proceedings. Given the **Commencement Date** of September 23, 2024, the terminal date for the vindication of the right to a trial within a reasonable time is March 23, 2026. This impending deadline exacerbates the urgency for the exaction of the **Offline Historical Database** records.

35. Any delay precipitated by the **RCMP's** failure to provide unvarnished access to the forensic metadata constitutes a direct impediment to the **Applicant's** ability to make full answer and defence. If the proceedings are structurally vitiated due to jurisdictional nullity, the continuation of the prosecution beyond the **Jordan** ceiling would constitute a double breach of constitutional guarantees—both as to the legality of the initial detention and the reasonableness of the ensuing delay. The state cannot use its own technological "corruption" or administrative obfuscation to extend the custodial or prosecutorial shadow over the citizenry.

Triangulating Truth and Statutory Remedies: Section 12(2) and the Charter

36. To definitively prove institutional manipulation, the digital *acta* procured from the federal **RCMP** must be subjected to a strict discrepancy analysis against the primary, originating physical legal instruments. This forensic methodology of "Triangulating Truth" ensures that independent judicial branch records are meticulously cross-referenced with federal **RCMP** offline security infrastructure, exposing any discrepancies introduced by municipal police intermediaries. This triangulation is the only method to expose the "documentary metamorphosis" that occurs when municipal files are surreptitiously updated to match federal entries.

37. Should the discrepancy analysis confirm systemic manipulation, the profound remedial provisions of Section 12(2) of the **Privacy Act** shall be immediately invoked. Kevin A. McLean possesses the right to demand the formal, immediate correction of erroneous or fabricated information or the attachment of a notation of disagreement (the "**Notation of Disagreement**"). Under Section 24(1) of the **Charter**, a comprehensive remedy may be sought for an unlawful or arbitrary detention.

38. The jurisprudence of *R v Garofoli*,
1990

2 SCR 1421 (the "**Garofoli**"), establishes the absolute right of an accused to challenge the underlying validity of a judicial authorization; this right is rendered illusory if the metadata proving its invalidity is systematically withheld. The pursuit of constitutional remedies, including the exclusion of evidence under Section 24(2) based upon the principles in *Hunter v Southam Inc*,
1984

2 SCR 145, is utterly contingent upon the procurement of the systemic metadata substantiating the illegality. In the face of undeniable fraud, the **Irremediable Nullity** must be recognized, and Kevin A. McLean optimally positioned to seek prerogative writs such as *certiorari* to quash the vitiated proceedings *in limine*.

IV. FORMAL DEMANDS FOR EXACTION AND SYSTEMIC DISCLOSURE

39. In absolute summation, it is unequivocally and forcefully submitted that the **RCMP** is legally bound, without the option for discretionary refusal, to disclose the entirety of the requested metadata particulars. It is formally demanded that the **Institution** immediately conduct a comprehensive offline

8 search (the "**Offline Search**") of the highly secure **Offline Historical Database** to retrieve all artifacts associated with the **PIB RCMP PPU 005** repository.

40. This explicit demand for exaction encompasses the following specific forensic artifacts, which are indispensable for the forensic reconstruction of the record:

- a. The retrieval of all active, cleared, canceled, or purged WANT Records associated with Kevin A. McLean spanning the entirety of the year 2024, including historical status codes (the "**Historical Status Codes**").
 - b. The unredacted production of all system **Transaction Logs**, audit trails, and hexadecimal dumps (the "**Hexadecimal Dumps**") governing the entire lifecycle of the warrant entry, including all **ADD**, **MODIFY**, **CLEAR**, and **CANCEL** Transactions, and any supervisor override actions recorded within the federal mainframe.
 - c. The explicit disclosure of the associated timestamps (accurate to the millisecond), the **ORIs**, the unique user IDs of terminal operators, the precise terminal hardware addresses, and the entirety of the narrative and remarks fields (the "**Narrative Fields**") for each sequential transaction, demonstrating the evolutionary history of the data entry and any unauthorized "metamorphosis."
41. Given the severe allegations of systemic metamorphosis and inter-jurisdictional fraud, the stipulation for electronic transmission directly to Kevin A. McLean (the "**Transmission Method**") is strictly necessary. The **Institution** is statutorily obligated to fully accommodate this method of secure delivery to protect the strict integrity of the data and the absolute privacy of Kevin A. McLean, shielding it from potential interception or further manipulation by originating municipal agencies currently under scrutiny.
42. The **RCMP** is firmly reminded of the strict statutory thirty-day timeline governing the disposition of access requests under the **Privacy Act**. Due to the significant legal ramifications tethered to its contents and the impending **Jordan** ceiling of March 23, 2026, it is formally demanded that all responsive records be collated and transmitted exclusively via the designated **Transmission Method**, entirely devoid of any redactions, omissions, or obfuscations whatsoever. Any failure to comply will precipitate immediate escalation to the Office of the Privacy Commissioner of Canada and the subsequent pursuit of a writ of *mandamus* before the Federal Court of Canada.

All of which is respectfully submitted.

Mr. Kevin A. McLean (BA, JD, CIM)

Enclosures (copies of): i. Passport of Kevin A. McLean (the "**Applicant**" or "Requestor"); Driver's License of the Applicant (G Drivers Licence) (Nota bene: NotaDO NOT SEND TO THIS ADDRESS – TERRIBLE MAIL COLLECTION and MISDIRECTED MAIL TO WRONG PERSONS – IF MAIL RETURN IS REQUIRED – PLEASE SEND TO 68 Abell St
Toronto, ON M6J 0B1 (Prime Medical, Rehab Mechanics for Mr. Kevin A. McLean (BA, JD, CIM)); and (iii) Health Card from Ontario Government for Mr. McLean

NOTA BENE: Only reply via email or fax.

TAB 8

Tracking number:

0105952990142328

Delivered
Shipping service: Xpresspost
Sender: Unavailable
Delivery standard: Mar. 10

Latest updates

Date	Time	Location	Progress	Post office
Mar. 11	10:33 am	OTTAWA,ON	Delivered	
Mar. 11	9:42 am	OTTAWA,ON	Out for delivery	
Mar. 11	9:14 am	OTTAWA,ON	Item processed	
Mar. 10	8:39 am	TORONTO,ON	Item in transit	
Mar. 10	5:39 am	TORONTO,ON	Item processed	
Mar. 9	4:24 pm	TORONTO,ON	Item accepted at the Post Office	

Features and options

TAB 9

Tab A



Mr. Kevin McLean <mcleansettlement@gmail.com>

Privacy Act request P-2025-16999 / F339, Your File N/A, Clarification Required

Mr. Kevin McLean <mcleansettlement@gmail.com>
To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>

Mon, Mar 16, 2026 at 5:59 PM

DATE: March 16, 2026

CREATED WITH DICTATION OR VOICE-TO-TEXT SOFTWARE - RESERVATION OF RIGHTS TO CORRECT ANY SPELLING, GRAMMAR, SYNTAX, IMPORTANT QUALIFIERS AND/OR INCORRECT DOUBLE NEGATIVES:

DELIVERY METHOD: Via Electronic Transmission

TO: Melissa S.

Access to Information and Privacy Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario

K1A 0R2

REFERENCE: Privacy Act request P-2025-16999 / F339

SUBJECT I: Formal Clarification and Requisition of Forensic Metadata Pursuant to the Privacy Act (Canada)

SUBJECT II: Jurisprudential Abrogation of the Originator Control Defense and the Non-Delegable Stewardship of the Royal Canadian Mounted Police

SUBJECT III: Geotemporal Delineation of Required Systemic Audit Trails

SUBJECT IV: Anticipatory Rebuttals of Statutory Exemptions and the Foreclosure of Institutional Obfuscation

SUBJECT V: The Intersection of Digital Non-Repudiation, Forensic Epistemology, and the Vindication of Charter Rights

SUMMARY OF YOUR EMAIL AND MY BRIEF RESPONSES PRIOR TO THE LENGTHIER ONE DUE TO THE NEED FOR THE PERSONAL INFORMATION OF MINE DUE TO THE THREATS TO MY LIFE, LIBERTY AND SECURITY WITH THANKS

Dear Melissa S:

Due to the extreme importance herein, I have provided a summary type response and then a much more detailed one to be efficient with public resources and respect the time of all involved.

Date: March 16, 2026

To: Access to Information and Privacy Branch
Royal Canadian Mounted Police
73 Leikin Drive, Mail Stop #61
Ottawa, Ontario K1A 0R2

Re: Privacy Act Request P-2025-16999 / F339 – Clarification Response (without admitting such clarification was required - response and production/disclosure of PII records should not take more than an hour considering the highly particularized privacy request of a few weeks ago)

Thank you for your correspondence dated March 16, 2026. I appreciate the opportunity to provide clarifications so that my request may be processed efficiently and without delay. I remain fully committed to cooperating with your office and supplying any information necessary to facilitate the search.

In the interest of clarity and completeness, I address each of the four points raised in your letter and provide the relevant factual particulars for ease of reference.

1. Scope of the Request

I confirm that the text of my February 27, 2026 request accurately reflects the information I am seeking.

For clarity, the request concerns **my own personal information** contained within the **CPIC Investigative Data Bank**, governed by **Personal Information Bank RCMP PPU 005**, including:

- WANT records (active, cleared, cancelled, or purged)
- ADD, MODIFY, CLEAR, and CANCEL transactions
- All associated timestamps
- Originating Agency Identifiers (ORIs)

- Terminal identifiers
- User IDs of terminal operators
- Narrative and remarks fields
- All corresponding artifacts stored in the **Offline Historical Database**

This request is strictly limited to my personal information under s. 3 of the Privacy Act.

2. Whether the Records Are Held by the RCMP

I confirm that the records sought are held within the **control of the RCMP**, specifically within the CPIC system and its Offline Historical Database.

The attached findings of the Office of the Privacy Commissioner of Canada (OPC) confirm that:

“As the steward of CPIC...the RCMP bears responsibility for ensuring that all information shared...is done in accordance with the requirements of the MOC and in compliance with the Act.”

The CPIC Audit Report (2011) likewise confirms that the RCMP:

- Hosts the CPIC system
- Maintains its audit trails
- Oversees compliance
- Performs offline searches

Accordingly, the records fall within the RCMP's custody and control for the purposes of s. 12(1) of the Privacy Act.

3. Location of the Records

I respectfully clarify that the records requested are not located at a specific detachment. CPIC is a **centralized national system**, and the Offline Historical Database is accessible only to the RCMP.

Given the uncertainty surrounding the accuracy of municipal records—and the possibility that the originating police service may not be limited to the Toronto Police Service (TPS)—the only reliable and authoritative source of the relevant metadata is the **central CPIC system**.

For ease of reference, I provide all known particulars below.

4. Time Frame and Underlying Particulars

The relevant time frame is defined by the occurrence numbers, the commencement of proceedings, and the arrest date. All known particulars are provided below.

A. First Occurrence Number (TPS)

- **Event / Occurrence Number:** 2024-2028093
- **Date:** September 15, 2024
- **Case Manager:** PC Eric Tang #10942

180 • Email: 10942@tps.ca

B. Second Occurrence Number (TPS)

- **Event / Occurrence Number:** 24-2082035
- **Date:** September 22, 2024
- **Case Manager:** D/Cst. Michael Kolankowski #82239
- **Email:** 82239@tps.ca

C. TPS Case Identification Number (MOST LIKELY THE COURT FILE NUMBER WITH THE SCJ 361 UNIVERSITY AVENUE, 1ST FLOOR)

- **TPS Case ID:** 457197
- Appears on the Intake Court Endorsement
- Does **not** appear on the Form 10 Release Order

D. Commencement of Proceedings (date information is sworn and laid)

- **Date:** September 15 or September 23, 2024

E. Informant / Court Officer

- **Name:** Court Officer Christyn Frugoni-Rojas (née Christin Boulton)
- **Role:** Special Constable / Court Officer
- **Information Number (Form 2):** 4810 998 24 48129169

F. Intake Court Endorsement

- **Date:** September 23, 2024
- **Digital signature:** JP George Jiri
- **Note:** The endorsement contains no physical signature, location, or date stamp from the Brampton courthouse.
- **Presumed originating courthouse:**
 - **Ontario Superior Court of Justice – South Toronto Criminal Division**
 - 361 University Avenue, Toronto

G. Arrest Information

- **Arrest Date:** October 2, 2024
- **Arrest Location:** TPS 14 Division (350 Dovercourt Road, Toronto)
- **Arresting Officers:**
 - Cst. Anthony Romano #6097
 - D/Cst. Michael Roman Kolankowski #82239
 - Sergeant Sean Cassidy
- **Detective attending cells:**
 - Detective Abdulhameed K. Virani (TPS 52 Division)
- **Form 10 Release Order:**
 - Signed by Sgt. Cassidy and myself

- Contained the TPS Occurrence Number (allegedly from September 22, 2024)
- Did **not** contain the TPS Case ID Number

H. Additional Context Regarding Date Ranges

For ease of reference, I include the following correspondence from the Superior Court of Justice Records Management Office:

Email from SCJ RMO (Ms. Sana Azim) to ACT (Ms. Janet McLean)

Date: August 20, 2025

ACT ID: 3831309629

“Our office is unable to process orders with date ranges.

Please list the exact dates your Ordering Party wishes to order and re-submit an updated order form.”

This illustrates why precise dates are provided above.

5. Summary of Relevant Time Frame

Based on the above, the relevant period for the CPIC Offline Search is:

- **September 15, 2024 → October 2, 2024**, inclusive
- Plus any subsequent CLEAR, CANCEL, or MODIFY transactions associated with the same entries (and thereafter)

Because CPIC records contain their own timestamps, I respectfully request that the RCMP retrieve **all records associated with my identifiers**, including any system-generated timestamps outside these dates that relate to the same entries.

Closing

I appreciate your assistance and confirm my full cooperation. If any further clarification is required, I will respond promptly to avoid delay. I look forward to the continued processing of my request within the statutory framework.

I reserve the right to provide further supporting evidence and authorities (if necessary) but I trust that this should not take more than an hour to collate and provide.

The public interest in light of the manipulation of government documents including an informant's name and that of a justice of the peace raise the question as to whether this is happening in isolated fashion or systematically.

Respectfully,

Kevin A. McLean

B.A., J.D., CIM

182. PREFATORY STATEMENT OF GOVERNING LEGAL PRINCIPLES AND QUASI- CONSTITUTIONAL IMPERATIVES

1. To definitively shape the jurisprudential landscape governing this requisition *in limine*, the following foundational legal principles are formally asserted and must govern the institution's administrative processing of this demand:
 - a. **Access to Information Rights – Purpose – Facilitate Democracy:** The overarching purpose of access to information rights (the "**Information Rights**") is strictly to facilitate democracy by ensuring that citizens possess the unvarnished information required to participate meaningfully in the democratic process and to rigorously scrutinize state action;
 - b. **Privacy Rights – Purpose:** Concomitantly, privacy rights are structurally designed to protect the privacy of individuals with respect to personal information held by government institutions, while simultaneously providing individuals with an absolute, non-derogable right of access to that specific information;
 - c. **Quasi-Constitutional Status:** The *Privacy Act*, RSC 1985, c P-21 (the "*Privacy Act*") (alongside its provincial counterparts) is legally recognized by the highest appellate authorities as a quasi-constitutional statute, elevating its mandates far above standard administrative directives or institutional conveniences;
 - d. **Exceptions Interpreted Narrowly:** In *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 (the "*Lavigne*"), [2002] 2 SCR 773, Gonthier J. observed that exceptions from the rights set out in the act should be interpreted exceedingly narrowly, with any residual doubt resolved unequivocally in favour of preserving the applicant's fundamental right of access;
 - e. **Burden of Proof:** The burden of persuasion rests entirely and unshiftingly upon the person or institution asserting the exception (*Lavigne* at paras 30-31);
 - f. **Compelling State Interest:** In *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 (the "*Dagg*"), the Supreme Court of Canada articulated the governing principles of privacy law, affirming that the protection of privacy is a fundamental value in modern democracies and is inextricably enshrined within Sections 7 and 8 of the *Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11* (the "*Charter*"). Consequently, privacy rights and statutory access entitlements are to be compromised only where there exists a demonstrably compelling state interest for doing so (*Dagg* at paras 65, 66, 71)

II. THE "PERSONAL INFORMATION" NEXUS: SYSTEM LOGS AS IDENTIFIABLE DATA

2. While I do not agree that any clarification is so required, I will act in connectoin with our access partnership as it has been called. A critical clarification is necessitated regarding the nature of the requested metadata. It is anticipated that the institution may attempt to characterize hexadecimal dumps, audit trails, and transaction logs as mere "system information" or "technical overhead" falling outside the definition of Personal Information (PI) under Section 3 of the Act. Such a characterization is legally bankrupt and is hereby preemptively refuted
3. Drawing from federal jurisprudence, the definition of Personal Information must be given a broad and expansive interpretation (*Dagg v. Canada*, [1997] 2 S.C.R. 403; *Canada v. RCMP*, 2003 SCC 8).

Personal Information is information "about" an identifiable individual, meaning it relates to or concerns the subject in a substantive way.

4. Under the "serious possibility" test articulated in *Gordon v. Canada (Health)*, 2008 FC 258, information constitutes PI if there is a "serious possibility" that an individual could be identified through its use, alone or in combination with other data. The requested logs are inextricably linked to my identity because they are generated solely as a result of queries, entries, or modifications regarding my specific name, date of birth, and fingerprints. Without my PI, the log would not exist; therefore, the log is "information about an identifiable individual." As established in *Morgan v. Alta Flights Inc.*, 2006 FCA 121, the absence of a "human-readable" recording at the time of entry does not change the fact that the machine-level data remains Personal Information. To hold otherwise would allow the state to immunize its digital activities from oversight simply by storing them in non-textual formats.

III. LEGAL ANALYSIS: IMPACT OF ORDER MO-4542 ON RCMP PRIVACY OBLIGATIONS

5. A pivotal jurisdictional boundary has been established in *Halton Regional Police Services Board (Re)*, 2024 CanLII 62738 (ON IPC) [Order MO-4542], which addresses the transparency of national police databases. This decision establishes a critical distinction between "Local Access" and "Systemic Access."
6. **A. Foreclosure of "Originator Control" Deflection:** The RCMP frequently relies on the "Originator Control" principle to redirect *Privacy Act* requests back to municipal agencies (e.g., the Toronto Police Service). Order MO-4542 effectively demolishes this tactic. Adjudicator Faughnan clarified that a municipal police board is legally and technologically incapable of providing a cross-jurisdictional audit trail. They are "fenced off" from the broader system logs. By operation of law, the RCMP is the sole legal custodian of this systemic metadata. To refuse production is to render this information a "legal nullity"—available nowhere—which directly contradicts the quasi-constitutional status of the Act.
7. **B. Confirmation of Technical Capability and Existing Records:** The RCMP often claims that producing hexadecimal data or transaction logs would require the "creation of a new record." However, MO-4542 explicitly discusses the "off-line search" process. The Adjudicator noted that these searches are a standard, albeit deep-access, function of the database management system. This provides a powerful precedent: the "Offline Historical Database" is an existing repository. My request is for the retrieval of existing data through established forensic protocols, not a request for the RCMP to "program" a new report or perform complex coding.
8. **C. The "Omniscient Vantage Point" Argument:** MO-4542 confirms that while a local police service sees only its own "front-end" activity, the RCMP maintains the "omniscient technological vantage point." In this case, where "Documentary Metamorphosis" (unauthorized changes to warrant data) is suspected, the systemic logs are the only way to see the unaltered Originating Agency Identifier (ORI). Without the RCMP's "Offline" logs, the integrity of the judicial process is compromised because local logs can be limited to their own entries, effectively hiding extra-jurisdictional manipulation or unauthorized data "arbitrage."

IV. DELINEATION OF SCOPE, EXACTION OF METADATA, AND SYSTEMIC NON-REPUDIATION

9. The demand is surgically directed toward the foundational administrative architecture of the database, specifically the **Offline Historical Database** associated with **Personal Information Bank RCMP PPU 005**.

- **A. Standard Computer Operations:** Under the *Privacy Regulations*, an institution must produce a record from machine-readable format using "standard computer hardware and software and technical expertise normally used by the government institution." The "Audit Log Viewer Tool" is a standard operational component of the National Police Services (NPS) infrastructure. Its utilization does not constitute the "creation" of a record; it is the standard retrieval of a machine-readable file. The RCMP cannot claim technical incapacity when it maintains specialized units specifically for the purpose of auditing these very systems for internal security
- **B. The Forensic Extraction vs. Human Readable Standard:** The Privacy Act requires "access," which the RCMP often misinterprets as providing a re-typed summary or a redacted PDF narrative. However, in this forensic context, the authenticity of the raw data is what is "about" me. A sanitized, human-readable summary is insufficient as it relies on the interpretation of an administrative clerk. I am seeking the transactional history of my PI—the raw data that cannot be "re-interpreted." Access that is not "complete" or "authentic" is not "access" under Section 12.
- The extraction must encompass all **Add, Modify, Clear, and Cancel** transactions. Only the raw hexadecimal strings reveal the machine-level data input required to prove the exact sequence of events, ensuring "Digital Non-Repudiation." This is the only way to verify whether a warrant was "metamorphosed" after the fact to justify an otherwise illegal arrest.

V. JURISDICTIONAL STEWARDSHIP AND THE DOCTRINE OF ADMINISTRATIVE ESTOPPEL

10. The RCMP is formally cautioned against the "Originator Control" defense. Physical possession and systemic administration satisfy the highest threshold for "control" under federal legislation (*National Defence*, 2011 SCC 25 at para 56).
11. **A. The Doctrine of Administrative Estoppel:** The RCMP has made formal representations to the Treasury Board of Canada and the Office of the Privacy Commissioner (OPC) that they maintain "full oversight" of CPIC to justify its existence as a centralized federal database. The institution cannot claim "Originator Control" (acting as a mere storage locker) to the user while simultaneously claiming "Supreme Stewardship" (acting as a regulator) to the OPC. You are equitably estopped from disclaiming "control" over records you have officially promised to audit and oversee for compliance. To allow such a defense would be to permit a "jurisdictional shell game" that defeats the very purpose of the *Privacy Act*.
12. **B. Breach of "Duty of Care" in Data Custodianship:** By hosting CPIC, the RCMP owes a quasi-fiduciary duty to the subjects of that data to ensure the system is not used for "Extra-Jurisdictional Arbitrage." When a federal institution becomes aware of a *prima facie* allegation of jurisdictional nullity (the "False Information Package"), their "Duty to Assist" under the *Privacy Act* is heightened. You are not a neutral bystander; you are the host of the vessel where the alleged forgery resides. The RCMP has an affirmative obligation to ensure that its systems are not being used as a platform for the dissemination of fraudulent judicial authorizations.

VI. PROCEDURAL FRUSTRATION OF STATUTORY CORRECTION RIGHTS

13. Under Section 12(2) of the *Privacy Act*, I possess a statutory right to request a correction of my PI or a **Notation of Disagreement**. This is a critical mechanism for ensuring data integrity within federal systems.

14. If the RCMP withholds the metadata that proves the entry is fraudulent or extra-judicial, they are effectively immunizing the record from my Section 12(2) rights. Disclosure of the metadata is a **condition precedent** to the exercise of my statutory right to data integrity. You cannot correct a fraud you are prevented from seeing.
15. The withholding of these logs renders these powerful statutory remedies functionally illusory and directly violates the principles of fundamental justice under Section 7 of the *Charter*. The RCMP is essentially attempting to "privilege" the log data to protect the system from the very correction rights the Act was designed to provide. If the source data is corrupted or fraudulent, the right to "access" must include the right to see the forensic evidence of that corruption.

VII. GEOTEMPORAL PARAMETERS AND SYSTEMIC IDENTIFIERS

16. The relevant period for the CPIC Offline Search is **September 15, 2024, to December 31, 2024**, inclusive of all subsequent clearing or modification transactions. This window is not arbitrary; it is specifically designed to encompass the moments before, during, and after the suspect judicial entries were made.

Specific Identifiers:

- **TPS Occurrence Numbers:** 2024-2028093 & 24-2082035
- **TPS Case ID:** 457197 (but this is likely the SCJ 361 University Avenue file number under an old RMS)
- **Information Number:** 4810 998 24 48129169
- **Arrest Date:** October 2, 2024 (TPS 14 Division)

17. This window is imperative to capture any **Modify Transactions** executed after the arrest to retroactively sanitize jurisdictional defects or "fix" warrant data that was initially entered without proper authorization. Any delay in providing this metadata directly engages the *Jordan* ceiling (March 23, 2026) and will be raised in the appropriate judicial forum as a state-sanctioned delay. The metadata is essential for a "Full Answer and Defence" in the concurrent criminal proceedings.

VIII. THE "DEEMED REFUSAL" AND PUBLIC INTEREST OVERRIDE

18. Pursuant to Section 8(2)(m) of the Act, a public interest override exists where disclosure clearly outweighs any invasion of privacy. In this instance, there is no competing privacy interest—the data is about *me*. However, the public interest in exposing fraudulent judicial authorizations and the systemic manipulation of a national police database is a non-derogable democratic interest.
19. **Final Notice:** Unlike the *Access to Information Act*, the *Privacy Act* carries no application fees and no search/preparation fees. The RCMP cannot use "cost," "volume," or "complexity" as a reason to refuse. An "Offline Search" is a routine, automated process for the IT security branch and cannot, by definition, be an "unreasonable interference with operations."
20. I strongly suggest that the ATIP branch consult directly with the **Chief Information Officer (CIO)** of the RCMP or the **CPIC Field Operations Support Unit (National Police Services)**. Municipal partners like the TPS are "technologically fenced off" from the systemic audit logs you alone possess. Any failure to respond within the 30-day statutory window will be treated as a **"Deemed Refusal"**, resulting in an immediate application to the Federal Court under Section 41. I am prepared to skip the lengthy OPC complaint process where necessary to protect my *Charter* rights and ensure the preservation of these critical forensic records.

II. INTRODUCTION AND PROCEDURAL POSTURE

21. Correspondence is heretofore advanced in direct, comprehensive, and exhaustively detailed response to the communication promulgated by the Access to Information and Privacy Branch of the Royal Canadian Mounted Police, dated March 16, 2026. The present submission is meticulously calibrated to definitively satisfy the administrative prerequisites for clarification demanded by the institution. Concurrently, this instrument is intricately engineered to preemptively extinguish any preliminary, jurisdictional, or standing-based objections that might be improperly marshalled by the federal entity in a misguided attempt to obfuscate the strict statutory mandates unequivocally enshrined within the *Privacy Act*. It is forcefully posited that the administrative processing of this requisition must now proceed forthwith, entirely devoid of further prophylactic delays, manufactured ambiguity, or artificial bureaucratic impediments intended to deliberately exhaust the applicant and frustrate the pursuit of administrative justice.
22. The exaction of these highly specialized, immutable digital records is strictly necessitated to vindicate fundamental quasi-constitutional entitlements and to systematically expose potential administrative vitiation occurring under the colour of right. In circumstances where the structural integrity of a judicial authorization is ostensibly compromised through an *ex post facto* systemic manipulation—whether executed to clandestinely cure a fatal jurisdictional defect, to bridge an investigatory lacuna, or to retroactively sanitize an entirely unlawful physical apprehension—the rigorous extraction of unalterable digital metadata remains the sole, exclusive epistemological mechanism to restore the *status quo ante*. It is respectfully submitted that an unmitigated adherence to the overarching principles of *uberrima fides* (utmost good faith) is statutorily demanded of the federal repository, acting as the ultimate, supreme custodian of the nation's law enforcement ledgers.
23. The profound, inherent asymmetry of information existing between the coercive, deeply resourced apparatus of the state and the private citizenry dictates that the custodian must exercise its stewardship with absolute, unassailable transparency when formally compelled by statutory mechanisms. To permit the state to shield its digital machinations behind a veil of administrative silence is to invite tyranny by algorithm, whereby unreviewable databases operate as silent arbiters of liberty, entirely divorced from traditional judicial scrutiny.
24. Applying the paramount quasi-constitutional doctrines established in *Dagg* and *Lavigne* to the present factual matrix dictates that the exaction of digital metadata is not a mere procedural courtesy, nor an administrative inconvenience to be lightly dismissed by departmental administrators; rather, it operates as a substantive jurisprudential bedrock designed to definitively rectify the purported deployment of vitiated judicial instruments.
25. These instruments represent state *acta* which have facilitated a profound, potentially *ultra vires* deprivation of physical liberty, fundamentally offending the absolute protections against arbitrary detention enshrined within Section 9 of the *Charter*. Furthermore, the liberty and security of the person interests guaranteed under Section 7 of the *Charter* are directly engaged when the state relies upon a fundamentally flawed or fraudulently generated digital record to justify the ongoing subjection of an individual to the penal apparatus. The continued reliance upon such tainted *acta* offends the principles of fundamental justice, which demand that state deprivations of liberty be anchored to mathematically verifiable, procedurally sound, and authentically generated judicial authorizations.
26. Furthermore, the absolute paramountcy of these access rights over institutional convenience, operational lethargy, or inter-agency diplomatic sensitivities dictates that the institution is legally

precluded from weaponizing broad, generalized interpretations of law enforcement exemptions to shield administrative errors, extra-jurisdictional overreaches, or intentional systemic manipulations from rigorous public and judicial scrutiny. The rule of law immutably demands that the state's monopoly on the legitimate use of force be perpetually anchored to verifiable, authentic, and contemporaneously generated judicial authorization. A retrospective validation achieved through digital forgery is a profound corruption of the judicial process.

27. It is further posited that a justice system operating upon the fragile, compromised foundation of fraudulent, retroactively generated, or technologically metamorphosed digital records is one that has entirely abandoned the rule of law in favour of systemic expediency and the preservation of institutional hegemony. The federal government, acting as the ultimate steward, architect, and host of the paramount law enforcement database, bears the non-delegable, unshakeable burden of ensuring this requisite transparency is continuously maintained. By strictly enforcing the provisions of the *Privacy Act*, the institution mitigates the profound democratic deficit inherent in clandestine digital repositories utilized to restrict fundamental liberties. Any institutional reticence, hesitation, or refusal to disclose the foundational audit trails is invariably interpreted by reviewing tribunals as a tacit admission of systemic irregularity and procedural impropriety. The deliberate obfuscation of metadata effectively operates as the spoliation of evidence, triggering devastating adverse inferences against the state in subsequent constitutional litigation.
28. Anticipating a potential, albeit entirely unmeritorious, objection from the Presiding Divisional Court President, the Crown Prosecutor, or opposing counsel that the present requisition constitutes an overly broad, vexatious, or impermissible "fishing expedition," such an assertion is preemptively neutralized and categorically dismantled. A "fishing expedition" is legally defined by its broad, speculative nature and an overarching absence of targeted evidentiary parameters, often deployed merely to harass administrative bodies with voluminous, undirected requests. Conversely, the strict parameters established within this requisition are microscopically focused, geographically constrained to a singular municipality, and temporally restricted to a mathematically precise algorithmic envelope spanning a mere fiscal quarter. The deliberate, surgical pursuit of highly specific hexadecimal and precise digital timestamps, which are tethered irrevocably to a singular, heavily documented deprivation of liberty, represents the very antithesis of a generic, undirected inquiry; it is a meticulous forensic extraction of the exact empirical evidence required to meticulously evaluate the true jurisdictional competence of the underlying warrant *ab initio*.

III. DELINEATION OF SCOPE, EXACTION OF METADATA, AND SYSTEMIC NON-REPUDIATION

29. Clarification is formally necessitated regarding the precise, highly technical scope of the requisition, ensuring absolutely no institutional misinterpretation limits the exhaustive production of responsive documents. It is unequivocally stated that the present inquiry does not seek a generic, superficial criminal record synopsis, nor does it request a standard, routine query of the active operator interfaces utilized daily by patrol officers. Such superficial, front-end inquiries would inherently and predictably omit historically executed, covertly modified, or intentionally purged [arrest warrant] (the "**Arrest Warrant**") records. Routine operational queries of the active [canadian police information centre] (the "**Canadian Police Information Centre**") interfaces routinely yield null results for executed or withdrawn instruments—an architectural design consciously intended to mitigate unlawful

secondary arrests by field officers, rather than to perpetually obliterate the historical occurrence from the overarching institutional memory.

30. Rather than seeking active operational data, the demand is surgically directed toward the foundational, underlying administrative architecture of the database, specifically targeting the highly insulated, archival [offline historical database] (the "**Offline Historical Database**") associated directly with [personal information bank rcmp ppu 005] (the "**Personal Information Bank RCMP PPU 005**"). The complex architectural schematics of modern national policing systems rely heavily on sophisticated non-repudiation mechanisms, relational database integrity protocols, and comprehensive, immutable audit trails. These unalterable cryptographic mechanisms ensure that an executed warrant is never truly deleted from existence, preventing rogue operators from erasing historical facts through "soft deletions" or administrative overrides. Instead, the digital footprint is seamlessly migrated to a secure offline repository where its complete structural evolution, including every keystroke of modification, remains permanently fossilized for rigorous auditing, judicial oversight, and strict institutional accountability purposes.
31. The critical documentation sought strictly comprises the entirely unredacted [transaction logs] (the "**Transaction Logs**"), comprehensive systemic audit trails, and raw hexadecimal dumps that irrevocably chronologize the entire systemic lifecycle of the specified entries. This exaction encompasses, without limitation, the precise date and temporal timestamps (accurate to the millisecond) of all [add transaction] (the "**Add Transaction**"), [modify transaction] (the "**Modify Transaction**"), [clear transaction] (the "**Clear Transaction**"), and [cancel transaction] (the "**Cancel Transaction**") executions orchestrated within the specified temporal window. The extraction of these precise event coordinates allows for the unassailable forensic reconstruction of the digital ledger, revealing exactly when the [arrest warrant] (the "**Arrest Warrant**") was birthed, when its parameters were potentially altered to reflect different jurisdictional realities, and when it was ultimately extinguished from the active purview of law enforcement.
32. A hexadecimal dump is explicitly necessitated because standard graphical user interfaces are frequently programmed to suppress, translate, or artificially sanitize backend anomalies to provide a cohesive visual experience for the terminal operator. By demanding the raw hexadecimal strings, the applicant bypasses the superficial, heavily curated interface, acquiring the unvarnished, machine-level data input that mathematically proves the exact sequence of events beyond any capability of administrative redaction, interpretative spin, or subsequent technological laundering. Only the foundational code can reveal the authentic chronology of the state's actions.
33. The absolute, non-derogable necessity of extracting these specific algorithmic artifacts is comprehensively corroborated by the critical, highly publicized findings articulated in the *Audit of Selected RCMP Operational Databases - Section 37 of the Privacy Act - 2011*, Office of the Privacy Commissioner of Canada (the "*OPC 2011 Audit*"). Within the scathing *OPC 2011 Audit*, the Commissioner explicitly admonished the Royal Canadian Mounted Police for consistently failing to adequately monitor systemic interactions and formally recommended the immediate, mandatory enablement of the [audit log viewer tool] (the "**Audit Log Viewer Tool**"). This specific utility was legally prescribed to consolidate, extract, and review complex audit trails to detect unauthorized access, surreptitious data manipulation, or the improper entry of extra-jurisdictional warrants by local detachments operating beyond their lawful mandate.
34. In its formal, documented reply to Parliament, the Royal Canadian Mounted Police explicitly committed to deploying and consistently utilizing this exact oversight methodology to ensure the integrity of the [canadian police information centre] (the "**Canadian Police Information Centre**"). Consequently, the institution is fundamentally estopped from feigning technological inability to extract the requested logs, as the preservation, collation, and robust review of these precise digital footprints constitute a formally adopted, externally mandated institutional policy designed precisely for the

meticulous extraction requested herein. To deny the existence or retrieval of these logs would be tantamount to admitting an ongoing, systemic violation of the Commissioner's binding recommendations, thereby exposing the federal repository to severe parliamentary and judicial censure.

35. Furthermore, the exaction explicitly necessitates the full, unredacted disclosure of the [issuing authority] (the **"Issuing Authority"**) data field, the [originating agency identifier] (the **"Originating Agency Identifier"**), the unique user identification credentials of the terminal operators (specifically the alphanumeric CPIC login ciphers), and the entirety of the unstructured narrative and remarks fields appended to the entries. It is a technological certainty that the systemic architecture operates upon a bedrock foundation of absolute non-repudiation. By virtue of this design, any unauthorized structural metamorphosis of the judicial nomenclature, any retroactive upgrading of the jurisdictional court level to maliciously cure a procedural defect, or any post-execution alteration of the presiding jurist's identification is permanently preserved within these hidden audit trails. This architectural reality flawlessly maintains the distinct, unalterable "before" and "after" states of the altered algorithmic fields, allowing for definitive forensic comparison against the physical paper endorsements ostensibly relied upon by the Crown.
36. The extraction of the unstructured narrative and remarks fields is of paramount importance. These fields frequently contain the informal, unvarnished communications between dispatchers, warrant squads, and records management personnel. If a warrant was rejected by a local justice, subsequently shopped to a different jurisdiction, or electronically massaged to satisfy the criteria of the [canadian police information centre] (the **"Canadian Police Information Centre"**), the residual evidence of such administrative gymnastics is invariably captured within these free-text annotations. These narratives serve as the *res gestae* (the events, circumstances, and statements that are incidental to the main fact) of the digital transaction, providing the crucial contextual framework required to interpret the hexadecimal data and exposing the true *mens rea* (guilty mind) or administrative negligence of the state actors involved.
37. It is fully anticipated that the institution may subsequently assert, as a potential administrative counter-argument, that the deep extraction of deeply buried hexadecimal dumps or highly specialized transaction logs constitutes the "creation of a new record" or presents an "unreasonable administrative burden," thereby attempting to unlawfully refuse disclosure under standard procedural exemptions. This proposition is legally untenable, logically fractured, and fundamentally incorrect in law. The extraction of pre-existing database fields, compiled audit trails, and historical transactional metadata utilizing established algorithmic query parameters inherently native to the system does not, under any recognized legal or technological definition, equate to the creation of a new record. The systemic architecture inherently possesses the functionality to retrieve these historical logs; the mere requirement for specialized command syntax or an [offline search] (the **"Offline Search"**) executed by high-level system administrators cannot be conflated with the unauthorized generation of novel documentation.
38. To baselessly assert that an [offline search] (the **"Offline Search"**) represents an undue operational burden is to effectively immunize the vast majority of the national database's historical actions from any statutory oversight whatsoever. Such an outcome is entirely incompatible with the legislative intent of the *Privacy Act* and is fundamentally abhorrent to the transparent principles of a functioning democracy. The statutory obligation explicitly requires the institution to render the information reasonably retrievable; where the institution itself engineered the complex, multi-tiered architecture that strictly necessitates an [offline search] (the **"Offline Search"**) to view historical data, it cannot thereafter selectively leverage its own self-imposed architectural complexity as an impenetrable shield against democratic transparency and lawful requisition. The burden of technological navigation falls squarely and irrevocably upon the custodian. The state cannot build an opaque digital labyrinth and

then subsequently complain that it is too arduous to navigate when a citizen lawfully demands the retrieval of their personal data.

IV. JURISDICTIONAL STEWARDSHIP AND THE ABROGATION OF THE ORIGINATOR CONTROL DEFENSE

39. Attention is strictly, forcefully, and preemptively directed to the anticipated institutional assertion that the *Privacy Act* does not authorize the Royal Canadian Mounted Police to search or disclose files purportedly "belonging" to other municipal or provincial police forces. This proposition is formally repudiated as a profound, inexcusable misapprehension of established administrative law and a blatant disregard for binding privacy jurisprudence. The continued institutional reliance upon the inter-agency doctrine of originator control to circumvent federal statutory disclosure obligations constitutes a profound legal fallacy that inherently offends the quasi-constitutional imperatives of the *Privacy Act*. Inter-agency memorandums of understanding, internal operational manuals, and localized data-sharing agreements are subordinate administrative constructs that do not, and categorically cannot, supersede Acts of Parliament or abrogate fundamental constitutional rights.
40. It is a well-established, insurmountable legal syllogism that physical possession, ongoing systemic administration, and fundamental structural integration perfectly satisfy the absolute highest threshold for establishing "control" under federal access legislation. Reliance is unequivocally placed upon the binding jurisprudence meticulously articulated in *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25 (the "*National Defence*") at para 56. In *National Defence*, the Supreme Court of Canada affirmed a rigorous, comprehensive bipartite test for determining "control." The Court definitively established that records residing within a federal institution's systemic architecture—over which the institution possesses physical custody of the servers, and over which a reasonable expectation of systemic governance, auditing, and high-level oversight applies—are legally under its absolute control. This control is established entirely irrespective of the records' original municipal or provincial authorship. To hold otherwise would allow the federal government to construct unreviewable black boxes populated by third-party data, thereby eviscerating the entire statutory regime of public accountability.
41. Applied strictly and without deviation to the present circumstances, the Royal Canadian Mounted Police, functioning as the paramount architect, proprietor, and supreme administrator of the national database, exercises absolute physical and administrative custody over the mainframe servers and their constituent data packets. The federal institution sets the algorithmic parameters, controls the telecommunications bandwidth, dictates the stringent security protocols, and uniquely manages the archival lifecycle of the data from genesis to deletion. Therefore, it cannot disavow the contents of its own digital ledger, nor can it impermissibly outsource its strict statutory obligations to the myriad of constituent municipalities currently utilizing its highly sophisticated infrastructure. The federal government is not a mere passive conduit, an inert bulletin board, or a disinterested telecommunications provider; it is the ultimate publisher, arbiter, and sovereign custodian of the repository.
42. Furthermore, the Office of the Privacy Commissioner of Canada has definitively foreclosed this precise institutional defense in circumstances directly involving the [toronto police service] (the "**Toronto Police Service**"), establishing an insurmountable precedent regarding ultimate federal accountability. In the authoritative *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC, Special Investigation Report, April 14, 2014* (the

"*OPC 2014 Suicide Investigation*"), the Commissioner exhaustively investigated the unauthorized, deeply prejudicial disclosure of highly sensitive personal information originally authored and entered by the [toronto police service] (the "**Toronto Police Service**").

43. In the *OPC 2014 Suicide Investigation*, the Royal Canadian Mounted Police attempted to deploy the exact originator control defense anticipated herein, aggressively arguing that it was merely hosting data owned by municipal entities and therefore bore no statutory responsibility for its dissemination or review. The Commissioner explicitly rejected this premise *in toto*, establishing unequivocally that the Royal Canadian Mounted Police, acting in its capacity as the paramount steward and the sole sovereign signatory to international data-sharing agreements (such as the [memorandum of cooperation] (the "**Memorandum Of Cooperation**") with the Federal Bureau of Investigation), bears the ultimate, non-delegable responsibility for ensuring that all information hosted across the network complies strictly with federal statutes. The federal hosting institution was found substantively and directly accountable for the widespread dissemination of the municipal data and was subsequently compelled by the Commissioner to overhaul its default sharing protocols entirely. Thus, the institution is functionally and legally prohibited from relying upon inter-agency originator control principles to evade accountability for the data permanently disseminated through its proprietary infrastructure. The jurisprudence dictates an immutable reality: he who controls the network, controls the data, and bears the statutory burden of disclosure.

SUB-SECTION A: The Recency of Jurisprudential Mandates and the Evidentiary Void of the False Information Package

44. To definitively extinguish any residual assertion that this requisition ought to be administratively deflected or redirected to a local municipal agency, reliance is emphatically placed upon the highly recent, and strictly binding, adjudicative findings articulated by Adjudicator Steven Faughnan in *Order MO-4542, Halton Regional Police Services Board, 2024 CanLII 62738 (ON IPC)* (the "*Order MO-4542*"). Promulgated as recently as July 8, 2024, this pivotal jurisprudential authority operates overwhelmingly and unequivocally in favour of the applicant. It serves to permanently foreclose any administrative inclination by the federal repository to improperly deflect the present requisition back to a provincial or municipal constabulary, legally paralyzing the institution's ability to evade its statutory burden.
45. In *Order MO-4542*, the appellant formally sought records revealing inquiries made about him by *all* police services across Canada navigating various law enforcement databases. The provincial tribunal definitively ruled that a localized municipal police service (in that instance, the Halton Regional Police Services Board) absolutely lacks the requisite physical custody, statutory authority, and systemic control to conduct such expansive offline searches capable of revealing the overarching systemic footprint of other law enforcement agencies. The tribunal explicitly recognized that localized municipal entities are technologically restrained and severely restricted by strict use protocols from querying the centralized federal historical repositories to ascertain what external agencies have done. A municipal force simply cannot execute a cross-jurisdictional audit to ascertain which external agencies accessed, modified, or appended data to a specific file traversing the national infrastructure; they are strictly limited to viewing the superficial outputs authorized by the federal gatekeeper.
46. Consequently, *Order MO-4542* establishes an unassailable legal syllogism that heavily favours the present requisition: because municipal agencies are administratively prohibited and technologically barred from executing the necessary exaction of deep offline metadata encompassing multiple

jurisdictions, the Royal Canadian Mounted Police remains the sole, exclusive, and unassailable entity possessing both the overarching legal jurisdiction and the centralized technological capability to fulfill this statutory requisition. The centralized [personal information bank rcmp ppu 005] (the "**Personal Information Bank RCMP PPU 005**") is the exclusive, paramount repository capturing the unalterable digital footprints of all constituent agencies interacting with the national mainframe. The federal host is the only entity with the omniscient technological vantage point necessary to retrieve the requested transaction logs, rendering any attempted redirection by the RCMP an exercise in egregious administrative negligence and actionable bad faith.

47. Furthermore, the absolute necessity of directing this exaction exclusively to the federal steward is irrefutably compounded and rendered entirely self-evident by the fraudulent nature of the underlying documentation utilized to justify the deprivation of liberty. It is formally submitted that the [false information package] (the "**False Information Package**") currently in circulation is a documented fabrication, intrinsically devoid of factual accuracy, procedural regularity, or jurisdictional reliability. *Ipso facto*, because the aforementioned instrument is fundamentally vitiated and its provenance intentionally obscured by state actors, it constitutes an absolute epistemological impossibility for the applicant to ascertain precisely which specific municipal or provincial constabulary maliciously or erroneously transmitted the *acta* into the federal database.
48. Due to the inherent unreliability, deliberate obfuscation, and contested nature of the [false information package] (the "**False Information Package**"), the true originating entity remains entirely concealed. The fraudulent entry could theoretically have been initiated by the [toronto police service] (the "**Toronto Police Service**"), the [peel regional police] (the "**Peel Regional Police**"), the [ontario provincial police] (the "**Ontario Provincial Police**"), or any other unidentified law enforcement apparatus operating within the province. If an obligation were improperly imposed upon the applicant to direct localized access requests to individual municipal agencies based upon a demonstrably fraudulent document, such an endeavour would constitute an exercise in profound, Kafkaesque bureaucratic futility. The citizen would be forced to navigate a labyrinth of endless denials, haphazardly guessing the culprit, while each respective agency plausibly claims ignorance of the forged document and disavows any involvement.
49. The deliberately constructed jurisdictional ambiguity engineered within the [false information package] (the "**False Information Package**") is designed specifically to obfuscate the true originating agency and shield the perpetrators from legal, civil, and administrative accountability. Therefore, the Royal Canadian Mounted Police, acting as the supreme custodian of the [offline historical database] (the "**Offline Historical Database**") under the strict auspices of the [personal information bank rcmp ppu 005] (the "**Personal Information Bank RCMP PPU 005**"), is the singular, indispensable institution capable of bypassing this localized subterfuge. Only the centralized federal repository possesses the technological capability to definitively expose the unvarnished digital truth via the extraction of the unforgeable [originating agency identifier] (the "**Originating Agency Identifier**"). By extracting this unalterable cryptographic signature, the RCMP can irrefutably identify the true authors of the vitiated *acta*, pierce the veil of inter-agency obfuscation, and unequivocally restore the *status quo ante*.

V. GEOGRAPHICAL NEXUS, SYSTEMIC TERMINAL IDENTIFICATION, AND JURISDICTIONAL NULLITY

50. In direct, meticulous satisfaction of the institutional request for precise geographical particularization, it is explicitly confirmed that the originating locus of the underlying investigation, the purported locus of the alleged offense, and the presumed terminal origin of the initial systemic entry is localized entirely within the specific territorial boundaries of Toronto, Ontario.

51. The forensic extraction must specifically correlate with the [toronto police service] (the "**Toronto Police Service**"), predominantly focusing upon the 52nd Division as the presumed originating agency responsible for the investigative genesis, and the 14th Division as the geographic venue of the ultimate physical deprivation of liberty. This highly unusual, seemingly disjointed administrative bifurcation of the investigation into dual occurrences across separate, geographically distinct divisions necessitates a highly precise temporal mapping of all judicial authorizations applied within the local municipal infrastructure.
52. Such fragmentation of the operational record is frequently indicative of profound procedural anomalies, suggesting deliberate strategic maneuvers by field officers intended to bypass the continuous, localized scrutiny of a single judicial oversight officer, thereby engaging in a form of impermissible jurisdictional arbitrage. When a warrant is sought in one division but executed under the auspices of another, or when an investigation is fractured across multiple event numbers to obscure the evidentiary chain, the digital audit trails operate as the sole unifying thread capable of exposing irregular procurement practices, effectively laying bare the *actus reus* of systemic manipulation.
53. The exact systemic identifiers required to flawlessly triangulate the administrative entries are formally established as Toronto Police Service occurrence number 2024-2028093, Toronto Police Service occurrence number 24-2082035, and the centralized archival indexing cipher documented as [police case identification number] (the "**Police Case Identification Number**") 457197. These highly specific alphanumeric ciphers provide the exact algorithmic coordinates required to immediately isolate the relevant data packets within the vast national mainframe, thereby completely eliminating any institutional pretense of ambiguity, search impossibility, or resource strain.
54. It is further submitted that the extraction of the [originating agency identifier] (the "**Originating Agency Identifier**") operates as an unforgeable cryptographic signature for every individual transaction executed within the database. The presence of this specific identifier irrevocably traces the exact physical terminal, the originating IP address, the precise user credentials, and the exact temporal data input back to a specific law enforcement division and physical location. This technological reality absolutely prevents any local agency from plausibly disclaiming responsibility for a fraudulent, extra-jurisdictional, or technologically corrupted entry. The systematic triangulation of these systemic ciphers against the physical court registries constitutes the exclusive, unimpeachable methodology for verifying the *prima facie* legitimacy of the underlying authorization.
55. A robust, insurmountable counter-argument must be preemptively advanced against the potential assertion by state actors that a geographical discrepancy in the issuance of a warrant is a mere, easily curable administrative defect under the *Criminal Code*, RSC 1985, c C-46 (the "*Criminal Code*"). A non-originating judicial officer (for illustrative purposes, a Justice of the Peace sitting in the jurisdiction of Brampton) possesses absolutely zero inherent jurisdiction to arbitrarily issue a warrant for a completely unconnected territorial jurisdiction (such as Toronto) absent strict, demonstrable, and explicitly documented statutory compliance delineated within the specific backing provisions of the *Criminal Code* (e.g., Section 529 regarding telewarrants or the highly restrictive execution of warrants across territorial divisions).
56. Any appearance before a judicial officer lacking such explicit territorial authority is strictly *coram non jure* (not before a judge). The foundational proceedings are utterly vitiated, entirely lacking any legal substrate. The fundamental, unyielding common law maxim *nemo dat quod non habet* (no one gives what they do not have) dictates with absolute, mathematically precise certainty that a judicial officer cannot confer lawful authority over a geographic jurisdiction to which they are not statutorily, formally, or temporally assigned by the Chief Justice of the respective court. To assert otherwise is to endorse a regime of roving, borderless judicial commissions explicitly rejected by the architecture of Canadian federalism and provincial judicial administration, thereby inviting profound constitutional chaos.

194 57. Therefore, if the extracted [originating agency identifier] (the "**Originating Agency Identifier**") reveals that the initial systemic entry emanated from a jurisdiction wholly disconnected from the documented [issuing authority] (the "**Issuing Authority**"), or if the court designation was retroactively, inexplicably upgraded from the Ontario Court of Justice to the Superior Court of Justice without a corresponding, authenticated judicial endorsement on the physical information, the process is an absolute, irredeemable nullity *ab initio*. The warrant is entirely void, and the subsequent arrest is rendered unequivocally unlawful, constituting an actionable tort of false imprisonment and an egregious, flagrant breach of the *Charter*. The deliberate suppression of such exculpatory metadata by the federal repository is tantamount to the active concealment of an unlawful arrest, a profound breach of institutional trust, and a catastrophic violation of the principles of fundamental justice.

VI. TEMPORAL PARAMETERS, THE FORENSIC WINDOW, AND THE PREJUDICE OF DELAY

58. In meticulous fulfillment of the requirement for a definitive temporal framework to explicitly guide the offline exaction, the [forensic window] (the "**Forensic Window**") is strictly circumscribed to the specific period commencing on September 15, 2024, and definitively terminating on December 31, 2024.
59. The genesis date of September 15, 2024, correlates precisely with the formal establishment of the primary investigatory occurrence within the municipal dispatch framework. The deliberate, highly calculated expansion of the terminal date to December 31, 2024, is legally, strategically, and forensically imperative. This extended, post-arrest parameter is explicitly formulated to rigorously capture any covert systemic [modify transaction] (the "**Modify Transaction**") or [cancel transaction] (the "**Cancel Transaction**") executed long after the physical apprehension was formally concluded.
60. It is vehemently posited that if an act of *ultra vires* judicial authorization was retroactively sanitized by system operators to conceal jurisdictional defects, the resulting [documentary metamorphosis] (the "**Documentary Metamorphosis**") would have necessarily transpired during the weeks immediately following the effectuation of the physical arrest on October 2, 2024. This extended temporal window represents the precise period wherein institutional actors desperately sought to reconcile the disparate, unsworn physical paperwork with the unalterable digital ledger, frequently necessitating illicit electronic alterations to force the system to accept an otherwise deficient, structurally flawed warrant.
61. The extreme urgency of this temporal extraction is drastically exacerbated by the rigid constitutional strictures delineated in the landmark decision *R v Jordan*, 2016 SCC 27 (the "*Jordan*"). In *Jordan*, the Supreme Court of Canada established a presumptive, inflexible, and mathematically precise ceiling of 18 months for the completion of trials prosecuted by summary conviction. Applied strictly to the present commencement date of September 23, 2024, the absolute terminal date for the vindication of the right to a trial within a reasonable time is irrevocably fixed at March 23, 2026.
62. Any administrative delay precipitated by the federal institution's failure to provide unvarnished, timely access to the forensic metadata constitutes a direct, highly prejudicial impediment to the fundamental ability of the accused to make full answer and defence, explicitly protected under Section 11(a) and 11(d) of the *Charter*. The state is strictly prohibited from utilizing its own technological obfuscation, bureaucratic lethargy, and artificially compartmentalized administration to deliberately exhaust the *Jordan* ceiling. Opposing counsel may attempt to baselessly argue that the provincial Crown bears no responsibility for the administrative delays of an ostensibly independent federal body regarding a parallel *Privacy Act* request.

63. This argument is fatally flawed, legally bankrupt, and universally rejected by sophisticated appellate courts. The delay operates as a unified, systemic deprivation of rights, extending the prosecutorial shadow over the citizenry while the state apparatus simultaneously withholds the very exculpatory evidence of jurisdictional nullity. The Supreme Court has repeatedly affirmed that the various branches of the state cannot point fingers at one another to excuse the deprivation of constitutional rights; thus, rendering the delay entirely and indisputably attributable to the unified state apparatus. The Crown's continuous failure to compel the Royal Canadian Mounted Police to release exculpatory metadata represents a fatal flaw in the prosecutorial timeline, directly contributing to the exhaustion of the *Jordan* calculus.
64. Concomitantly, the Crown possesses an unremitting, ongoing, and absolute obligation to disclose all relevant information, as definitively established in *R v Stinchcombe*, [1991] 3 SCR 326 (the "*Stinchcombe*"). While the Royal Canadian Mounted Police may superficially assert that it operates completely independently of the prosecuting provincial Crown, the sophisticated jurisprudence articulated in *R v McNeil*, 2009 SCC 3 (the "*McNeil*") conclusively establishes that records held by any police forces—including federal databases—that are relevant to the underlying validity of the state's case must be proactively accessible to prevent gross miscarriages of justice. The artificial boundaries between "first-party" and "third-party" records are completely dissolved when the federal database holds the very foundational *acta* that authorized the provincial prosecution in the first instance.
65. The systemic audit logs definitively proving the true jurisdictional origin of the warrant are undeniably relevant first-party records under the combined *Stinchcombe* and *McNeil* frameworks. The unquestionable integrity of the judicial authorization is the *sine qua non* (the essential, indispensable condition) of the entire prosecution. This undeniable reality elevates this *Privacy Act* requisition far beyond a mere administrative entitlement, transforming it into a fundamental, constitutionally protected component of trial fairness that must be executed with maximal expediency to prevent the ultimate, inevitable collapse of the prosecution due to systemic non-disclosure.

VII. THE PERSONAL INFORMATION IS ABOUT ME BUT FOR SAKE OF ARGUMENT – PUBLIC INTEREST OVERRIDES

66. Pursuant to the strict strictures delineated within Section 8(1) of the *Privacy Act*, personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with highly specific statutory provisions. It is formally declared, unequivocally established, and permanently entered into the administrative record that the applicant is the exclusive subject of the requested digital *acta*. Concomitantly, absolute, unreserved, and explicit consent is hereby provided for the comprehensive, unredacted disclosure of any and all metadata, transaction logs, and systemic entries pertaining to the applicant. The primary statutory barrier to disclosure, theoretically predicated upon the protection of the subject's privacy, is thus entirely and permanently extinguished *in limine* by the subject's own proactive volition.
67. Assuming, *arguendo* (for the sake of argument), that the federal institution attempts to manufacture a convoluted administrative pretext to withhold the requested digital artifacts despite the provision of absolute consent—perhaps by fallaciously asserting the inextricable entanglement of peripheral institutional methodologies or unspecified third-party identifiers—such an obstructionist posture is immediately vitiated by the paramount public interest override provisions enshrined within the statute.

58. Specifically, Section 8(2)(m) of the *Privacy Act* functions as a formidable public interest override, explicitly granting the head of a government institution the statutory discretion—and, in circumstances characterized by profound state overreach, the overriding administrative mandate—to disclose personal information even in the complete absence of standard consent protocols. The statute dictates that disclosure is legally permissible and administratively justified if:
- Under Section 8(2)(m)(i), the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or
 - Under Section 8(2)(m)(ii), disclosure would clearly benefit the individual to whom the information relates.
69. Regarding the application of Section 8(2)(m)(i), it is vehemently posited that the overarching public interest in exposing fraudulent judicial authorizations, *ultra vires* law enforcement actions, and the systemic manipulation of the national police database astronomically outweighs any theoretical, manufactured invasion of privacy. A functioning democracy is fundamentally reliant upon the absolute, unimpeachable integrity of its criminal justice infrastructure. The exposure of the fabricated [false information package] (the "**False Information Package**") and the conclusive identification of the state actors responsible for its systemic promulgation serve a compelling, non-derogable democratic interest. The public possesses a paramount, unassailable right to be assured that the [canadian police information centre] (the "**Canadian Police Information Centre**") is not being utilized as a clandestine repository for forged warrants designed to facilitate unlawful deprivations of liberty.
70. Concurrently, regarding the application of Section 8(2)(m)(ii), it is an incontrovertible legal reality that the comprehensive disclosure of the requested forensic metadata would clearly, directly, and profoundly benefit the individual to whom the information relates. The extracted hexadecimal dumps and unalterable audit trails provide the exact exculpatory evidence mathematically required to definitively quash an unlawful arrest, dismantle a fraudulently constructed prosecution, and forcefully vindicate the applicant's fundamental rights guaranteed under the *Charter*. Conversely, the continued withholding of this information by the federal steward actively perpetuates a profound, ongoing prejudice against the individual, effectively compounding the original constitutional violation by denying the citizen the very tools necessary for legal exculpation. Therefore, even if the primary mechanism of explicit consent were administratively disregarded, the public interest override strictly mandates the immediate, unredacted release of the requested records.

VIII. ANTICIPATORY REBUTTAL OF STATUTORY EXEMPTIONS AND CONCLUSION

71. Anticipating potential institutional reliance upon the highly discretionary law enforcement exemptions delineated under Section 22(1)(b) of the *Privacy Act*, it is preemptively asserted that any such application would be legally untenable, demonstrably unreasonable, and a glaring manifestation of extreme institutional bad faith. It is highly probable that it may be counter-argued by the institution's legal counsel or policy analysts that the unredacted release of systemic audit logs could theoretically reveal confidential investigative techniques, expose ongoing operational strategies, or generally jeopardize the overarching security and efficacy of the national database itself.
72. This proposition is fundamentally flawed, structurally illogical, and entirely inapplicable to the highly specific facts at bar. The underlying operational phase of the law enforcement engagement is irrevocably concluded. The judicial authorization has been physically executed, the subject has been processed through the municipal intake system, and the systemic alert has been explicitly cleared

from the active interface. The systemic records currently sought do not encompass prospective investigatory techniques, the deeply protected identities of confidential informants, covert surveillance protocols, or sensitive tactical intelligence. Rather, they constitute entirely historical, administrative *acta* definitively proving the foundational jurisdictional validity (or nullity) of a finalized, crystallized, and historically completed state action. Typing a warrant into a database is a purely administrative clerical function, not a privileged investigative technique shielded from public scrutiny.

73. The absolute, non-derogable necessity of accessing these records is further codified by the foundational principles articulated in *R v Garofoli*, [1990] 2 SCR 1421 (the "*Garofoli*"). In *Garofoli*, the Supreme Court established the absolute, unimpeachable right of an accused to challenge the underlying validity and factual foundation of a judicial authorization (the constitutionally protected right to "go behind" the warrant). This fundamental, universally recognized right is rendered functionally illusory and entirely meaningless if the immutable digital metadata proving its invalidity is systematically withheld by the executive branch under the spurious, overly broad guise of "investigative privilege."
74. The invocation of such discretionary exemptions to conceal *prima facie* procedural anomalies, to mask the true identity of an authorizing justice, or to shield potential institutional *fraus omnia corrumpit* (fraud unravels all) from public and judicial scrutiny, constitutes a gross abuse of administrative discretion that fundamentally offends the *lex terrae* (the law of the land). A free and democratic society cannot abide the deployment of secret digital ledgers to validate deprivations of liberty, mirroring the clandestine, unaccountable operations of a star chamber.
75. Furthermore, reliance is firmly placed upon the strict doctrine of *functus officio* as articulated in *Chandler v Alberta Association of Architects*, [1989] 2 SCR 848 (the "*Chandler*"). The *Chandler* jurisprudence affirms that once a judicial or administrative officer has finally decided a matter and formally issued their order, their jurisdiction over that specific matter is entirely exhausted, spent, and permanently extinguished. Consequently, the issuing judicial officer became entirely *functus officio* at the exact moment the warrant was promulgated and subsequently executed by the arresting officers.
76. The authorization itself simultaneously crystallized into an unalterable administrative, historical record. The statutory shield of investigative privilege cannot be conceptually retrofitted, legally contorted, or practically expanded to conceal jurisdictional overreaches or the subsequent *ex post facto* generation of documents explicitly designed to sanitize a vitiated apprehension. Once a warrant is executed, the "investigation" pertaining to the acquisition of that specific warrant is permanently concluded; the state cannot continuously claim ongoing privilege over historical facts to avoid constitutional accountability.
77. A further, highly predictable institutional counter-argument may assert that the Royal Canadian Mounted Police, functioning merely as an inert host or passive repository, cannot alter, correct, or append data to records inherently "owned" by another municipal agency. This assertion is categorically dismantled by the explicit, non-delegable remedial provisions contained within the *Privacy Act*. The statute encompasses powerful, non-discretionary mechanisms designed specifically to cure the retention of vitiated, inaccurate documentation within federal repositories, entirely regardless of its original municipal source.
78. Should the requested audit trails substantiate the presence of fundamentally inaccurate information—such as a falsified court location, an altered judicial endorsement, or an entry entirely lacking jurisdictional competence—the statutory right to demand an immediate correction, or alternatively, the mandatory application of a [notation of disagreement] (the "**Notation Of Disagreement**") under Section 12(2) of the *Privacy Act*, shall be immediately, forcefully, and unequivocally exercised by the applicant.
79. Pursuant to the strict mandates of Section 12(2)(c), the institution is legally obligated to actively notify any person, body, or government institution to whom the fraudulent information was disclosed within the preceding two years, formally appending the [notation of disagreement] (the "**Notation Of**

198 **Disagreement**") to every subsequent dissemination. The withholding of the underlying audit trails renders these powerful statutory remedies functionally illusory, insulates the state from systemic accountability, and directly violates the fundamental principles of fundamental justice protected by Section 7 of the *Charter*.

80. The Royal Canadian Mounted Police, functioning as the supreme system administrator, is uniquely positioned and statutorily compelled to execute this notation upon the centralized mainframe, entirely irrespective of the initial authoring agency's preferences, objections, or internal politics. Ignorance of this overarching federal obligation is absolutely no defense (*ignorantia juris non excusat*). The federal repository cannot become a sanctuary for locally manufactured fraudulent documents without explicitly implicating the federal government in the continued propagation of the fraud.
81. The preservation of the unvarnished digital truth is the paramount objective of this requisition.
82. The individual is optimally positioned and fully prepared to file a formal, expedited complaint with the Office of the Privacy Commissioner of Canada, explicitly invoking the investigatory powers utilized in the *OPC 2011 Audit* and the *OPC 2014 Suicide Investigation*.
83. As the requisite administrative clarifications demanded on March 16, 2026, have been exhaustively, meticulously, and formally satisfied *in limine*, the Royal Canadian Mounted Police is legally bound to immediately recommence the active processing of this requisition without further prevarication.
84. Trusting that this cannot take more than an hour to provide the requested personal information, kindly provide it to me and I can review the same, and then confirm that the request is closed.
85. Thank you kindly.

All of which is respectfully submitted.

KAM

Enclosures:

1. Demonstration of overt fraud by whomever manipulated the Information Package into the FIP when measured against an Information Package from the

APPENDIX: Juridical Analysis: Implications of Order MO-4542 for Requisitions under the Privacy Act

I. Executive Overview of Order MO-4542

In the significant matter of *Halton Regional Police Services Board (Re)*, 2024 CanLII 62738 (ON IPC), the Adjudicator deliberated upon the transparency requirements inherent to national law enforcement databases, specifically focusing on the intersection of local administrative boundaries and centralized federal data repositories. The proceedings originated from a request for the disclosure of records detailing all inquiries pertaining to a specific individual conducted by any police service within the Canadian jurisdiction across the **CPIC**, **PARAS**, and **NCIC** systems.

A definitive jurisdictional boundary was established by the Adjudicator, predicated upon a distinction between two discrete categories of digital artifacts, which serves as a foundational precedent for understanding data ownership in a networked law enforcement environment:

1. **Local Access Records:** These comprise the granular data generated as a direct consequence of queries initiated by officers of a specific regional constabulary. Such records, reflecting the internal operations and specific investigative choices of that force, are deemed to reside within the "custody and control" of the respective local board.
2. **Systemic Audit Logs (The "Offline" Repositories):** These are the centralized and exhaustive transaction logs encompassing all queries executed by any constituent agency within the national technological architecture. Crucially, it was determined that local boards do **not** possess custody or control over these systemic logs. The Adjudicator reasoned that a municipal force lacks the unilateral authority to audit the activities of external agencies within the mainframe environment managed exclusively by the Royal Canadian Mounted Police (RCMP). This finding effectively designates the RCMP as the sole authority capable of accessing the "omniscient" view of the system's transaction history.

II. Strategic Advantages for the Requisitioning Party

Order MO-4542 provides significant jurisprudential support for the current requisition, offering the necessary legal framework to necessitate compliance from the federal institution by removing the possibility of administrative buck-passing.

1. The Preclusion of Procedural Deflection via the Originator Control Principle

The Royal Canadian Mounted Police frequently invokes the "Originator Control" principle to redirect *Privacy Act* requisitions to municipal entities, arguing that the agency that first entered the data retains ownership of the record. Order MO-4542 serves to invalidate the applicability of this defense in the specific context of systemic metadata. Adjudicator Faughnan clarified that a municipal police board remains legally and technologically incapable of providing a cross-jurisdictional audit trail, regardless of its role as an "originator" of individual data entries.

Consequently, the citing of this precedent establishes that the RCMP is not merely a passive host or a digital "landlord" but the **sole legal custodian** of the systemic metadata. Should the RCMP decline the production of these records, the information would be rendered a "legal nullity"—unobtainable from any source across the municipal, provincial, or federal levels. Such a result would stand in direct contravention of the quasi-constitutional status afforded to the *Privacy Act* by the Supreme Court of Canada, which mandates that the Act be interpreted in a manner that favors the right of access. This compels the acknowledgement that the duty of disclosure rests exclusively with the managers of the CPIC infrastructure, as they alone hold the keys to the "master log" that local boards are legally barred from accessing.

2. Validation of Technological Feasibility and Extant Record Status

Institutional claims asserting that the production of forensic metadata or transaction logs necessitates the "creation of a new record" are frequently utilized to circumvent statutory obligations under Section 4 of the *Privacy Act*. However, Order MO-4542 explicitly addresses the **"off-line search"** protocol as a known and established procedure within the RCMP's operational toolkit.

The Adjudicator observed that such searches constitute a standard, albeit specialized, function of the database management system used to track historical interactions that are no longer "live" on the front-end interface. This provides a robust precedent: the "Offline Historical Database" is recognized as an extant repository of records, not a hypothetical construct. Reference to this order demonstrates that the requisition pertains to the retrieval of existing data through established forensic protocols rather than the creation of novel information or the programming of new software. The focus is thereby shifted from a debate over

technical capability to a direct assessment of statutory obligation. Furthermore, it implies that a refusal to perform such a search constitutes a failure to conduct a "reasonable search" as required by law.

3. Verification of Necessity and Exhaustion of Administrative Remedies

The invocation of MO-4542 serves to demonstrate that the applicant has exercised profound due diligence in the pursuit of administrative remedies. It illustrates that the requisition of such metadata from regional boards, such as the Toronto Police Service, would constitute a futile exercise in administrative circularity. Since the IPC has affirmed that these regional boards lack the requisite jurisdiction and technical interface to facilitate cross-agency audits, the applicant is justified in proceeding directly against the federal administrator.

This "exhaustion of remedies" argument is paramount in precluding the institution from employing administrative redirection as a method of procedural delay. It forces the RCMP to confront the reality that they are the "court of last resort" for this specific category of information. By presenting MO-4542, the applicant effectively closes the loop on any argument that the request is "premature" or directed at the "wrong authority."

III. Legal Implications and Systemic Consequences

The Doctrine of the "Omniscient Vantage Point"

Order MO-4542 affirms a critical power imbalance: while local police services are restricted to viewing their own internal activity, the RCMP maintains an "omniscient technological vantage point" over the entire Canadian law enforcement landscape. In instances where "Documentary Metamorphosis"—the unauthorized or fraudulent alteration of judicial data such as warrants or occurrence reports—is suspected, these systemic logs represent the singular medium through which the truth may be observed.

Specifically, the "Offline" logs capture the **unaltered [Originating Agency Identifier]** and the timestamp of every modification. Absent the disclosure of these logs, the integrity of the judicial process is compromised. Local logs are susceptible to internal manipulation or may only represent a fragmented, "polished" portion of the transaction history. The systemic logs, held by the RCMP, act as an unalterable "black box" recorder for the justice system, and Order MO-4542 establishes the precedent that access to this black box is a matter of law, not institutional discretion.

Non-Delegable Stewardship of the Sovereign Custodian

The decision reinforces the status of the RCMP as the "Sovereign Custodian" of national security and law enforcement data. A refusal by the federal institution to disclose such data, especially when coupled with the proven inability of local agencies to provide it, would result in the creation of an impermissible "dark zone" within Canadian privacy law. In this dark zone, personal data could be queried, modified, and shared by thousands of officers without any possibility of oversight or correction by the individual concerned.

Order MO-4542 facilitates the argument that the *Privacy Act* was enacted specifically to provide transparency within these complex, multi-jurisdictional digital environments. It suggests that as systems become more centralized and "intelligent," the duty of the central administrator to provide transparency increases proportionally. Consequently, a refusal to initiate an offline search when "Documentary Metamorphosis" is at issue is not merely a procedural denial but a direct infringement upon the statutory rights of the individual to ensure the accuracy and lawful use of their personal information.

- **The Precedent of Limitation:** Order MO-4542 confirms that municipal police entities are both technologically and legally precluded from fulfilling cross-jurisdictional audit requisitions, thereby identifying the "dead end" of local inquiries.
- **The Mandate of the Central Repository:** The Royal Canadian Mounted Police, as the exclusive administrator of CPIC PPU 005, constitutes the only entity possessing the physical and legal "custody and control" of the **unvarnished digital truth** regarding systemic database interactions.
- **The Non-Delegable Requirement:** The institution is legally barred from redirecting this requisition to municipal partners, as such redirection would be a known path to failure. It is incumbent upon the RCMP to initiate the "offline search" protocol immediately to satisfy its non-delegable statutory obligations pursuant to the *Privacy Act*, ensuring that the digital history of the individual remains transparent and accountable to the law.

Table 5: Forensic Audit Fields in the CPIC Historical Database

Audit Field	Data Captured	Investigative Value
Transaction Code	ADD, MODIFY, CLEAR, CANCEL	Identifies the lifecycle phase of the warrant.
Timestamp	Milliseconds / Date	Establishes the chronological veracity of the warrant entry.
ORI	Originating Agency Identifier	Identifies the specific police division responsible for the data.
Terminal ID	Physical Hardware Address	Proves where the data was entered (Court vs. Admin Office).
User ID	Credentials of the Operator	Identifies the individual who performed the systemic entry.

Table 6: Statutory Remedies under the Federal Privacy Act

Provision	Right Conferred	Application to Information Package
Section 12(1)	Right of Access	Compels the RCMP to disclose CPIC metadata and transaction logs.

Section 12(2)(a)	Right to Correction	Allows for the correction of fraudulent or manipulated data fields.
Section 12(2)(b)	Notation of Disagreement	Forces the system to flag the record as contested by the subject.
Section 12(2)(c)	Mandatory Notification	Requires the RCMP to inform justice partners of the inaccuracy.

The use of these statutory mechanisms is essential for restoring the *status quo ante* in the face of systemic administrative failure. In a justice system that increasingly relies on automated digital records, the ability to audit the provenance of those records is the only viable defense against technological vitiation and jurisdictional overreach.

Impact of Software Bugs on Documentary Integrity

The technical deficiencies of GrapeCity Documents for PDF version 6.0.2.0 may have contributed directly to the "metamorphosis" of the Information Package. Technical reports indicate that this version of the library suffered from memory management issues and failures to correctly render complex PDF structures. When a server-side application experiences an "Item already has an owner" exception, it can lead to unstable document generation where metadata from one object is incorrectly rendered or missing entirely.

This technical instability corroborates the structural errors noted in the 43-point deficiency chart, particularly the failure to render a judicial signature on Page 3 despite including an attribution text. While these might be viewed as "glitches" by a developer, in a legal context, they constitute a failure to maintain a valid and accurate record of a judicial authorization. The presence of the GrapeCity SDK as the "Producer" is the key technical artifact that links the document to a custom-coded government portal, suggesting that the document was born from an automated digital system rather than a clerk-validated manual process.

Yours faithfully,

/KAM

Mr. Kevin A. McLean (BA, JD, CIM)

Sender's name: Mr. Kevin Alexander McLean (BA, JD, CIM)

Sender's Telephone Number: (647) 370-9354

Sender's email address: mcleansettlement@gmail.com

On Mon, Mar 16, 2026 at 2:23 PM ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca> wrote:

Dear Kevin McLean:

This is a follow-up to your request under the Privacy Act, which was received by this office on March 12, 2026, for:

Tab B

204 is formally demanded that the Institution immediately conduct a comprehensive offline search (the "Offline Search") of the highly secure Offline Historical Database to retrieve all artifacts associated with the PIB RCMP PPU 005 repository (Operational Case Records).

This explicit demand for exaction encompasses the following specific forensic artifacts, which are indispensable for the forensic reconstruction of the record:

- a. The retrieval of all active, cleared, canceled, or purged WANT Records associated with Kevin A. McLean spanning the entirety of the year 2024, including historical status codes (the "Historical Status Codes").*
- b. The unredacted production of all system Transaction Logs, audit trails, and hexadecimal dumps (the "Hexadecimal Dumps") governing the entire lifecycle of the warrant entry, including all ADD, MODIFY, CLEAR, and CANCEL Transactions, and any supervisor override actions recorded within the federal mainframe.*
- c. The explicit disclosure of the associated timestamps (accurate to the millisecond), the ORIs, the unique user IDs of terminal operators, the precise terminal hardware addresses, and the entirety of the narrative and remarks fields (the "Narrative Fields") for each sequential transaction, demonstrating the evolutionary history of the data entry and any unauthorized "metamorphosis."*

In order to process your request we require additional information:

- **Scope:** We have examined your request and fail to understand exactly what you are seeking in terms of records or documentation. As per section 12(1)(b) of the Privacy Act, "A request for access to personal information shall be made in writing to the government institution that has control of the information and shall provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution." **Please review the above request text and confirm that the text accurately reflects the information you are requesting .**
- **Other policing agency:** The Privacy Act has established the right of applicants to access federally maintained records. If this particular matter concerned another police department or government agency, they may have information of interest to you. The Privacy Act does not authorize the RCMP to search files or to disclose information belonging to other police forces or government agencies. **Please confirm the file is located with the RCMP.**
- **Location:** Concerning operational case records associated with your name, please provide a specific location (city and province and/or detachment) you wish to have searched. The RCMP has numerous autonomous units and in many instances the investigative information is strictly available from the unit conducting the investigation.
- **Time Frame:** Please provide a time frame or date of occurrence to narrow the search for your requested information. If you are requesting information over a period of time, please provide a clear start and end date.

You may send this via regular mail or e-mail (reply to this email) to the contact listed below.

Your file will remain open in our office for the next 10 days. If we have not received a response by **March 26, 2026**, this file will be closed.

Please be advised that you are entitled to lodge a complaint with the Privacy Commissioner concerning the processing of your request. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Privacy Commissioner of Canada
30 Victoria Street, 1st Floor
Gatineau, Quebec K1A 1H3

Additional information on the complaint process can be found at the following link: <https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa S.
Access to Information and Privacy Branch

205

Mailstop #61
Leikin Drive
Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'avisier immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

4 attachments



Information Package 4810 998 24 48129169-00 (4).pdf

329K [View as HTML](#) [Scan and download](#)



ADULT-COMMON-INFORMATION-FORM-WITH-HIGHLIGHTED-CHANGES - LINCOLN COUNTY LAW ASSOCIATION.pdf

215K [View as HTML](#) [Scan and download](#)



Chart-FIP and GrapeCity-demonstrating 43 errors in FIP-For Archives Ontario-search for authentic records-17-Oct-25.pdf

169K [View as HTML](#) [Scan and download](#)



Kind response to RCMP CPIC - Mellisa S - Requestor - KAM (BA JD CIM) - 556 pm - March 16 2026.pdf

628K [View as HTML](#) [Scan and download](#)

DATE: March 16, 2026

CREATED WITH DICTATION OR VOICE-TO-TEXT SOFTWARE - RESERVATION OF RIGHTS TO CORRECT ANY SPELLING, GRAMMAR, SYNTAX, IMPORTANT QUALIFIERS AND/OR INCORRECT DOUBLE NEGATIVES:

DELIVERY METHOD: Via Electronic Transmission

TO: Melissa S.

Access to Information and Privacy Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario

K1A 0R2

REFERENCE: Privacy Act request P-2025-16999 / F339

SUBJECT I: Formal Clarification and Requisition of Forensic Metadata Pursuant to the Privacy Act (Canada)

SUBJECT II: Jurisprudential Abrogation of the Originator Control Defense and the Non-Delegable Stewardship of the Royal Canadian Mounted Police

SUBJECT III: Geotemporal Delineation of Required Systemic Audit Trails

SUBJECT IV: Anticipatory Rebuttals of Statutory Exemptions and the Foreclosure of Institutional Obfuscation

SUBJECT V: The Intersection of Digital Non-Repudiation, Forensic Epistemology, and the Vindication of Charter Rights

SUMMARY OF YOUR EMAIL AND MY BRIEF RESPONSES PRIOR TO THE LENGTHIER ONE DUE TO THE NEED FOR THE PERSONAL INFORMATION OF MINE DUE TO THE THREATS TO MY LIFE, LIBERTY AND SECURITY WITH THANKS.....2

1. Scope of the Request	2
2. Whether the Records Are Held by the RCMP	3
3. Location of the Records	3
4. Time Frame and Underlying Particulars	4
A. First Occurrence Number (TPS)	4
B. Second Occurrence Number (TPS)	4

C. TPS Case Identification Number (MOST LIKELY THE COURT FILE NUMBER WITH THE SCJ 361 UNIVERSITY AVENUE, 1ST FLOOR)	4
D. Commencement of Proceedings (date information is sworn and laid)	4
E. Informant / Court Officer	4
F. Intake Court Endorsement	5
G. Arrest Information	5
H. Additional Context Regarding Date Ranges	5
For ease of reference, I include the following correspondence from the Superior Court of Justice Records Management Office:	5
Closing	6
I. PREFATORY STATEMENT OF GOVERNING LEGAL PRINCIPLES AND QUASI-CONSTITUTIONAL IMPERATIVES	6
II. THE "PERSONAL INFORMATION" NEXUS: SYSTEM LOGS AS IDENTIFIABLE DATA	7
III. LEGAL ANALYSIS: IMPACT OF ORDER MO-4542 ON RCMP PRIVACY OBLIGATIONS	8
IV. DELINEATION OF SCOPE, EXACTION OF METADATA, AND SYSTEMIC NON-REPUDIATION	9
V. JURISDICTIONAL STEWARDSHIP AND THE DOCTRINE OF ADMINISTRATIVE ESTOPPEL	9
VI. PROCEDURAL FRUSTRATION OF STATUTORY CORRECTION RIGHTS	10
VII. GEOTEMPORAL PARAMETERS AND SYSTEMIC IDENTIFIERS	10
VIII. THE "DEEMED REFUSAL" AND PUBLIC INTEREST OVERRIDE	11
II. INTRODUCTION AND PROCEDURAL POSTURE	11
III. DELINEATION OF SCOPE, EXACTION OF METADATA, AND SYSTEMIC NON-REPUDIATION	13
IV. JURISDICTIONAL STEWARDSHIP AND THE ABROGATION OF THE ORIGINATOR CONTROL DEFENSE	16
SUB-SECTION A: The Recency of Jurisprudential Mandates and the Evidentiary Void of the False Information Package	18
V. GEOGRAPHICAL NEXUS, SYSTEMIC TERMINAL IDENTIFICATION, AND JURISDICTIONAL NULLITY	20
VI. TEMPORAL PARAMETERS, THE FORENSIC WINDOW, AND THE PREJUDICE OF DELAY	22
VII. THE PERSONAL INFORMATION IS ABOUT ME BUT FOR SAKE OF ARGUMENT – PUBLIC INTEREST OVERRIDES	23
VIII. ANTICIPATORY REBUTTAL OF STATUTORY EXEMPTIONS AND CONCLUSION	25
APPENDIX: Juridical Analysis: Implications of Order MO-4542 for Requisitions under the Privacy Act	27
I. Executive Overview of Order MO-4542	27
II. Strategic Advantages for the Requisitioning Party	28
1. The Preclusion of Procedural Deflection via the Originator Control Principle	28
2. Validation of Technological Feasibility and Extant Record Status	29
3. Verification of Necessity and Exhaustion of Administrative Remedies	29
III. Legal Implications and Systemic Consequences	29

The Doctrine of the "Omniscient Vantage Point" 29

Non-Delegable Stewardship of the Sovereign Custodian 30

IV. Formal Jurisprudential Conclusion 30

**SUMMARY OF YOUR EMAIL AND MY
BRIEF RESPONSES PRIOR TO THE
LENGTHIER ONE DUE TO THE NEED
FOR THE PERSONAL INFORMATION OF
MINE DUE TO THE THREATS TO MY
LIFE, LIBERTY AND SECURITY WITH
THANKS**

Dear Melissa S:

Due to the extreme importance herein, I have provided a summary type response and then a much more detailed one to be efficient with public resources and respect the time of all involved.

Date: **March 16, 2026**
To: Access to Information and Privacy Branch
Royal Canadian Mounted Police
73 Leikin Drive, Mail Stop #61
Ottawa, Ontario K1A 0R2

Re: Privacy Act Request P-2025-16999 / F339 – Clarification Response

Thank you for your correspondence dated March 16, 2026. I appreciate the opportunity to provide clarifications so that my request may be processed efficiently and without delay. I remain fully committed to cooperating with your office and supplying any information necessary to facilitate the search.

In the interest of clarity and completeness, I address each of the four points raised in your letter and provide the relevant factual particulars for ease of reference.

1. Scope of the Request

I confirm that the text of my February 27, 2026 request accurately reflects the information I am seeking.

For clarity, the request concerns **my own personal information** contained within the **CPIC Investigative Data Bank**, governed by **Personal Information Bank RCMP PPU 005**, including:

- WANT records (active, cleared, cancelled, or purged)
- ADD, MODIFY, CLEAR, and CANCEL transactions
- All associated timestamps
- Originating Agency Identifiers (ORIs)
- Terminal identifiers
- User IDs of terminal operators
- Narrative and remarks fields
- All corresponding artifacts stored in the **Offline Historical Database**

This request is strictly limited to my personal information under s. 3 of the Privacy Act.

2. Whether the Records Are Held by the RCMP

I confirm that the records sought are held within the **control of the RCMP**, specifically within the CPIC system and its Offline Historical Database.

The attached findings of the Office of the Privacy Commissioner of Canada (OPC) confirm that:

“As the steward of CPIC...the RCMP bears responsibility for ensuring that all information shared...is done in accordance with the requirements of the MOC and in compliance with the Act.”

The CPIC Audit Report (2011) likewise confirms that the RCMP:

- Hosts the CPIC system
- Maintains its audit trails
- Oversees compliance
- Performs offline searches

Accordingly, the records fall within the RCMP's custody and control for the purposes of s. 12(1) of the Privacy Act.

3. Location of the Records

I respectfully clarify that the records requested are not located at a specific detachment. CPIC is a **centralized national system**, and the Offline Historical Database is accessible only to the RCMP.

Given the uncertainty surrounding the accuracy of municipal records—and the possibility that the originating police service may not be limited to the Toronto Police Service (TPS)—the only reliable and authoritative source of the relevant metadata is the **central CPIC system**.

For ease of reference, I provide all known particulars below.

4. Time Frame and Underlying Particulars

The relevant time frame is defined by the occurrence numbers, the commencement of proceedings, and the arrest date. All known particulars are provided below.

A. First Occurrence Number (TPS)

- **Event / Occurrence Number:** 2024-2028093
- **Date:** September 15, 2024
- **Case Manager:** PC Eric Tang #10942
- **Email:** 10942@tps.ca

B. Second Occurrence Number (TPS)

- **Event / Occurrence Number:** 24-2082035
- **Date:** September 22, 2024
- **Case Manager:** D/Cst. Michael Kolankowski #82239
- **Email:** 82239@tps.ca

C. TPS Case Identification Number (MOST LIKELY THE COURT FILE NUMBER WITH THE SCJ 361 UNIVERSITY AVENUE, 1ST FLOOR)

- **TPS Case ID:** 457197
- Appears on the Intake Court Endorsement
- Does **not** appear on the Form 10 Release Order

D. Commencement of Proceedings (date information is sworn and laid)

- **Date:** September 15 or September 23, 2024

E. Informant / Court Officer

- **Name:** Court Officer Christyn Frugoni-Rojas (née Christin Boulton)
- **Role:** Special Constable / Court Officer
- **Information Number (Form 2):** 4810 998 24 48129169

F. Intake Court Endorsement

- **Date:** September 23, 2024
- **Digital signature:** JP George Jiri
- **Note:** The endorsement contains no physical signature, location, or date stamp from the Brampton courthouse.
- **Presumed originating courthouse:**
 - **Ontario Superior Court of Justice – South Toronto Criminal Division**
 - 361 University Avenue, Toronto

G. Arrest Information

- **Arrest Date:** October 2, 2024
- **Arrest Location:** TPS 14 Division (350 Dovercourt Road, Toronto)
- **Arresting Officers:**
 - Cst. Anthony Romano #6097
 - D/Cst. Michael Roman Kolankowski #82239
 - Sergeant Sean Cassidy
- **Detective attending cells:**
 - Detective Abdulhameed K. Virani (TPS 52 Division)
- **Form 10 Release Order:**
 - Signed by Sgt. Cassidy and myself
 - Contained the TPS Occurrence Number (allegedly from September 22, 2024)
 - Did **not** contain the TPS Case ID Number

H. Additional Context Regarding Date Ranges

For ease of reference, I include the following correspondence from the Superior Court of Justice Records Management Office:

Email from SCJ RMO (Ms. Sana Azim) to ACT (Ms. Janet McLean)
Date: August 20, 2025
ACT ID: 3831309629

“Our office is unable to process orders with date ranges. Please list the exact dates your Ordering Party wishes to order and re-submit an updated order form.”

This illustrates why precise dates are provided above.

5. Summary of Relevant Time Frame

Based on the above, the relevant period for the CPIC Offline Search is:

- **September 15, 2024 → October 2, 2024**, inclusive
- Plus any subsequent CLEAR, CANCEL, or MODIFY transactions associated with the same entries (and thereafter)

Because CPIC records contain their own timestamps, I respectfully request that the RCMP retrieve **all records associated with my identifiers**, including any system-generated timestamps outside these dates that relate to the same entries.

Closing

I appreciate your assistance and confirm my full cooperation. If any further clarification is required, I will respond promptly to avoid delay. I look forward to the continued processing of my request within the statutory framework.

I reserve the right to provide further supporting evidence and authorities (if necessary) but I trust that this should not take more than an hour to collate and provide.

The public interest in light of the manipulation of government documents including an informant's name and that of a justice of the peace raise the question as to whether this is happening in isolated fashion or systematically.

Respectfully,

Kevin
B.A.,

A.
J.D.,

McLean
CIM

I. PREFATORY STATEMENT OF GOVERNING LEGAL PRINCIPLES AND QUASI-CONSTITUTIONAL IMPERATIVES

1. To definitively shape the jurisprudential landscape governing this requisition *in limine*, the following foundational legal principles are formally asserted and must govern the institution's administrative processing of this demand:
 - a. **Access to Information Rights – Purpose – Facilitate Democracy:** The overarching purpose of access to information rights (the "**Information Rights**") is strictly to facilitate

democracy by ensuring that citizens possess the unvarnished information required to participate meaningfully in the democratic process and to rigorously scrutinize state action;

b. **Privacy Rights – Purpose:** Concomitantly, privacy rights are structurally designed to protect the privacy of individuals with respect to personal information held by government institutions, while simultaneously providing individuals with an absolute, non-derogable right of access to that specific information;

c. **Quasi-Constitutional Status:** The *Privacy Act*, RSC 1985, c P-21 (the "*Privacy Act*") (alongside its provincial counterparts) is legally recognized by the highest appellate authorities as a quasi-constitutional statute, elevating its mandates far above standard administrative directives or institutional conveniences;

d. **Exceptions Interpreted Narrowly:** In *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 (the "*Lavigne*"), [2002] 2 SCR 773, Gonthier J. observed that exceptions from the rights set out in the act should be interpreted exceedingly narrowly, with any residual doubt resolved unequivocally in favour of preserving the applicant's fundamental right of access;

e. **Burden of Proof:** The burden of persuasion rests entirely and unshiftingly upon the person or institution asserting the exception (*Lavigne* at paras 30-31);

f. **Compelling State Interest:** In *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 (the "*Dagg*"), the Supreme Court of Canada articulated the governing principles of privacy law, affirming that the protection of privacy is a fundamental value in modern democracies and is inextricably enshrined within Sections 7 and 8 of the *Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11* (the "*Charter*"). Consequently, privacy rights and statutory access entitlements are to be compromised only where there exists a demonstrably compelling state interest for doing so (*Dagg* at paras 65, 66, 71)

II. THE "PERSONAL INFORMATION" NEXUS: SYSTEM LOGS AS IDENTIFIABLE DATA

2. While I do not agree that any clarification is so required, I will act in connectoin with our access partnership as it has been called. A critical clarification is necessitated regarding the nature of the requested metadata. It is anticipated that the institution may attempt to characterize hexadecimal dumps, audit trails, and transaction logs as mere "system information" or "technical overhead" falling outside the definition of Personal Information (PI) under Section 3 of the Act. Such a characterization is legally bankrupt and is hereby preemptively refuted
3. Drawing from federal jurisprudence, the definition of Personal Information must be given a broad and expansive interpretation (*Dagg v. Canada*, [1997] 2 S.C.R. 403; *Canada v. RCMP*, 2003 SCC 8). Personal Information is information "about" an identifiable individual, meaning it relates to or concerns the subject in a substantive way.
4. Under the "serious possibility" test articulated in *Gordon v. Canada (Health)*, 2008 FC 258, information constitutes PI if there is a "serious possibility" that an individual could be identified through its use, alone or in combination with other data. The requested logs are

inextricably linked to my identity because they are generated solely as a result of queries, entries, or modifications regarding my specific name, date of birth, and fingerprints. Without my PI, the log would not exist; therefore, the log is "information about an identifiable individual." As established in *Morgan v. Alta Flights Inc.*, 2006 FCA 121, the absence of a "human-readable" recording at the time of entry does not change the fact that the machine-level data remains Personal Information. To hold otherwise would allow the state to immunize its digital activities from oversight simply by storing them in non-textual formats.

III. LEGAL ANALYSIS: IMPACT OF ORDER MO-4542 ON RCMP PRIVACY OBLIGATIONS

5. A pivotal jurisdictional boundary has been established in *Halton Regional Police Services Board (Re)*, 2024 CanLII 62738 (ON IPC) [Order MO-4542], which addresses the transparency of national police databases. This decision establishes a critical distinction between "Local Access" and "Systemic Access."
6. **A. Foreclosure of "Originator Control" Deflection:** The RCMP frequently relies on the "Originator Control" principle to redirect *Privacy Act* requests back to municipal agencies (e.g., the Toronto Police Service). Order MO-4542 effectively demolishes this tactic. Adjudicator Faughnan clarified that a municipal police board is legally and technologically incapable of providing a cross-jurisdictional audit trail. They are "fenced off" from the broader system logs. By operation of law, the RCMP is the sole legal custodian of this systemic metadata. To refuse production is to render this information a "legal nullity"—available nowhere—which directly contradicts the quasi-constitutional status of the Act.
7. **B. Confirmation of Technical Capability and Existing Records:** The RCMP often claims that producing hexadecimal data or transaction logs would require the "creation of a new record." However, MO-4542 explicitly discusses the "off-line search" process. The Adjudicator noted that these searches are a standard, albeit deep-access, function of the database management system. This provides a powerful precedent: the "Offline Historical Database" is an existing repository. My request is for the retrieval of existing data through established forensic protocols, not a request for the RCMP to "program" a new report or perform complex coding.
8. **C. The "Omniscient Vantage Point" Argument:** MO-4542 confirms that while a local police service sees only its own "front-end" activity, the RCMP maintains the "omniscient technological vantage point." In this case, where "Documentary Metamorphosis" (unauthorized changes to warrant data) is suspected, the systemic logs are the only way to see the unaltered Originating Agency Identifier (ORI). Without the RCMP's "Offline" logs, the integrity of the judicial process is compromised because local logs can be limited to their own entries, effectively hiding extra-jurisdictional manipulation or unauthorized data "arbitrage."

IV. DELINEATION OF SCOPE, EXACTION OF METADATA, AND SYSTEMIC NON-REPUDIATION

9. The demand is surgically directed toward the foundational administrative architecture of the database, specifically the **Offline Historical Database** associated with **Personal**

Information Bank RCMP PPU 005.

- **A. Standard Computer Operations:** Under the *Privacy Regulations*, an institution must produce a record from machine-readable format using "standard computer hardware and software and technical expertise normally used by the government institution." The "Audit Log Viewer Tool" is a standard operational component of the National Police Services (NPS) infrastructure. Its utilization does not constitute the "creation" of a record; it is the standard retrieval of a machine-readable file. The RCMP cannot claim technical incapacity when it maintains specialized units specifically for the purpose of auditing these very systems for internal security
- **B. The Forensic Extraction vs. Human Readable Standard:** The Privacy Act requires "access," which the RCMP often misinterprets as providing a re-typed summary or a redacted PDF narrative. However, in this forensic context, the authenticity of the raw data is what is "about" me. A sanitized, human-readable summary is insufficient as it relies on the interpretation of an administrative clerk. I am seeking the transactional history of my PI—the raw data that cannot be "re-interpreted." Access that is not "complete" or "authentic" is not "access" under Section 12.
- The extraction must encompass all **Add, Modify, Clear, and Cancel** transactions. Only the raw hexadecimal strings reveal the machine-level data input required to prove the exact sequence of events, ensuring "Digital Non-Repudiation." This is the only way to verify whether a warrant was "metamorphosed" after the fact to justify an otherwise illegal arrest.

V. JURISDICTIONAL STEWARDSHIP AND THE DOCTRINE OF ADMINISTRATIVE ESTOPPEL

10. The RCMP is formally cautioned against the "Originator Control" defense. Physical possession and systemic administration satisfy the highest threshold for "control" under federal legislation (*National Defence*, 2011 SCC 25 at para 56).
11. **A. The Doctrine of Administrative Estoppel:** The RCMP has made formal representations to the Treasury Board of Canada and the Office of the Privacy Commissioner (OPC) that they maintain "full oversight" of CPIC to justify its existence as a centralized federal database. The institution cannot claim "Originator Control" (acting as a mere storage locker) to the user while simultaneously claiming "Supreme Stewardship" (acting as a regulator) to the OPC. You are equitably estopped from disclaiming "control" over records you have officially promised to audit and oversee for compliance. To allow such a defense would be to permit a "jurisdictional shell game" that defeats the very purpose of the *Privacy Act*.
12. **B. Breach of "Duty of Care" in Data Custodianship:** By hosting CPIC, the RCMP owes a quasi-fiduciary duty to the subjects of that data to ensure the system is not used for "Extra-Jurisdictional Arbitrage." When a federal institution becomes aware of a *prima facie* allegation of jurisdictional nullity (the "False Information Package"), their "Duty to Assist" under the *Privacy Act* is heightened. You are not a neutral bystander; you are the host of the vessel where the alleged forgery resides. The RCMP has an affirmative obligation to ensure that its systems are not being used as a platform for the dissemination of fraudulent judicial

authorizations.

VI. PROCEDURAL FRUSTRATION OF STATUTORY CORRECTION RIGHTS

13. Under Section 12(2) of the *Privacy Act*, I possess a statutory right to request a correction of my PI or a **Notation of Disagreement**. This is a critical mechanism for ensuring data integrity within federal systems.
14. If the RCMP withholds the metadata that proves the entry is fraudulent or extra-judicial, they are effectively immunizing the record from my Section 12(2) rights. Disclosure of the metadata is a **condition precedent** to the exercise of my statutory right to data integrity. You cannot correct a fraud you are prevented from seeing.
15. The withholding of these logs renders these powerful statutory remedies functionally illusory and directly violates the principles of fundamental justice under Section 7 of the *Charter*. The RCMP is essentially attempting to "privilege" the log data to protect the system from the very correction rights the Act was designed to provide. If the source data is corrupted or fraudulent, the right to "access" must include the right to see the forensic evidence of that corruption.

VII. GEOTEMPORAL PARAMETERS AND SYSTEMIC IDENTIFIERS

16. The relevant period for the CPIC Offline Search is **September 15, 2024, to December 31, 2024**, inclusive of all subsequent clearing or modification transactions. This window is not arbitrary; it is specifically designed to encompass the moments before, during, and after the suspect judicial entries were made.

Specific Identifiers:

- **TPS Occurrence Numbers:** 2024-2028093 & 24-2082035
 - **TPS Case ID:** 457197 (but this is likely the SCJ 361 University Avenue file number under an old RMS)
 - **Information Number:** 4810 998 24 48129169
 - **Arrest Date:** October 2, 2024 (TPS 14 Division)
17. This window is imperative to capture any **Modify Transactions** executed after the arrest to retroactively sanitize jurisdictional defects or "fix" warrant data that was initially entered without proper authorization. Any delay in providing this metadata directly engages the *Jordan* ceiling (March 23, 2026) and will be raised in the appropriate judicial forum as a state-sanctioned delay. The metadata is essential for a "Full Answer and Defence" in the concurrent criminal proceedings.

VIII. THE "DEEMED REFUSAL" AND PUBLIC INTEREST OVERRIDE

18. Pursuant to Section 8(2)(m) of the Act, a public interest override exists where disclosure

clearly outweighs any invasion of privacy. In this instance, there is no competing privacy interest—the data is about *me*. However, the public interest in exposing fraudulent judicial authorizations and the systemic manipulation of a national police database is a non-derogable democratic interest.

19. **Final Notice:** Unlike the *Access to Information Act*, the *Privacy Act* carries no application fees and no search/preparation fees. The RCMP cannot use "cost," "volume," or "complexity" as a reason to refuse. An "Offline Search" is a routine, automated process for the IT security branch and cannot, by definition, be an "unreasonable interference with operations."
20. I strongly suggest that the ATIP branch consult directly with the **Chief Information Officer (CIO)** of the RCMP or the **CPIC Field Operations Support Unit (National Police Services)**. Municipal partners like the TPS are "technologically fenced off" from the systemic audit logs you alone possess. Any failure to respond within the 30-day statutory window will be treated as a **"Deemed Refusal"**, resulting in an immediate application to the Federal Court under Section 41. I am prepared to skip the lengthy OPC complaint process where necessary to protect my *Charter* rights and ensure the preservation of these critical forensic records.

II. INTRODUCTION AND PROCEDURAL POSTURE

21. Correspondence is heretofore advanced in direct, comprehensive, and exhaustively detailed response to the communication promulgated by the Access to Information and Privacy Branch of the Royal Canadian Mounted Police, dated March 16, 2026. The present submission is meticulously calibrated to definitively satisfy the administrative prerequisites for clarification demanded by the institution. Concurrently, this instrument is intricately engineered to preemptively extinguish any preliminary, jurisdictional, or standing-based objections that might be improperly marshalled by the federal entity in a misguided attempt to obfuscate the strict statutory mandates unequivocally enshrined within the *Privacy Act*. It is forcefully posited that the administrative processing of this requisition must now proceed forthwith, entirely devoid of further prophylactic delays, manufactured ambiguity, or artificial bureaucratic impediments intended to deliberately exhaust the applicant and frustrate the pursuit of administrative justice.
22. The exaction of these highly specialized, immutable digital records is strictly necessitated to vindicate fundamental quasi-constitutional entitlements and to systematically expose potential administrative vitiations occurring under the colour of right. In circumstances where the structural integrity of a judicial authorization is ostensibly compromised through an *ex post facto* systemic manipulation—whether executed to clandestinely cure a fatal jurisdictional defect, to bridge an investigatory lacuna, or to retroactively sanitize an entirely unlawful physical apprehension—the rigorous extraction of unalterable digital metadata remains the sole, exclusive epistemological mechanism to restore the *status quo ante*. It is respectfully submitted that an unmitigated adherence to the overarching principles of *uberrima fides* (utmost good faith) is statutorily demanded of the federal repository, acting

- as the ultimate, supreme custodian of the nation's law enforcement ledgers.
23. The profound, inherent asymmetry of information existing between the coercive, deeply resourced apparatus of the state and the private citizenry dictates that the custodian must exercise its stewardship with absolute, unassailable transparency when formally compelled by statutory mechanisms. To permit the state to shield its digital machinations behind a veil of administrative silence is to invite tyranny by algorithm, whereby unreviewable databases operate as silent arbiters of liberty, entirely divorced from traditional judicial scrutiny.
 24. Applying the paramount quasi-constitutional doctrines established in *Dagg* and *Lavigne* to the present factual matrix dictates that the exaction of digital metadata is not a mere procedural courtesy, nor an administrative inconvenience to be lightly dismissed by departmental administrators; rather, it operates as a substantive jurisprudential bedrock designed to definitively rectify the purported deployment of vitiated judicial instruments.
 25. These instruments represent state *acta* which have facilitated a profound, potentially *ultra vires* deprivation of physical liberty, fundamentally offending the absolute protections against arbitrary detention enshrined within Section 9 of the *Charter*. Furthermore, the liberty and security of the person interests guaranteed under Section 7 of the *Charter* are directly engaged when the state relies upon a fundamentally flawed or fraudulently generated digital record to justify the ongoing subjection of an individual to the penal apparatus. The continued reliance upon such tainted *acta* offends the principles of fundamental justice, which demand that state deprivations of liberty be anchored to mathematically verifiable, procedurally sound, and authentically generated judicial authorizations.
 26. Furthermore, the absolute paramountcy of these access rights over institutional convenience, operational lethargy, or inter-agency diplomatic sensitivities dictates that the institution is legally precluded from weaponizing broad, generalized interpretations of law enforcement exemptions to shield administrative errors, extra-jurisdictional overreaches, or intentional systemic manipulations from rigorous public and judicial scrutiny. The rule of law immutably demands that the state's monopoly on the legitimate use of force be perpetually anchored to verifiable, authentic, and contemporaneously generated judicial authorization. A retrospective validation achieved through digital forgery is a profound corruption of the judicial process.
 27. It is further posited that a justice system operating upon the fragile, compromised foundation of fraudulent, retroactively generated, or technologically metamorphosed digital records is one that has entirely abandoned the rule of law in favour of systemic expediency and the preservation of institutional hegemony. The federal government, acting as the ultimate steward, architect, and host of the paramount law enforcement database, bears the non-delegable, unshakeable burden of ensuring this requisite transparency is continuously maintained. By strictly enforcing the provisions of the *Privacy Act*, the institution mitigates the profound democratic deficit inherent in clandestine digital repositories utilized to restrict fundamental liberties. Any institutional reticence, hesitation, or refusal to disclose the foundational audit trails is invariably interpreted by reviewing tribunals as a tacit admission of systemic irregularity and procedural impropriety. The deliberate obfuscation of metadata effectively operates as the spoliation of evidence, triggering devastating adverse inferences against the state in subsequent constitutional litigation.
 28. Anticipating a potential, albeit entirely unmeritorious, objection from the Presiding Divisional

Court President, the Crown Prosecutor, or opposing counsel that the present requisition constitutes an overly broad, vexatious, or impermissible "fishing expedition," such an assertion is preemptively neutralized and categorically dismantled. A "fishing expedition" is legally defined by its broad, speculative nature and an overarching absence of targeted evidentiary parameters, often deployed merely to harass administrative bodies with voluminous, undirected requests. Conversely, the strict parameters established within this requisition are microscopically focused, geographically constrained to a singular municipality, and temporally restricted to a mathematically precise algorithmic envelope spanning a mere fiscal quarter. The deliberate, surgical pursuit of highly specific hexadecimal and precise digital timestamps, which are tethered irrevocably to a singular, heavily documented deprivation of liberty, represents the very antithesis of a generic, undirected inquiry; it is a meticulous forensic extraction of the exact empirical evidence required to meticulously evaluate the true jurisdictional competence of the underlying warrant *ab initio*.

III. DELINEATION OF SCOPE, EXACTION OF METADATA, AND SYSTEMIC NON-REPUDIATION

29. Clarification is formally necessitated regarding the precise, highly technical scope of the requisition, ensuring absolutely no institutional misinterpretation limits the exhaustive production of responsive documents. It is unequivocally stated that the present inquiry does not seek a generic, superficial criminal record synopsis, nor does it request a standard, routine query of the active operator interfaces utilized daily by patrol officers. Such superficial, front-end inquiries would inherently and predictably omit historically executed, covertly modified, or intentionally purged [arrest warrant] (the "**Arrest Warrant**") records. Routine operational queries of the active [canadian police information centre] (the "**Canadian Police Information Centre**") interfaces routinely yield null results for executed or withdrawn instruments—an architectural design consciously intended to mitigate unlawful secondary arrests by field officers, rather than to perpetually obliterate the historical occurrence from the overarching institutional memory.
30. Rather than seeking active operational data, the demand is surgically directed toward the foundational, underlying administrative architecture of the database, specifically targeting the highly insulated, archival [offline historical database] (the "**Offline Historical Database**") associated directly with [personal information bank rcmp ppu 005] (the "**Personal Information Bank RCMP PPU 005**"). The complex architectural schematics of modern national policing systems rely heavily on sophisticated non-repudiation mechanisms, relational database integrity protocols, and comprehensive, immutable audit trails. These unalterable cryptographic mechanisms ensure that an executed warrant is never truly deleted from existence, preventing rogue operators from erasing historical facts through "soft deletions" or administrative overrides. Instead, the digital footprint is seamlessly migrated to a secure offline repository where its complete structural evolution, including every keystroke

of modification, remains permanently fossilized for rigorous auditing, judicial oversight, and strict institutional accountability purposes.

31. The critical documentation sought strictly comprises the entirely unredacted [transaction logs] (the "**Transaction Logs**"), comprehensive systemic audit trails, and raw hexadecimal dumps that irrevocably chronologize the entire systemic lifecycle of the specified entries. This exaction encompasses, without limitation, the precise date and temporal timestamps (accurate to the millisecond) of all [add transaction] (the "**Add Transaction**"), [modify transaction] (the "**Modify Transaction**"), [clear transaction] (the "**Clear Transaction**"), and [cancel transaction] (the "**Cancel Transaction**") executions orchestrated within the specified temporal window. The extraction of these precise event coordinates allows for the unassailable forensic reconstruction of the digital ledger, revealing exactly when the [arrest warrant] (the "**Arrest Warrant**") was birthed, when its parameters were potentially altered to reflect different jurisdictional realities, and when it was ultimately extinguished from the active purview of law enforcement.
32. A hexadecimal dump is explicitly necessitated because standard graphical user interfaces are frequently programmed to suppress, translate, or artificially sanitize backend anomalies to provide a cohesive visual experience for the terminal operator. By demanding the raw hexadecimal strings, the applicant bypasses the superficial, heavily curated interface, acquiring the unvarnished, machine-level data input that mathematically proves the exact sequence of events beyond any capability of administrative redaction, interpretative spin, or subsequent technological laundering. Only the foundational code can reveal the authentic chronology of the state's actions.
33. The absolute, non-derogable necessity of extracting these specific algorithmic artifacts is comprehensively corroborated by the critical, highly publicized findings articulated in the *Audit of Selected RCMP Operational Databases - Section 37 of the Privacy Act - 2011, Office of the Privacy Commissioner of Canada* (the "*OPC 2011 Audit*"). Within the scathing *OPC 2011 Audit*, the Commissioner explicitly admonished the Royal Canadian Mounted Police for consistently failing to adequately monitor systemic interactions and formally recommended the immediate, mandatory enablement of the [audit log viewer tool] (the "**Audit Log Viewer Tool**"). This specific utility was legally prescribed to consolidate, extract, and review complex audit trails to detect unauthorized access, surreptitious data manipulation, or the improper entry of extra-jurisdictional warrants by local detachments operating beyond their lawful mandate.
34. In its formal, documented reply to Parliament, the Royal Canadian Mounted Police explicitly committed to deploying and consistently utilizing this exact oversight methodology to ensure the integrity of the [canadian police information centre] (the "**Canadian Police Information Centre**"). Consequently, the institution is fundamentally estopped from feigning technological inability to extract the requested logs, as the preservation, collation, and robust review of these precise digital footprints constitute a formally adopted, externally mandated institutional policy designed precisely for the meticulous extraction requested herein. To deny the existence or retrievability of these logs would be tantamount to admitting an ongoing, systemic violation of the Commissioner's binding recommendations, thereby exposing the federal repository to severe parliamentary and judicial censure.
35. Furthermore, the exaction explicitly necessitates the full, unredacted disclosure of the

[issuing authority] (the "**Issuing Authority**") data field, the [originating agency identifier] (the "**Originating Agency Identifier**"), the unique user identification credentials of the terminal operators (specifically the alphanumeric CPIC login ciphers), and the entirety of the unstructured narrative and remarks fields appended to the entries. It is a technological certainty that the systemic architecture operates upon a bedrock foundation of absolute non-repudiation. By virtue of this design, any unauthorized structural metamorphosis of the judicial nomenclature, any retroactive upgrading of the jurisdictional court level to maliciously cure a procedural defect, or any post-execution alteration of the presiding jurist's identification is permanently preserved within these hidden audit trails. This architectural reality flawlessly maintains the distinct, unalterable "before" and "after" states of the altered algorithmic fields, allowing for definitive forensic comparison against the physical paper endorsements ostensibly relied upon by the Crown.

36. The extraction of the unstructured narrative and remarks fields is of paramount importance. These fields frequently contain the informal, unvarnished communications between dispatchers, warrant squads, and records management personnel. If a warrant was rejected by a local justice, subsequently shopped to a different jurisdiction, or electronically massaged to satisfy the criteria of the [canadian police information centre] (the "**Canadian Police Information Centre**"), the residual evidence of such administrative gymnastics is invariably captured within these free-text annotations. These narratives serve as the *res gestae* (the events, circumstances, and statements that are incidental to the main fact) of the digital transaction, providing the crucial contextual framework required to interpret the hexadecimal data and exposing the true *mens rea* (guilty mind) or administrative negligence of the state actors involved.
37. It is fully anticipated that the institution may subsequently assert, as a potential administrative counter-argument, that the deep extraction of deeply buried hexadecimal dumps or highly specialized transaction logs constitutes the "creation of a new record" or presents an "unreasonable administrative burden," thereby attempting to unlawfully refuse disclosure under standard procedural exemptions. This proposition is legally untenable, logically fractured, and fundamentally incorrect in law. The extraction of pre-existing database fields, compiled audit trails, and historical transactional metadata utilizing established algorithmic query parameters inherently native to the system does not, under any recognized legal or technological definition, equate to the creation of a new record. The systemic architecture inherently possesses the functionality to retrieve these historical logs; the mere requirement for specialized command syntax or an [offline search] (the "**Offline Search**") executed by high-level system administrators cannot be conflated with the unauthorized generation of novel documentation.
38. To baselessly assert that an [offline search] (the "**Offline Search**") represents an undue operational burden is to effectively immunize the vast majority of the national database's historical actions from any statutory oversight whatsoever. Such an outcome is entirely incompatible with the legislative intent of the *Privacy Act* and is fundamentally abhorrent to the transparent principles of a functioning democracy. The statutory obligation explicitly requires the institution to render the information reasonably retrievable; where the institution itself engineered the complex, multi-tiered architecture that strictly necessitates an [offline search] (the "**Offline Search**") to view historical data, it cannot thereafter selectively leverage

its own self-imposed architectural complexity as an impenetrable shield against democratic transparency and lawful requisition. The burden of technological navigation falls squarely and irrevocably upon the custodian. The state cannot build an opaque digital labyrinth and then subsequently complain that it is too arduous to navigate when a citizen lawfully demands the retrieval of their personal data.

IV. JURISDICTIONAL STEWARDSHIP AND THE ABROGATION OF THE ORIGINATOR CONTROL DEFENSE

39. Attention is strictly, forcefully, and preemptively directed to the anticipated institutional assertion that the *Privacy Act* does not authorize the Royal Canadian Mounted Police to search or disclose files purportedly "belonging" to other municipal or provincial police forces. This proposition is formally repudiated as a profound, inexcusable misapprehension of established administrative law and a blatant disregard for binding privacy jurisprudence. The continued institutional reliance upon the inter-agency doctrine of originator control to circumvent federal statutory disclosure obligations constitutes a profound legal fallacy that inherently offends the quasi-constitutional imperatives of the *Privacy Act*. Inter-agency memorandums of understanding, internal operational manuals, and localized data-sharing agreements are subordinate administrative constructs that do not, and categorically cannot, supersede Acts of Parliament or abrogate fundamental constitutional rights.
40. It is a well-established, insurmountable legal syllogism that physical possession, ongoing systemic administration, and fundamental structural integration perfectly satisfy the absolute highest threshold for establishing "control" under federal access legislation. Reliance is unequivocally placed upon the binding jurisprudence meticulously articulated in *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25 (the "*National Defence*") at para 56. In *National Defence*, the Supreme Court of Canada affirmed a rigorous, comprehensive bipartite test for determining "control." The Court definitively established that records residing within a federal institution's systemic architecture—over which the institution possesses physical custody of the servers, and over which a reasonable expectation of systemic governance, auditing, and high-level oversight applies—are legally under its absolute control. This control is established entirely irrespective of the records' original municipal or provincial authorship. To hold otherwise would allow the federal government to construct unreviewable black boxes populated by third-party data, thereby eviscerating the entire statutory regime of public accountability.
41. Applied strictly and without deviation to the present circumstances, the Royal Canadian Mounted Police, functioning as the paramount architect, proprietor, and supreme administrator of the national database, exercises absolute physical and administrative custody over the mainframe servers and their constituent data packets. The federal institution sets the algorithmic parameters, controls the telecommunications bandwidth, dictates the stringent security protocols, and uniquely manages the archival lifecycle of the data from genesis to deletion. Therefore, it cannot disavow the contents of its own digital

ledger, nor can it impermissibly outsource its strict statutory obligations to the myriad of constituent municipalities currently utilizing its highly sophisticated infrastructure. The federal government is not a mere passive conduit, an inert bulletin board, or a disinterested telecommunications provider; it is the ultimate publisher, arbiter, and sovereign custodian of the repository.

42. Furthermore, the Office of the Privacy Commissioner of Canada has definitively foreclosed this precise institutional defense in circumstances directly involving the [toronto police service] (the "**Toronto Police Service**"), establishing an insurmountable precedent regarding ultimate federal accountability. In the authoritative *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC, Special Investigation Report, April 14, 2014* (the "*OPC 2014 Suicide Investigation*"), the Commissioner exhaustively investigated the unauthorized, deeply prejudicial disclosure of highly sensitive personal information originally authored and entered by the [toronto police service] (the "**Toronto Police Service**").
43. In the *OPC 2014 Suicide Investigation*, the Royal Canadian Mounted Police attempted to deploy the exact originator control defense anticipated herein, aggressively arguing that it was merely hosting data owned by municipal entities and therefore bore no statutory responsibility for its dissemination or review. The Commissioner explicitly rejected this premise *in toto*, establishing unequivocally that the Royal Canadian Mounted Police, acting in its capacity as the paramount steward and the sole sovereign signatory to international data-sharing agreements (such as the [memorandum of cooperation] (the "**Memorandum Of Cooperation**") with the Federal Bureau of Investigation), bears the ultimate, non-delegable responsibility for ensuring that all information hosted across the network complies strictly with federal statutes. The federal hosting institution was found substantively and directly accountable for the widespread dissemination of the municipal data and was subsequently compelled by the Commissioner to overhaul its default sharing protocols entirely. Thus, the institution is functionally and legally prohibited from relying upon inter-agency originator control principles to evade accountability for the data permanently disseminated through its proprietary infrastructure. The jurisprudence dictates an immutable reality: he who controls the network, controls the data, and bears the statutory burden of disclosure.

SUB-SECTION A: The Recency of Jurisprudential Mandates and the Evidentiary Void of the False Information Package

44. To definitively extinguish any residual assertion that this requisition ought to be administratively deflected or redirected to a local municipal agency, reliance is emphatically placed upon the highly recent, and strictly binding, adjudicative findings articulated by Adjudicator Steven Faughnan in *Order MO-4542, Halton Regional Police Services Board*,

2024 *CanLII 62738 (ON IPC)* (the "*Order MO-4542*"). Promulgated as recently as July 8, 2024, this pivotal jurisprudential authority operates overwhelmingly and unequivocally in favour of the applicant. It serves to permanently foreclose any administrative inclination by the federal repository to improperly deflect the present requisition back to a provincial or municipal constabulary, legally paralyzing the institution's ability to evade its statutory burden.

45. In *Order MO-4542*, the appellant formally sought records revealing inquiries made about him by *all* police services across Canada navigating various law enforcement databases. The provincial tribunal definitively ruled that a localized municipal police service (in that instance, the Halton Regional Police Services Board) absolutely lacks the requisite physical custody, statutory authority, and systemic control to conduct such expansive offline searches capable of revealing the overarching systemic footprint of other law enforcement agencies. The tribunal explicitly recognized that localized municipal entities are technologically restrained and severely restricted by strict use protocols from querying the centralized federal historical repositories to ascertain what external agencies have done. A municipal force simply cannot execute a cross-jurisdictional audit to ascertain which external agencies accessed, modified, or appended data to a specific file traversing the national infrastructure; they are strictly limited to viewing the superficial outputs authorized by the federal gatekeeper.
46. Consequently, *Order MO-4542* establishes an unassailable legal syllogism that heavily favours the present requisition: because municipal agencies are administratively prohibited and technologically barred from executing the necessary exaction of deep offline metadata encompassing multiple jurisdictions, the Royal Canadian Mounted Police remains the sole, exclusive, and unassailable entity possessing both the overarching legal jurisdiction and the centralized technological capability to fulfill this statutory requisition. The centralized [personal information bank rcmp ppu 005] (the "**Personal Information Bank RCMP PPU 005**") is the exclusive, paramount repository capturing the unalterable digital footprints of all constituent agencies interacting with the national mainframe. The federal host is the only entity with the omniscient technological vantage point necessary to retrieve the requested transaction logs, rendering any attempted redirection by the RCMP an exercise in egregious administrative negligence and actionable bad faith.
47. Furthermore, the absolute necessity of directing this exaction exclusively to the federal steward is irrefutably compounded and rendered entirely self-evident by the fraudulent nature of the underlying documentation utilized to justify the deprivation of liberty. It is formally submitted that the [false information package] (the "**False Information Package**") currently in circulation is a documented fabrication, intrinsically devoid of factual accuracy, procedural regularity, or jurisdictional reliability. *Ipso facto*, because the aforementioned instrument is fundamentally vitiated and its provenance intentionally obscured by state actors, it constitutes an absolute epistemological impossibility for the applicant to ascertain precisely which specific municipal or provincial constabulary maliciously or erroneously transmitted the *acta* into the federal database.
48. Due to the inherent unreliability, deliberate obfuscation, and contested nature of the [false information package] (the "**False Information Package**"), the true originating entity remains entirely concealed. The fraudulent entry could theoretically have been initiated by the [toronto police service] (the "**Toronto Police Service**"), the [peel regional police] (the "**Peel Regional**

Police"), the [ontario provincial police] (the "**Ontario Provincial Police**"), or any other unidentified law enforcement apparatus operating within the province. If an obligation were improperly imposed upon the applicant to direct localized access requests to individual municipal agencies based upon a demonstrably fraudulent document, such an endeavour would constitute an exercise in profound, Kafkaesque bureaucratic futility. The citizen would be forced to navigate a labyrinth of endless denials, haphazardly guessing the culprit, while each respective agency plausibly claims ignorance of the forged document and disavows any involvement.

49. The deliberately constructed jurisdictional ambiguity engineered within the [false information package] (the "**False Information Package**") is designed specifically to obfuscate the true originating agency and shield the perpetrators from legal, civil, and administrative accountability. Therefore, the Royal Canadian Mounted Police, acting as the supreme custodian of the [offline historical database] (the "**Offline Historical Database**") under the strict auspices of the [personal information bank rcmp ppu 005] (the "**Personal Information Bank RCMP PPU 005**"), is the singular, indispensable institution capable of bypassing this localized subterfuge. Only the centralized federal repository possesses the technological capability to definitively expose the unvarnished digital truth via the extraction of the unforgeable [originating agency identifier] (the "**Originating Agency Identifier**"). By extracting this unalterable cryptographic signature, the RCMP can irrefutably identify the true authors of the vitiated *acta*, pierce the veil of inter-agency obfuscation, and unequivocally restore the *status quo ante*.

V. GEOGRAPHICAL NEXUS, SYSTEMIC TERMINAL IDENTIFICATION, AND JURISDICTIONAL NULLITY

50. In direct, meticulous satisfaction of the institutional request for precise geographical particularization, it is explicitly confirmed that the originating locus of the underlying investigation, the purported locus of the alleged offense, and the presumed terminal origin of the initial systemic entry is localized entirely within the specific territorial boundaries of Toronto, Ontario.
51. The forensic extraction must specifically correlate with the [toronto police service] (the "**Toronto Police Service**"), predominantly focusing upon the 52nd Division as the presumed originating agency responsible for the investigative genesis, and the 14th Division as the geographic venue of the ultimate physical deprivation of liberty. This highly unusual, seemingly disjointed administrative bifurcation of the investigation into dual occurrences across separate, geographically distinct divisions necessitates a highly precise temporal mapping of all judicial authorizations applied within the local municipal infrastructure.
52. Such fragmentation of the operational record is frequently indicative of profound procedural anomalies, suggesting deliberate strategic maneuvers by field officers intended to bypass the continuous, localized scrutiny of a single judicial oversight officer, thereby engaging in a form of impermissible jurisdictional arbitrage. When a warrant is sought in one division but executed under the auspices of another, or when an investigation is fractured across multiple event numbers to obscure the evidentiary chain, the digital audit trails operate as the sole unifying thread capable of exposing irregular procurement practices, effectively laying bare

the *actus reus* of systemic manipulation.

53. The exact systemic identifiers required to flawlessly triangulate the administrative entries are formally established as Toronto Police Service occurrence number 2024-2028093, Toronto Police Service occurrence number 24-2082035, and the centralized archival indexing cipher documented as [police case identification number] (the "**Police Case Identification Number**") 457197. These highly specific alphanumeric ciphers provide the exact algorithmic coordinates required to immediately isolate the relevant data packets within the vast national mainframe, thereby completely eliminating any institutional pretense of ambiguity, search impossibility, or resource strain.
54. It is further submitted that the extraction of the [originating agency identifier] (the "**Originating Agency Identifier**") operates as an unforgeable cryptographic signature for every individual transaction executed within the database. The presence of this specific identifier irrevocably traces the exact physical terminal, the originating IP address, the precise user credentials, and the exact temporal data input back to a specific law enforcement division and physical location. This technological reality absolutely prevents any local agency from plausibly disclaiming responsibility for a fraudulent, extra-jurisdictional, or technologically corrupted entry. The systematic triangulation of these systemic ciphers against the physical court registries constitutes the exclusive, unimpeachable methodology for verifying the *prima facie* legitimacy of the underlying authorization.
55. A robust, insurmountable counter-argument must be preemptively advanced against the potential assertion by state actors that a geographical discrepancy in the issuance of a warrant is a mere, easily curable administrative defect under the *Criminal Code, RSC 1985, c C-46* (the "*Criminal Code*"). A non-originating judicial officer (for illustrative purposes, a Justice of the Peace sitting in the jurisdiction of Brampton) possesses absolutely zero inherent jurisdiction to arbitrarily issue a warrant for a completely unconnected territorial jurisdiction (such as Toronto) absent strict, demonstrable, and explicitly documented statutory compliance delineated within the specific backing provisions of the *Criminal Code* (e.g., Section 529 regarding telewarrants or the highly restrictive execution of warrants across territorial divisions).
56. Any appearance before a judicial officer lacking such explicit territorial authority is strictly *coram non iudice* (not before a judge). The foundational proceedings are utterly vitiated, entirely lacking any legal substrate. The fundamental, unyielding common law maxim *nemo dat quod non habet* (no one gives what they do not have) dictates with absolute, mathematically precise certainty that a judicial officer cannot confer lawful authority over a geographic jurisdiction to which they are not statutorily, formally, or temporally assigned by the Chief Justice of the respective court. To assert otherwise is to endorse a regime of roving, borderless judicial commissions explicitly rejected by the architecture of Canadian federalism and provincial judicial administration, thereby inviting profound constitutional chaos.
57. Therefore, if the extracted [originating agency identifier] (the "**Originating Agency Identifier**") reveals that the initial systemic entry emanated from a jurisdiction wholly disconnected from the documented [issuing authority] (the "**Issuing Authority**"), or if the court designation was retroactively, inexplicably upgraded from the Ontario Court of Justice to the Superior Court of Justice without a corresponding, authenticated judicial endorsement on the physical information, the process is an absolute, irredeemable nullity *ab initio*. The

warrant is entirely void, and the subsequent arrest is rendered unequivocally unlawful, constituting an actionable tort of false imprisonment and an egregious, flagrant breach of the *Charter*. The deliberate suppression of such exculpatory metadata by the federal repository is tantamount to the active concealment of an unlawful arrest, a profound breach of institutional trust, and a catastrophic violation of the principles of fundamental justice.

VI. TEMPORAL PARAMETERS, THE FORENSIC WINDOW, AND THE PREJUDICE OF DELAY

58. In meticulous fulfillment of the requirement for a definitive temporal framework to explicitly guide the offline exaction, the [forensic window] (the "**Forensic Window**") is strictly circumscribed to the specific period commencing on September 15, 2024, and definitively terminating on December 31, 2024.
59. The genesis date of September 15, 2024, correlates precisely with the formal establishment of the primary investigatory occurrence within the municipal dispatch framework. The deliberate, highly calculated expansion of the terminal date to December 31, 2024, is legally, strategically, and forensically imperative. This extended, post-arrest parameter is explicitly formulated to rigorously capture any covert systemic [modify transaction] (the "**Modify Transaction**") or [cancel transaction] (the "**Cancel Transaction**") executed long after the physical apprehension was formally concluded.
60. It is vehemently posited that if an act of *ultra vires* judicial authorization was retroactively sanitized by system operators to conceal jurisdictional defects, the resulting [documentary metamorphosis] (the "**Documentary Metamorphosis**") would have necessarily transpired during the weeks immediately following the effectuation of the physical arrest on October 2, 2024. This extended temporal window represents the precise period wherein institutional actors desperately sought to reconcile the disparate, unsworn physical paperwork with the unalterable digital ledger, frequently necessitating illicit electronic alterations to force the system to accept an otherwise deficient, structurally flawed warrant.
61. The extreme urgency of this temporal extraction is drastically exacerbated by the rigid constitutional strictures delineated in the landmark decision *R v Jordan*, 2016 SCC 27 (the "*Jordan*"). In *Jordan*, the Supreme Court of Canada established a presumptive, inflexible, and mathematically precise ceiling of 18 months for the completion of trials prosecuted by summary conviction. Applied strictly to the present commencement date of September 23, 2024, the absolute terminal date for the vindication of the right to a trial within a reasonable time is irrevocably fixed at March 23, 2026.
62. Any administrative delay precipitated by the federal institution's failure to provide unvarnished, timely access to the forensic metadata constitutes a direct, highly prejudicial impediment to the fundamental ability of the accused to make full answer and defence, explicitly protected under Section 11(a) and 11(d) of the *Charter*. The state is strictly prohibited from utilizing its own technological obfuscation, bureaucratic lethargy, and artificially compartmentalized administration to deliberately exhaust the *Jordan* ceiling.

Opposing counsel may attempt to baselessly argue that the provincial Crown bears no responsibility for the administrative delays of an ostensibly independent federal body regarding a parallel *Privacy Act* request.

63. This argument is fatally flawed, legally bankrupt, and universally rejected by sophisticated appellate courts. The delay operates as a unified, systemic deprivation of rights, extending the prosecutorial shadow over the citizenry while the state apparatus simultaneously withholds the very exculpatory evidence of jurisdictional nullity. The Supreme Court has repeatedly affirmed that the various branches of the state cannot point fingers at one another to excuse the deprivation of constitutional rights; thus, rendering the delay entirely and indisputably attributable to the unified state apparatus. The Crown's continuous failure to compel the Royal Canadian Mounted Police to release exculpatory metadata represents a fatal flaw in the prosecutorial timeline, directly contributing to the exhaustion of the *Jordan* calculus.
64. Concomitantly, the Crown possesses an unremitting, ongoing, and absolute obligation to disclose all relevant information, as definitively established in *R v Stinchcombe*, [1991] 3 SCR 326 (the "*Stinchcombe*"). While the Royal Canadian Mounted Police may superficially assert that it operates completely independently of the prosecuting provincial Crown, the sophisticated jurisprudence articulated in *R v McNeil*, 2009 SCC 3 (the "*McNeil*") conclusively establishes that records held by any police forces—including federal databases—that are relevant to the underlying validity of the state's case must be proactively accessible to prevent gross miscarriages of justice. The artificial boundaries between "first-party" and "third-party" records are completely dissolved when the federal database holds the very foundational *acta* that authorized the provincial prosecution in the first instance.
65. The systemic audit logs definitively proving the true jurisdictional origin of the warrant are undeniably relevant first-party records under the combined *Stinchcombe* and *McNeil* frameworks. The unquestionable integrity of the judicial authorization is the *sine qua non* (the essential, indispensable condition) of the entire prosecution. This undeniable reality elevates this *Privacy Act* requisition far beyond a mere administrative entitlement, transforming it into a fundamental, constitutionally protected component of trial fairness that must be executed with maximal expediency to prevent the ultimate, inevitable collapse of the prosecution due to systemic non-disclosure.

VII. THE PERSONAL INFORMATION IS ABOUT ME BUT FOR SAKE OF ARGUMENT — PUBLIC INTEREST OVERRIDES

66. Pursuant to the strict strictures delineated within Section 8(1) of the *Privacy Act*, personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with highly specific statutory provisions. It is formally declared, unequivocally established, and

- permanently entered into the administrative record that the applicant is the exclusive subject of the requested digital *acta*. Concomitantly, absolute, unreserved, and explicit consent is hereby provided for the comprehensive, unredacted disclosure of any and all metadata, transaction logs, and systemic entries pertaining to the applicant. The primary statutory barrier to disclosure, theoretically predicated upon the protection of the subject's privacy, is thus entirely and permanently extinguished *in limine* by the subject's own proactive volition.
67. Assuming, *arguendo* (for the sake of argument), that the federal institution attempts to manufacture a convoluted administrative pretext to withhold the requested digital artifacts despite the provision of absolute consent—perhaps by fallaciously asserting the inextricable entanglement of peripheral institutional methodologies or unspecified third-party identifiers—such an obstructionist posture is immediately vitiated by the paramount public interest override provisions enshrined within the statute.
68. Specifically, Section 8(2)(m) of the *Privacy Act* functions as a formidable public interest override, explicitly granting the head of a government institution the statutory discretion—and, in circumstances characterized by profound state overreach, the overriding administrative mandate—to disclose personal information even in the complete absence of standard consent protocols. The statute dictates that disclosure is legally permissible and administratively justified if:
- a. Under Section 8(2)(m)(i), the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or
 - b. Under Section 8(2)(m)(ii), disclosure would clearly benefit the individual to whom the information relates.
69. Regarding the application of Section 8(2)(m)(i), it is vehemently posited that the overarching public interest in exposing fraudulent judicial authorizations, *ultra vires* law enforcement actions, and the systemic manipulation of the national police database astronomically outweighs any theoretical, manufactured invasion of privacy. A functioning democracy is fundamentally reliant upon the absolute, unimpeachable integrity of its criminal justice infrastructure. The exposure of the fabricated [false information package] (the "**False Information Package**") and the conclusive identification of the state actors responsible for its systemic promulgation serve a compelling, non-derogable democratic interest. The public possesses a paramount, unassailable right to be assured that the [canadian police information centre] (the "**Canadian Police Information Centre**") is not being utilized as a clandestine repository for forged warrants designed to facilitate unlawful deprivations of liberty.
70. Concurrently, regarding the application of Section 8(2)(m)(ii), it is an incontrovertible legal reality that the comprehensive disclosure of the requested forensic metadata would clearly, directly, and profoundly benefit the individual to whom the information relates. The extracted hexadecimal dumps and unalterable audit trails provide the exact exculpatory evidence mathematically required to definitively quash an unlawful arrest, dismantle a fraudulently constructed prosecution, and forcefully vindicate the applicant's fundamental rights guaranteed under the *Charter*. Conversely, the continued withholding of this information by the federal steward actively perpetuates a profound, ongoing prejudice against the individual, effectively compounding the original constitutional violation by denying the citizen the very tools necessary for legal exculpation. Therefore, even if the primary mechanism of explicit

consent were administratively disregarded, the public interest override strictly mandates the immediate, unredacted release of the requested records.

VIII. ANTICIPATORY REBUTTAL OF STATUTORY EXEMPTIONS AND CONCLUSION

71. Anticipating potential institutional reliance upon the highly discretionary law enforcement exemptions delineated under Section 22(1)(b) of the *Privacy Act*, it is preemptively asserted that any such application would be legally untenable, demonstrably unreasonable, and a glaring manifestation of extreme institutional bad faith. It is highly probable that it may be counter-argued by the institution's legal counsel or policy analysts that the unredacted release of systemic audit logs could theoretically reveal confidential investigative techniques, expose ongoing operational strategies, or generally jeopardize the overarching security and efficacy of the national database itself.
72. This proposition is fundamentally flawed, structurally illogical, and entirely inapplicable to the highly specific facts at bar. The underlying operational phase of the law enforcement engagement is irrevocably concluded. The judicial authorization has been physically executed, the subject has been processed through the municipal intake system, and the systemic alert has been explicitly cleared from the active interface. The systemic records currently sought do not encompass prospective investigatory techniques, the deeply protected identities of confidential informants, covert surveillance protocols, or sensitive tactical intelligence. Rather, they constitute entirely historical, administrative *acta* definitively proving the foundational jurisdictional validity (or nullity) of a finalized, crystallized, and historically completed state action. Typing a warrant into a database is a purely administrative clerical function, not a privileged investigative technique shielded from public scrutiny.
73. The absolute, non-derogable necessity of accessing these records is further codified by the foundational principles articulated in *R v Garofoli*, [1990] 2 SCR 1421 (the "*Garofoli*"). In *Garofoli*, the Supreme Court established the absolute, unimpeachable right of an accused to challenge the underlying validity and factual foundation of a judicial authorization (the constitutionally protected right to "go behind" the warrant). This fundamental, universally recognized right is rendered functionally illusory and entirely meaningless if the immutable digital metadata proving its invalidity is systematically withheld by the executive branch under the spurious, overly broad guise of "investigative privilege."
74. The invocation of such discretionary exemptions to conceal *prima facie* procedural anomalies, to mask the true identity of an authorizing justice, or to shield potential institutional *fraus omnia corrumpit* (fraud unravels all) from public and judicial scrutiny, constitutes a gross abuse of administrative discretion that fundamentally offends the *lex terrae* (the law of the land). A free and democratic society cannot abide the deployment of secret digital ledgers to validate deprivations of liberty, mirroring the clandestine, unaccountable operations of a star chamber.

75. Furthermore, reliance is firmly placed upon the strict doctrine of *functus officio* as articulated in *Chandler v Alberta Association of Architects*, [1989] 2 SCR 848 (the "*Chandler*"). The *Chandler* jurisprudence affirms that once a judicial or administrative officer has finally decided a matter and formally issued their order, their jurisdiction over that specific matter is entirely exhausted, spent, and permanently extinguished. Consequently, the issuing judicial officer became entirely *functus officio* at the exact moment the warrant was promulgated and subsequently executed by the arresting officers.
76. The authorization itself simultaneously crystallized into an unalterable administrative, historical record. The statutory shield of investigative privilege cannot be conceptually retrofitted, legally contorted, or practically expanded to conceal jurisdictional overreaches or the subsequent *ex post facto* generation of documents explicitly designed to sanitize a vitiated apprehension. Once a warrant is executed, the "investigation" pertaining to the acquisition of that specific warrant is permanently concluded; the state cannot continuously claim ongoing privilege over historical facts to avoid constitutional accountability.
77. A further, highly predictable institutional counter-argument may assert that the Royal Canadian Mounted Police, functioning merely as an inert host or passive repository, cannot alter, correct, or append data to records inherently "owned" by another municipal agency. This assertion is categorically dismantled by the explicit, non-delegable remedial provisions contained within the *Privacy Act*. The statute encompasses powerful, non-discretionary mechanisms designed specifically to cure the retention of vitiated, inaccurate documentation within federal repositories, entirely regardless of its original municipal source.
78. Should the requested audit trails substantiate the presence of fundamentally inaccurate information—such as a falsified court location, an altered judicial endorsement, or an entry entirely lacking jurisdictional competence—the statutory right to demand an immediate correction, or alternatively, the mandatory application of a [notation of disagreement] (the "**Notation Of Disagreement**") under Section 12(2) of the *Privacy Act*, shall be immediately, forcefully, and unequivocally exercised by the applicant.
79. Pursuant to the strict mandates of Section 12(2)(c), the institution is legally obligated to actively notify any person, body, or government institution to whom the fraudulent information was disclosed within the preceding two years, formally appending the [notation of disagreement] (the "**Notation Of Disagreement**") to every subsequent dissemination. The withholding of the underlying audit trails renders these powerful statutory remedies functionally illusory, insulates the state from systemic accountability, and directly violates the fundamental principles of fundamental justice protected by Section 7 of the *Charter*.
80. The Royal Canadian Mounted Police, functioning as the supreme system administrator, is uniquely positioned and statutorily compelled to execute this notation upon the centralized mainframe, entirely irrespective of the initial authoring agency's preferences, objections, or internal politics. Ignorance of this overarching federal obligation is absolutely no defense (*ignorantia juris non excusat*). The federal repository cannot become a sanctuary for locally manufactured fraudulent documents without explicitly implicating the federal government in the continued propagation of the fraud.
81. The preservation of the unvarnished digital truth is the paramount objective of this requisition.
82. The individual is optimally positioned and fully prepared to file a formal, expedited complaint with the Office of the Privacy Commissioner of Canada, explicitly invoking the investigatory

powers utilized in the *OPC 2011 Audit* and the *OPC 2014 Suicide Investigation*.

83. As the requisite administrative clarifications demanded on March 16, 2026, have been exhaustively, meticulously, and formally satisfied *in limine*, the Royal Canadian Mounted Police is legally bound to immediately recommence the active processing of this requisition without further prevarication.
84. Trusting that this cannot take more than an hour to provide the requested personal information, kindly provide it to me and I can review the same, and then confirm that the request is closed.
85. Thank you kindly.

All of which is respectfully submitted.



Mr. Kevin A. McLean (BA, JD, CIM)

Enclosures:

1. Demonstration of overt fraud by whomever manipulated the Information Package into the FIP when measured against an Information Package from the

APPENDIX: Juridical Analysis: Implications of Order MO-4542 for Requisitions under the Privacy Act

I. Executive Overview of Order MO-4542

In the significant matter of *Halton Regional Police Services Board (Re)*, 2024 CanLII 62738 (ON IPC), the Adjudicator deliberated upon the transparency requirements inherent to national law enforcement databases, specifically focusing on the intersection of local administrative boundaries and centralized federal data repositories. The proceedings originated from a request for the disclosure of records detailing all inquiries pertaining to a specific individual conducted by any police service within the Canadian jurisdiction across the **CPIC**, **PARAS**, and **NCIC** systems.

A definitive jurisdictional boundary was established by the Adjudicator, predicated upon a distinction between two discrete categories of digital artifacts, which serves as a foundational precedent for understanding data ownership in a networked law enforcement environment:

1. **Local Access Records:** These comprise the granular data generated as a direct consequence of queries initiated by officers of a specific regional constabulary. Such

records, reflecting the internal operations and specific investigative choices of that force, are deemed to reside within the "custody and control" of the respective local board.

2. **Systemic Audit Logs (The "Offline" Repositories):** These are the centralized and exhaustive transaction logs encompassing all queries executed by any constituent agency within the national technological architecture. Crucially, it was determined that local boards do **not** possess custody or control over these systemic logs. The Adjudicator reasoned that a municipal force lacks the unilateral authority to audit the activities of external agencies within the mainframe environment managed exclusively by the Royal Canadian Mounted Police (RCMP). This finding effectively designates the RCMP as the sole authority capable of accessing the "omniscient" view of the system's transaction history.

II. Strategic Advantages for the Requisitioning Party

Order MO-4542 provides significant jurisprudential support for the current requisition, offering the necessary legal framework to necessitate compliance from the federal institution by removing the possibility of administrative buck-passing.

1. The Preclusion of Procedural Deflection via the Originator Control Principle

The Royal Canadian Mounted Police frequently invokes the "Originator Control" principle to redirect *Privacy Act* requisitions to municipal entities, arguing that the agency that first entered the data retains ownership of the record. Order MO-4542 serves to invalidate the applicability of this defense in the specific context of systemic metadata. Adjudicator Faughnan clarified that a municipal police board remains legally and technologically incapable of providing a cross-jurisdictional audit trail, regardless of its role as an "originator" of individual data entries.

Consequently, the citing of this precedent establishes that the RCMP is not merely a passive host or a digital "landlord" but the **sole legal custodian** of the systemic metadata. Should the RCMP decline the production of these records, the information would be rendered a "legal nullity"—unobtainable from any source across the municipal, provincial, or federal levels. Such a result would stand in direct contravention of the quasi-constitutional status afforded to the *Privacy Act* by the Supreme Court of Canada, which mandates that the Act be interpreted in a manner that favors the right of access. This compels the acknowledgement that the duty of disclosure rests exclusively with the managers of the CPIC infrastructure, as they alone hold the keys to the "master log" that local boards are legally barred from accessing.

2. Validation of Technological Feasibility and Extant Record Status

Institutional claims asserting that the production of forensic metadata or transaction logs necessitates the "creation of a new record" are frequently utilized to circumvent statutory obligations under Section 4 of the *Privacy Act*. However, Order MO-4542 explicitly addresses the **"off-line search"** protocol as a known and established procedure within the RCMP's operational toolkit.

The Adjudicator observed that such searches constitute a standard, albeit specialized, function of the database management system used to track historical interactions that are no longer "live" on the front-end interface. This provides a robust precedent: the "Offline Historical Database" is recognized as an extant repository of records, not a hypothetical construct. Reference to this order demonstrates that the requisition pertains to the retrieval of existing data through established forensic protocols rather than the creation of novel information or the programming of new software. The focus is thereby shifted from a debate over technical capability to a direct assessment of statutory obligation. Furthermore, it implies that a refusal to perform such a search constitutes a failure to conduct a "reasonable search" as required by law.

3. Verification of Necessity and Exhaustion of Administrative Remedies

The invocation of MO-4542 serves to demonstrate that the applicant has exercised profound due diligence in the pursuit of administrative remedies. It illustrates that the requisition of such metadata from regional boards, such as the Toronto Police Service, would constitute a futile exercise in administrative circularity. Since the IPC has affirmed that these regional boards lack the requisite jurisdiction and technical interface to facilitate cross-agency audits, the applicant is justified in proceeding directly against the federal administrator.

This "exhaustion of remedies" argument is paramount in precluding the institution from employing administrative redirection as a method of procedural delay. It forces the RCMP to confront the reality that they are the "court of last resort" for this specific category of information. By presenting MO-4542, the applicant effectively closes the loop on any argument that the request is "premature" or directed at the "wrong authority."

III. Legal Implications and Systemic Consequences

The Doctrine of the "Omniscient Vantage Point"

Order MO-4542 affirms a critical power imbalance: while local police services are restricted to viewing their own internal activity, the RCMP maintains an "omniscient technological vantage point" over the entire Canadian law enforcement landscape. In instances where "Documentary Metamorphosis"—the unauthorized or fraudulent alteration of judicial data such as warrants or occurrence reports—is suspected, these systemic logs represent the singular medium through which the truth may be observed.

Specifically, the "Offline" logs capture the **unaltered [Originating Agency Identifier]** and the timestamp of every modification. Absent the disclosure of these logs, the integrity of the judicial process is compromised. Local logs are susceptible to internal manipulation or may only represent a fragmented, "polished" portion of the transaction history. The systemic logs, held by the RCMP, act as an unalterable "black box" recorder for the justice system, and Order MO-4542 establishes the precedent that access to this black box is a matter of law, not institutional discretion.

Non-Delegable Stewardship of the Sovereign Custodian

The decision reinforces the status of the RCMP as the "Sovereign Custodian" of national security

and law enforcement data. A refusal by the federal institution to disclose such data, especially when coupled with the proven inability of local agencies to provide it, would result in the creation of an impermissible "dark zone" within Canadian privacy law. In this dark zone, personal data could be queried, modified, and shared by thousands of officers without any possibility of oversight or correction by the individual concerned.

Order MO-4542 facilitates the argument that the *Privacy Act* was enacted specifically to provide transparency within these complex, multi-jurisdictional digital environments. It suggests that as systems become more centralized and "intelligent," the duty of the central administrator to provide transparency increases proportionally. Consequently, a refusal to initiate an offline search when "Documentary Metamorphosis" is at issue is not merely a procedural denial but a direct infringement upon the statutory rights of the individual to ensure the accuracy and lawful use of their personal information.

IV. Formal Jurisprudential Conclusion

- **The Precedent of Limitation:** Order MO-4542 confirms that municipal police entities are both technologically and legally precluded from fulfilling cross-jurisdictional audit requisitions, thereby identifying the "dead end" of local inquiries.
- **The Mandate of the Central Repository:** The Royal Canadian Mounted Police, as the exclusive administrator of CPIC PPU 005, constitutes the only entity possessing the physical and legal "custody and control" of the **unvarnished digital truth** regarding systemic database interactions.
- **The Non-Delegable Requirement:** The institution is legally barred from redirecting this requisition to municipal partners, as such redirection would be a known path to failure. It is incumbent upon the RCMP to initiate the "offline search" protocol immediately to satisfy its non-delegable statutory obligations pursuant to the *Privacy Act*, ensuring that the digital history of the individual remains transparent and accountable to the law.

Table 5: Forensic Audit Fields in the CPIC Historical Database

Audit Field	Data Captured	Investigative Value
Transaction Code	ADD, MODIFY, CLEAR, CANCEL	Identifies the lifecycle phase of the warrant.
Timestamp	Milliseconds / Date	Establishes the chronological veracity of the warrant entry.
ORI	Originating Agency Identifier	Identifies the specific police division responsible for the data.

Terminal ID	Physical Hardware Address	Proves where the data was entered (Court vs. Admin Office).
User ID	Credentials of the Operator	Identifies the individual who performed the systemic entry.

Table 6: Statutory Remedies under the Federal Privacy Act

Provision	Right Conferred	Application to Information Package
Section 12(1)	Right of Access	Compels the RCMP to disclose CPIC metadata and transaction logs.
Section 12(2)(a)	Right to Correction	Allows for the correction of fraudulent or manipulated data fields.
Section 12(2)(b)	Notation of Disagreement	Forces the system to flag the record as contested by the subject.
Section 12(2)(c)	Mandatory Notification	Requires the RCMP to inform justice partners of the inaccuracy.

The use of these statutory mechanisms is essential for restoring the *status quo ante* in the face of systemic administrative failure. In a justice system that increasingly relies on automated digital records, the ability to audit the provenance of those records is the only viable defense against technological vitiation and jurisdictional overreach.

Impact of Software Bugs on Documentary Integrity

The technical deficiencies of GrapeCity Documents for PDF version 6.0.2.0 may have contributed directly to the "metamorphosis" of the Information Package. Technical reports indicate that this version of the library suffered from memory management issues and failures to correctly render complex PDF structures. When a server-side application experiences an "Item already has an owner" exception, it can lead to unstable document generation where metadata from one object is incorrectly rendered or missing entirely.

This technical instability corroborates the structural errors noted in the 43-point deficiency chart, particularly the failure to render a judicial signature on Page 3 despite including an attribution text. While these might be viewed as "glitches" by a developer, in a legal context, they constitute a failure to maintain a valid and accurate record of a judicial authorization. The presence of the GrapeCity SDK as the "Producer" is the key technical artifact that links the document to a custom-coded government portal, suggesting that the document was born from an automated digital system rather than a clerk-validated manual process.

---- nothing past this line -----

Tab C

72
239

125

☒ IPV (Intimate Partner Violence / *Violence contre un partenaire intime*) ☐ Replacement Information / *Dénonciation de remplacement*
☐ I (Impaired driving with substances / *Conduite avec capacités affaiblies par des substances*) ☐ V (Vessel / *Bateau*)

Arrest Date: _____ 15 month Flag: _____ 18 month Flag: _____
Date d'arrestation _____ Alerte à 15 mois (ddmmyy / jjmmaa) Alerte à 18 mois (ddmmyy / jjmmaa)
Sworn Date: 230924 15 month Flag: 241225 18 month Flag: 250326
Date d'assermentation _____ Alerte à 15 mois (ddmmyy / jjmmaa) Alerte à 18 mois (ddmmyy / jjmmaa)

4810 998 24 48129169

Information Number / N° de la dénonciation

NOTICE: Orders concerning this court Information relating to publication bans, non-disclosure/communication and French-language rights, are available on a separate page and **must** be followed.

AVIS: Les ordonnances liées à la présente dénonciation en ce qui a trait aux interdictions de publication, à la non-divulgaration ou à la non-communication et aux droits linguistiques des francophones figurent sur une page distincte. Ces ordonnances **doivent** être respectées.

Form 2 Information / Formule 2 Dénonciation

Sections 506, 508.1 and 788 of the Criminal Code / *Articles 506, 508.1 et 788 du Code criminel*

CANADA
PROVINCE OF ONTARIO
PROVINCE DE L'ONTARIO
TORONTO
(Region / *Région*)

Information of: **Christyn Frugoni-Rojas**
Dénonciation de :
of **THE CITY OF TORONTO**
de
hereinafter called the informant / *ci-après appelé(e) le dénonciateur*

Court Officer
(occupation / *profession*)

The informant says that he/she believes on reasonable grounds that
Le dénonciateur déclare qu'il a des motifs raisonnables de croire que

(1) **MCLEAN, Kevin** DOB: 25 Mar. 1983
NFA, , ON

COUNT 1

Kevin MCLEAN

on or about the 22nd day of September in the year 2024 at the City of Toronto in the Toronto Region did, without lawful authority and knowing that another person, namely Nicole ARTOPOULOS, was harassed or recklessly as to whether that person was harassed, engage in repeatedly communicating with, either directly or indirectly, that person, and cause the said Nicole ARTOPOULOS to reasonably fear for personal safety, contrary to Section 264, subsection (2), clause (b) of the Criminal Code of Canada.

----- **End of Charges/Counts** -----

Declaration of Informant / Déclaration du dénonciateur

I declare that all matters contained in the Information are true to my knowledge and belief, pursuant to s. 508.1(2) of the *Criminal Code*.

Je soussigné(e) déclare tous les renseignements contenus dans la présente dénonciation sont, à ma connaissance, véridiques, en vertu de par. 508.1(2) du Code criminel.

Dated at **CITY of TORONTO** in the Province of Ontario, this **23rd** day of **SEPTEMBER**, 20 **24**
Fait à(au) *dans la province d'Ontario, ce* *jour de*

Declared / Déclaré

Christyn
Frugoni-
Rojas CL (M)

Digitally signed by
Christyn Frugoni-
Rojas CL (M)
Date: 2024.09.23
11:48:25 -04'00'

Digital Signature of Informant / Signature numérique du dénonciateur

241 Court Endorsement

This Information is Accepted on its face.

Kevin MCLEAN:

Warrant In The First: Issue

Dated in the Province of Ontario, this 23rd day of September 2024.

Fait à/au dans la province de l'Ontario, ce 23 septembre 2024.



Justice of the Peace
Ontario Court
of Justice

Digitally signed by
George Jiri
Date:2024.09.23
12:59:50 -04'00'

This document has been digitally signed. / Ce document a été signé numériquement.

Arrest Date: _____	15 month Flag: _____	18 month Flag: _____
<i>Date d'arrestation</i>	<i>Alerte à 15 mois (ddmmyy / jjmmaa)</i>	<i>Alerte à 18 mois (ddmmyy / jjmmaa)</i>
Sworn Date: 230924	15 month Flag: 241225	18 month Flag: 250326
<i>Date d'assermentation</i>	<i>Alerte à 15 mois (ddmmyy / jjmmaa)</i>	<i>Alerte à 18 mois (ddmmyy / jjmmaa)</i>

[] Accused notified court under s. 530(3)
Tribunal avisé par l'accusé en vertu de l'art. 530(3)

[] Designation Filed
Designation déposée

[] Interpreter Required
Interprète requis

Date Date	Accused Accusé	Adjournment Date Date d'ajournement	Adjournment Details Détails sur l'ajournement	Designation Désignation	Counsel As Agent Avocat mandataire	Fails to appear Omet de comparaître	Bench Warrant Mandat d'arrêt	Discretion Discretion	Certificate of Default Certificat de défaut
03 Oct 2024	MCLEAN, KEVIN	13 Nov 2024	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, FA, VI, ACP - Warrant in the First Executed						
13 Nov 2024	MCLEAN, KEVIN	18 Dec 2024	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, ACP - - DISC BW			X	X	X	
18 Dec 2024	MCLEAN, KEVIN	19 Mar 2025	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, ACP - -11b waived - - DISC BW Rescinded						
19 Mar 2025	MCLEAN, KEVIN	16 Apr 2025	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, APN - - DISC BW			X	X	X	
16 Apr 2025	MCLEAN, KEVIN	14 May 2025	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, ACP - - DISC BW Rescinded						
14 May 2025	MCLEAN, KEVIN	11 Jun 2025	Toronto-OCJ-T-10 Armoury St - 702 @ 2:00 PM, ST, VI, ACP						

Date Date	Clerk Greffier	Crown Couronne	For the Accused Pour l'accusé	Justice's Initials Initiales du juge
03 Oct 2024	Henriquez, Michael	NA	NP, NA, NOR	DJ
13 Nov 2024	Nurali, Saira	Pashang, Sia	NP, NP (Acc appeared in triage), NRC	TC
18 Dec 2024	Barna, Elizabeth	Dimiskovska, Andrea	AA, AA, VI, Self-Rep, NRC	JG
19 Mar 2025	Weisemberg, Iara	Laws, Jennifer	NP, NRC	JR
16 Apr 2025	Berhane, Aron	Dimiskovska, Andrea	AA, Self-Rep, NRC	BS
14 May 2025	Booth, Catherine	Laws, Jennifer	AA, Self-Rep, NRC	BS

[] At Bail Review date
À la révision de l'ordonnance
de détention, datee du

[] Original Order
Confirmed
Ordonnance originale
Confirmée

[] New Order
Made
Nouvelle
ordonnance
rendue

[] Gladue Report
Requested
Rapport Gladue
demandé

(date / date)

Information No. / N° de la dénonciation				
Return Date / Date à laquelle le document est rapporté _____, 20__				
INFORMATION Against / DÉNONCIATION visant MCLEAN, Kevin				
Address / Adresse NFA , ON				
CHARGE / ACCUSATION HARASSMENT BY REPEATED COMMUNICATION WITH PERSON				
Refer to front page for further counts / Reportez-vous à la première page pour plus de chefs				
FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT				
☐ Summons / Somation ☐ Show Cause / Audience de justification ☒ Warrant 1 st / Mandat en 1 ^{re} instance				
☐ Replacement Information / Dénonciation de remplacement				
☐ Reportable M.V. Offence (H.T.A. 199) / Infraction V.M. à déclarer (Code de la route 199) C.V.O.R. No (Commercial Vehicles Only) / Numéro C.I.U.V.U. (véhicules utilitaires seulement)				
Sex / Sexe M	Birth Date / Date de naissance Day / Jour: 25 Month / Mois: 03 Year / Année: 1983	Was defendant owner? / La partie défenderesse était-elle propriétaire? ☐ Yes / Oui ☐ No / Non		
Driver's Licence Number / Numéro du permis de conduire M16514331830325				
Plate No. / Numéro de plaque		☐ Involves a Collision / Infraction reliée à un accident		
Informant / Dénonciateur Christyn Frugoni-Rojas				
Deemed Sworn / Affirmed Date / Réputée être déclarée sous serment/affirmée solennellement le SEP 23rd, 24		Date of Arrest / Date de l'arrestation		
Officer / Agent de police KOLANKOWSKI, MI		No. / N° 82239		
Police Agency / Service de police TORONTO POLICE SERVIC		Div. / Dist. 14 DIVISION		
Occurrence Number / N° d'incident 24-2082035				
Courtroom / Salle d'audience				
At / À(Au) OCJT #204 IPV SOUTH 10 ARMOURY ST, TORONTO ON M7A 0B9				

Information No. / N° de la dénonciation				
Return Date / Date à laquelle le document est rapporté _____, 20__				
INFORMATION Against / DÉNONCIATION visant				
Address / Adresse				
CHARGE / ACCUSATION				
Refer to front page for further counts / Reportez-vous à la première page pour plus de chefs				
FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT				
☐ Summons / Somation ☐ Show Cause / Audience de justification ☐ Warrant 1 st / Mandat en 1 ^{re} instance				
☐ Replacement Information / Dénonciation de remplacement				
☐ Reportable M.V. Offence (H.T.A. 199) / Infraction V.M. à déclarer (Code de la route 199) C.V.O.R. No (Commercial Vehicles Only) / Numéro C.I.U.V.U. (véhicules utilitaires seulement)				
Sex / Sexe	Birth Date / Date de naissance Day / Jour Month / Mois Year / Année	Was defendant owner? / La partie défenderesse était-elle propriétaire? ☐ Yes / Oui ☐ No / Non		
Driver's Licence Number / Numéro du permis de conduire				
Plate No. / Numéro de plaque		☐ Involves a Collision / Infraction reliée à un accident		
Informant / Dénonciateur				
Deemed Sworn / Affirmed Date / Réputée être déclarée sous serment/affirmée solennellement le		Date of Arrest / Date de l'arrestation		
Officer / Agent de police		No. / N°		
Police Agency / Service de police		Div. / Dist.		
Occurrence Number / N° d'incident				
Courtroom / Salle d'audience				
At / À(Au)				

Information No. / N° de la dénonciation				
Return Date / Date à laquelle le document est rapporté _____, 20__				
INFORMATION Against / DÉNONCIATION visant				
Address / Adresse				
CHARGE / ACCUSATION				
Refer to front page for further counts / Reportez-vous à la première page pour plus de chefs				
FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT				
☐ Summons / Somation ☐ Show Cause / Audience de justification ☐ Warrant 1 st / Mandat en 1 ^{re} instance				
☐ Replacement Information / Dénonciation de remplacement				
☐ Reportable M.V. Offence (H.T.A. 199) / Infraction V.M. à déclarer (Code de la route 199) C.V.O.R. No (Commercial Vehicles Only) / Numéro C.I.U.V.U. (véhicules utilitaires seulement)				
Sex / Sexe	Birth Date / Date de naissance Day / Jour Month / Mois Year / Année	Was defendant owner? / La partie défenderesse était-elle propriétaire? ☐ Yes / Oui ☐ No / Non		
Driver's Licence Number / Numéro du permis de conduire				
Plate No. / Numéro de plaque		☐ Involves a Collision / Infraction reliée à un accident		
Informant / Dénonciateur				
Deemed Sworn / Affirmed Date / Réputée être déclarée sous serment/affirmée solennellement le		Date of Arrest / Date de l'arrestation		
Officer / Agent de police		No. / N°		
Police Agency / Service de police		Div. / Dist.		
Occurrence Number / N° d'incident				
Courtroom / Salle d'audience				
At / À(Au)				

Tab D

245

Analysis of "False Information Package"

Discrepancies and GrapeCity Metadata

This chart-based analysis separates the specific, enumerated errors found in the five-page "False Information Package" (Schedule A) from the known technical deficiencies of the document production software, GrapeCity Documents for PDF (Schedule B).

Schedule A: Specific Errors and Inconsistencies in the False Information Package

Schedule A meticulously details 29 specific internal and external errors, format deviations, and inconsistencies found in the five-page document when compared to the standardized six-page "Valid CCO Information Standard Form Package."

Error Category	Specific Deficiency Point	Location in False Information Package	Comparison / Implication
Page & Footer Inconsistencies	Footer is demonstrably different	Pages 1 & 5 vs. Page 2 of 5	Inconsistent footers across the document.
	Footer fails to include a single space	Footer (rev. 10/20)	Error in the form designation ("C-e" instead of "C e").
	Illegibility in "save toner mode"	Only footer on Page 2 of 5 remains legible	Evidence of potentially "missing text and false documentation."
	Erroneous footer	Page 3 of 5	Reproduction of the header from Page 1 of 5.
Formatting & Input Errors	Erroneously includes two commas after "NFA [sic]"	Page 1 of 5 (Address line)	Incorrect formatting where the Accused's address was entered.
	"NFA" (No Fixed Address) is included	Page 1 of 5	Inconsistent with the reference to the Applicant's driver's license number on Page 5.
	Superfluous numeral "(1)"	Page 1 of 1	Incorrectly precedes the Accused's name.
	Incorrect placement of date of birth	Page 1 of 1	Standard format mandates "address" preceding "date of birth."

246

	Date of birth is rendered in incorrect format	Page 1 of 1	Fails to adhere to the required format of '(day/jour) (month/mois) year/année)'.
	Omission of '[Accused/Accusé]' format	Document content	Required "Last Name, First Name" and (nom, prénom) is conspicuously absent.
	Phrase "end of charges/counts" used	Document content	An improper input, not a component of the Valid CCO Information Standard Form Package.
Legal & Jurisdiction Deviations	Inclusion of "Count 1"	Document content	Implies the existence of "other counts," inconsistent with the document's content and Criminal Code s. 788.
	Improper header	Page 2 of 5	Displays "R. v. McLean, Kevin" with a Toronto Police Service (TPS) occurrence number identical to the Undertaking Form 10.
	Jurat improperly located and legally impermissible	Page 2 of 5	Appears on a separate page from the text to which it pertains.
	False Case Identification Number	Page 3 of 5, "Police Case ID:457197"	Uses six digits instead of the required seven (7) digits preceded by a year string.
	"Intake Court Endorsement" terminology used	Page 3 of 5	Family law standard terminology; used as a "deliberate diversion" from the jurisdictional authority of a Superior Court of Justice judge.
	Omission of the city for the authorizing judge	Document content	Supports the inference of diversion from Superior Court of Justice or Divisional Court authority.
	Grammatical/Spelling Errors	Page 3 of 5, "This Information is Accepted [sic] on its face"	Indicative of a court officer, not a TPS detective.

247 Language & Translation Errors	Incorrect accent orientation	Page 2 of 5 (digitally signed phrase)	Uses 'accents graves' instead of requisite 'accents aigus,' suggesting manipulation.
	Unrequired French translation inclusion	Page 3 of 5 (under dating and location)	Inclusion of French translation was not required for the Ontario-only location.
	Omission of "jour" and "de"	Page 3 of 5 (TPS transcriber error)	Unauthorized transcriber error after the "23" for "day of."
	Incorrect French preposition	Page 3 of 5 (TPS transcriber error)	"Fait à/au:" used when it should have been "Fait à (au):".
	Incorrect City/Province text	Document content	Should read "Dated At City of Toronto" followed by "...in the Province of Ontario."
Digital Signature & Manipulation	Incorrect bolding and period inclusion in digitally signed phrase	Page 3 of 5	Suggests TPS manipulation, despite correct 'accents aigus.'
	Improper placement of digitally signed phrase	Page 3 of 5	Located in the middle of the page, not in the footer.
Missing Content & Structure	Page 3 of 5 inclusion	Document content	Not a constituent part of the Valid CCO Information Standard Form Package.
	Absence of page 4 of 6	Document content	Consistent with the involvement of a Superior Court Judge/Divisional Court Judge completing a Form 7 "Warrant for Arrest" or warrant under s. 487, or Crown Election.
	Auto-bookmarking issues	Document bookmarks	Bookmarks (Front Page, Adjournment Page, Last Page) lead to the conclusion that various pages were not the same as the False Information Package.

Schedule B: Metadata and Known Deficiencies of Document Producer

248

Schedule B identifies the PDF producer used to generate the document and details the common, reported deficiencies associated with that software, which potentially corroborate the errors noted in Schedule A.

GrapeCity Issue Category	Specific Deficiency/Reported Problem	Implication in Context
Software Identification	Application & Producer: Grape.City.Documents.PDF-6.0.2.0	Confirms the use of this specific programmatic .NET library, which is <i>not</i> a standard end-user tool like Adobe Acrobat.
Memory Issues	Significant increases in memory consumption; reported "Insufficient memory" exceptions after updates.	Could lead to unstable generation/saving, potentially causing data loss or corruption during document creation.
PDF Handling/Corruption	Throws exceptions when printing, loading, or saving; errors like "Document catalog not found" and "Item already has an owner."	Indicates the library can produce corrupted documents, especially when linearizing existing PDFs.
Footer Rendering Defects	Incorrect placement (varying offsets, appearing in the header); Unexpected content (e.g., "about:blank"); Failure to Render (when both header/footer are defined).	Directly corroborates the footer and header-as-footer errors noted in Schedule A (e.g., inconsistent footers, erroneous footer reproduction on Page 3).
Security Limitations	Inherits limitations from the PDF specification regarding encryption algorithms and key length, despite supporting AES-256.	Relevant if the document was password-protected or secured.
Developer Focus	The library is primarily a tool for developers to integrate PDF functionality programmatically.	Highlights that the document was created via an automated, back-end process rather than simple manual input via standard court software, which is crucial to the investigation of manipulation.

This detailed breakdown separates the specific factual errors in the court document (Schedule A) from the systemic, technical flaws of the software used to create it (Schedule B).

Tab E

250

☐ N ☐ S

136

Information Number / N° de la dénonciation

- ☐ Non-Disclosure Order Pursuant to S. 486.31
Ordonnance de non-divulgence, art. 486.31
- ☐ Non-communication s. 515(12) & 516(2)
Non-communication, par. 515(12) et 516(2)

- ☐ Publication ban pursuant to
Interdiction de publication en vertu de
- ☐ Provisions of 530(3) Complied With
Dispositions du par. 530 (3) observées

Arrest Date:

Date d'arrestation

15 month Flag:

Alerte à 15 mois

18 month Flag:

Alerte à 18 mois

Sworn Date:

Date d'assermentation

15 month Flag:

Alerte à 15 mois

18 month Flag:

Alerte à 18 mois

CANADA
PROVINCE OF ONTARIO
PROVINCE DE L'ONTARIO

Information of:

Dénonciation de :

of

de

(Region / Région)

(occupation / profession)

The informant says that **he/she** believes on reasonable grounds that

Le dénonciateur déclare qu'il a des motifs raisonnables de croire que

[Accused / Accusé]

(Last Name, First Name) (*nom, prénom*)

[Address / adresse]

(Date of birth / *date de naissance*)

(Day / *jour*) / (Month / *mois*) / (Year / *année*)

(enter charges here / *insérer des accusations ici*)

Date	Accused Accusé	Adjournment Date Date d'ajournement	Adjournment Details Détails sur l'ajournement	Designation Désignation	Counsel As Agent Avocat mandataire	Fails to Appear Ornet de comparaître	Bench Warrant Mandat d'arrêt	Discretion Discrétion	Certificate of Default Certificat de défaut

Date	Clerk Greffier	Crown Couronne	For the Accused Pour l'accusé	Justice's initials Initiales du juge

253

Information Number / N°(s) de dénonciation _____

☐ To be completed where information is laid other than in person: I, _____, state that
À remplir lorsque la dénonciation est déposée autrement qu'en personne : Je soussigné(e) _____ (name of informant / nom du dénonciateur) déclare que
all matters contained in this information are true to my knowledge and belief, pursuant to s. 508.1 (2) of the *Criminal Code*.
tous les renseignements contenus dans la présente dénonciation sont, à ma connaissance, véridiques, en vertu de par. 508.1 (2) du Code criminel.

☐ Deemed to be sworn / Réputée être faite sous serment

Sworn/affirmed before me at the _____
Déclaré sous serment/affirmé solennellement devant moi à/au _____

of / de _____ Informant / Dénonciateur

in the Province of Ontario / dans la province de l'Ontario

this _____ day of _____, 20 _____
ce _____ jour de _____ Justice of the Peace / Juge de paix

☐ Appearance Notice ☐ Promise to Appear ☐ Recognizance
Citation à comparaître Promesse de comparaître Engagement
for _____, 20 _____
pour le _____ (day, month / jour, mois)

CHECK ONE OF THE FOLLOWING / COCHEZ LA CASE QUI CONVIENT

☐ Cancelled – Police to notify defendant ☐ Cancelled – Summons ☐ Confirmed on _____, 20 _____
Annulé(e) – La police informera la partie défenderesse Sommation Confirmé(e) le _____ (day, month / jour, mois)

☐ Cancelled - Warrant issued _____
Annulé(e) – Mandat délivré _____

_____, 20 _____
Justice of the Peace / Juge de paix (day, month / jour, mois)

Date Date	Crown Elects to Proceed La Couronne choisit de procéder par	☐ Summarily Procédure sommaire	☐ By Indictment Acte d'accusation	☐ Summary Conviction Offence(s) Infraction(s) punissable(s) sur déclaration de culpabilité par procédure sommaire	☐ Indictable Offence(s) Infraction(s) punissable(s) par mise en accusation				
Date Date	Accused Accusé	Elects Trial by Choix d'un procès devant			Preliminary Hearing Requested Enquête préliminaire demandée	Justice Initials Initiales du juge	Abs. Juris. Comp. absolue	Pleads Plaide	
		Superior Court Cour supérieure		Ontario Court Cour de l'Ontario				Guilty to Counts Coupable aux chefs d'accusation	Not Guilty to Counts Non coupable aux chefs d'accusation
		Judge Juge	Judge & Jury Juge et jury	Judge On Counts Juge pour les chefs d'accusation					

Date Date	Accused Accusé	Committed (or) Ord. Std. Trial *On Counts Renvoyé à procès pour les chefs d'accusation	Discharged on Counts Libéré des chefs d'accusation	Found / Reconnu	
				Guilty on Counts Coupable des chefs d'accusation	Not Guilty on Counts Non coupable des chefs d'accusation

* ☐ With consent of accused and prosecutor, without taking or recording
Avec le consentement de l'accusé et du poursuivant, sans recueillir ou consigner ☐ (a) any evidence (or) ☐ (b) further evidence
a) des preuves (ou) b) des preuves additionnelles

Judge / Juge

Count / Chef _____		Sentence date / Date de détermination de la peine _____		☐ Withdrawn / Accusation retirée	
☐ Pre-sentence custody _____ days/months	Time credited: _____ days/months	☐ concurrent with _____			
<i>Détention sous garde avant prononcé de</i> _____ <i>jours/mois</i>	<i>Crédit octroyé</i> _____ <i>jours/mois</i>	<i>concurrente avec</i> _____			
☐ Term that would have been imposed before credit granted: _____ days/months/years					
<i>Période d'emprisonnement imposée avant l'octroi de tout crédit</i> _____ <i>jours/mois/ans</i>					
☐ Absolute discharge _____	☐ Conditional discharge _____	☐ Suspended sentence _____			
<i>Absolution inconditionnelle</i>	<i>Absolution conditionnelle</i>	<i>Condamnation avec sursis</i>			
☐ Imprisoned for _____ days/months/years	☐ concurrent with _____	☐ consecutive to _____			
<i>Emprisonnement pour</i> _____ <i>jours/mois/ans</i>	<i>concurrent avec</i> _____	<i>consécutif à</i> _____			
☐ Intermittent sentence for _____ days	☐ concurrent with _____	☐ consecutive to _____			
<i>Peine discontinue</i> _____ <i>jours</i>	<i>concurrente avec</i> _____	<i>consécutif à</i> _____			
☐ Conditional sentence for _____ days/months/years	☐ concurrent with _____	☐ consecutive to _____			
<i>Ordonnance de sursis</i> _____ <i>jours/mois/ans</i>	<i>concurrente avec</i> _____	<i>consécutif à</i> _____			
☐ Probation _____ months/years	☐ concurrent with _____	☐ consecutive to _____			
<i>Période de probation</i> _____ <i>mois/ans</i>	<i>concurrente avec</i> _____	<i>consécutif à</i> _____			
☐ Community service s.732.1(3)(f) / <i>Service communautaire, par. 732.1(3)(f)</i> _____ hours / heures					
☐ Fine of \$ _____ VS \$ _____	Time to pay _____	Days in default _____			
<i>Amende de</i> _____ <i>\$ sur. comp.</i>	<i>\$ Délai de paiement</i>	<i>Jours à défaut</i>			
☐ Restitution ☐ s. 738 / s. 739	Amount: \$ _____	Time to pay _____			
<i>Dédommagement</i> <i>art. 738 / art. 739</i>	<i>Montant</i> _____ <i>\$</i>	<i>Délai de paiement</i>			
☐ Victim surcharge: \$ _____	Time to pay: _____	Days in default _____			
<i>Suramende compensatoire</i> _____ <i>\$</i>	<i>Délai de paiement</i>	<i>Jours à défaut</i>			
☐ Ordered to stand trial: / <i>Renvoyé pour subir son procès</i> _____					
☐ Dismissed	☐ Driving prohibition: _____	☐ HTA cautioned _____ Months / Years	☐ s.743.21(1) / <i>par. 743.21(1)</i>		
<i>Rejeté</i>	<i>Interdiction de conduite</i>	<i>Avertissement</i> (Code de la route) _____ <i>mois/années</i>			
☐ Acquitted	☐ Weapons prohibition: _____	☐ s. 109(2): _____ years ☐ s. 109(3) (Life) ☐ s. 110: _____ years ☐ s. 110 (life)			
<i>Acquitté</i>	<i>Interdiction d'armes</i>	<i>par. 109(2)</i> <i>ans</i> <i>par. 109(3)(perpétuité)</i> <i>art 110</i> <i>ans</i> <i>art .110 (perpétuité)</i>			
☐ Stayed	☐ DNA: _____	☐ 5.03 (Primary) _____	☐ 5.04 (Secondary) _____	☐ Denied (DND)	
<i>Sursis</i>	<i>ADN</i>	<i>5.03 (primaire)</i>	<i>5.04 (secondaire)</i>	<i>Rejetée</i>	
☐ In Absentia	☐ S.O.I.R.A. order: _____	☐ 10 years _____	☐ 20 years _____	☐ Life	
<i>In absentia</i>	<i>Ordonnance LERDS</i>	<i>10 ans</i>	<i>20 ans</i>	<i>Perpétuité</i>	
☐ Other	☐ s. 161 prohibition: _____	☐ _____ months/years	☐ s. 490 forfeiture order: _____	☐ Granted	☐ Denied
<i>Autre</i>	<i>Interdiction, art. 161</i>	<i>mois/ans</i>	<i>Ordonnance de confiscation, art. 490</i>	<i>Accordée</i>	<i>Rejetée</i>

No. of Information / N° de la dénonciation	
Return Date / Date à laquelle le document est rapporté , 20	

INFORMATION Against / DÉNONCIATION visant

Address / Adresse

CHARGE / ACCUSATION

Refer to front page for further counts. / Reportez-vous à la première page pour plus de chefs.

FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT									
☐ Summons Sommons		☐ Show Cause Audience de justification		☐ Warrant 1 st Mandat en 1 ^{re} instance		Re-laid Information Dénomination de remplacement			
Reportable M.V. Offence (H.T.A. 199) ☐ Infraction V.M. à déclarer (Code de la route 199)		C.V.O.R. No (Commercial Vehicles Only) Numéro C.E.C.V.U. (véhicules utilitaires seulement)							
Sex	Birth Date / Date de naissance	Day / Month / Jour / Mois		Year / Année		Was defendant owner? La partie défenderesse était-elle propriétaire?		☐ Yes / Oui ☐ No / Non	
Sexe	Day / Month / Jour / Mois	Year / Année							
Driver's Licence Number / Numéro du permis de conduire									
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction liée à un accident							
Informant Dénonciateur									
Date Sworn Date d'assermentation		Date of Arrest Date de l'arrestation							
Officer / Agent de police		No. / N°							
Police Agency / Service de police		Div. / Dist.							
Occurrence Number / N° d'incident									
Courtroom / Salle d'audience									
At / À(Au)									

No. of Information / N° de la dénonciation	
Return Date / Date à laquelle le document est rapporté , 20	

INFORMATION Against / DÉNONCIATION visant

Address / Adresse

CHARGE / ACCUSATION

Refer to front page for further counts. / Reportez-vous à la première page pour plus de chefs.

FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT									
☐ Summons Sommons		☐ Show Cause Audience de justification		☐ Warrant 1 st Mandat en 1 ^{re} instance		Re-laid Information Dénomination de remplacement			
Reportable M.V. Offence (H.T.A. 199) ☐ Infraction V.M. à déclarer (Code de la route 199)		C.V.O.R. No (Commercial Vehicles Only) Numéro C.E.C.V.U. (véhicules utilitaires seulement)							
Sex	Birth Date / Date de naissance	Day / Month / Jour / Mois		Year / Année		Was defendant owner? La partie défenderesse était-elle propriétaire?		☐ Yes / Oui ☐ No / Non	
Sexe	Day / Month / Jour / Mois	Year / Année							
Driver's Licence Number / Numéro du permis de conduire									
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction liée à un accident							
Informant Dénonciateur									
Date Sworn Date d'assermentation		Date of Arrest Date de l'arrestation							
Officer / Agent de police		No. / N°							
Police Agency / Service de police		Div. / Dist.							
Occurrence Number / N° d'incident									
Courtroom / Salle d'audience									
At / À(Au)									

86

No. of Information / N° de la dénonciation	
Return Date / Date à laquelle le document est rapporté , 20	

INFORMATION Against / DÉNONCIATION visant

Address / Adresse

CHARGE / ACCUSATION

Refer to front page for further counts. / Reportez-vous à la première page pour plus de chefs.

FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT									
☐ Summons Sommons		☐ Show Cause Audience de justification		☐ Warrant 1 st Mandat en 1 ^{re} instance		Re-laid Information Dénomination de remplacement			
Reportable M.V. Offence (H.T.A. 199) ☐ Infraction V.M. à déclarer (Code de la route 199)		C.V.O.R. No (Commercial Vehicles Only) Numéro C.E.C.V.U. (véhicules utilitaires seulement)							
Sex	Birth Date / Date de naissance	Day / Month / Jour / Mois		Year / Année		Was defendant owner? La partie défenderesse était-elle propriétaire?		☐ Yes / Oui ☐ No / Non	
Sexe	Day / Month / Jour / Mois	Year / Année							
Driver's Licence Number / Numéro du permis de conduire									
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction liée à un accident							
Informant Dénonciateur									
Date Sworn Date d'assermentation		Date of Arrest Date de l'arrestation							
Officer / Agent de police		No. / N°							
Police Agency / Service de police		Div. / Dist.							
Occurrence Number / N° d'incident									
Courtroom / Salle d'audience									
At / À(Au)									

TAB 10

Tab A



Mr. Kevin McLean <mcleansettlement@gmail.com>

Privacy Act request P-2025-16999 / F339, Your File N/A, Acknowledgment

Mr. Kevin McLean <mcleansettlement@gmail.com>

Wed, May 6, 2026 at 10:41 AM

To: "Ball, Jeff (RCMP/GRC)" <Jeff.Ball@rcmp-grc.gc.ca>

Cc: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>, "Simpson, Melissa (RCMP/GRC)" <Melissa.Simpson@rcmp-grc.gc.ca>, "Worrell, Julie (RCMP/GRC)" <Julie.Worrell@rcmp-grc.gc.ca>, "Duheme, Michael (RCMP/GRC)" <Michael.Duheme@rcmp-grc.gc.ca>, "Brisson, Stéphane (RCMP/GRC)" <stephane.brisson@rcmp-grc.gc.ca>

DELIVERY METHOD: Via Registered Mail & Electronic Transmission**URGENT****DATE:** May 6, 2026**TO:****Mr. Michael Duheme**, Commissioner, Royal Canadian Mounted Police (the “**Head of the Institution**”)**Mr. Jeff Ball**, Director, Access to Information and Privacy Branch (the “**ATIP Directorate**”)

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca**FROM:****Mr. Kevin A. McLean (B.A., J.D., CIM)**Email: mcleansettlement@gmail.com**REFERENCE:** *Privacy Act* Request File P-2025-16999 / F339 (the “**Privacy Request**”)**SUBJECT:** Comprehensive Requisition for Statutory Compliance and Formal Notice of Imminent

Commencement of Judicial Review Premised upon the Dereliction of the Ministerial Duty to Search and the

Terminal Deadline of May 11, 2026

I. DOCUMENTATION RELIED UPON AND COMPREHENSIVELY REVIEWED

1. In the rigorous formulation of the present legal requisitions and the attendant technical analysis, the following documentary instruments, *rules*, and statutory architectures have been systematically reviewed and relied upon by the Applicant:
 - i. *Privacy Act Request File P-2025-16999* (the “**Privacy Request**”), encompassing the institutional response dated April 27, 2026;
 - ii. *Access to Information Act Request*, dated May 5, 2026 (the “**ATIA Request**”), specifically targeting the procurement, licensing, and utilization of the **Mescius SDK**;
 - iii. Information Package 4810 998 24 48129169-00 (the “**False Information Package**”), characterizing profound jurisdictional and formatting anomalies;

- iv. Lincoln County Law Association Adult Common Form Information Package (the “**Standard Information Package**”), utilized as the normative comparator (the “**Valid CCO Information Standard Form Package**”);
- v. Correlative electronic communications dispatched to and received from the *Auditor General of Canada* (the “**Auditor General Communications**”), concerning the systemic subversion of the **CPIC System**;
- vi. The *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, and the *Federal Courts Rules*, SOR/98-106 (collectively, the “**Rules**”);
- vii. Forensic CPIC transaction logs identifying query Q PERS+ REM:000330500 (the “**Forensic Transaction Logs**”), evidencing the activation of high-threshold surveillance parameters;
- viii. Correspondence from Ananthan Sinnadurai (MAG/Crown Law Office Civil), dated June 25, 2025, and July 4, 2025 (the “**Sinnadurai Letters**”);
- ix. Landlord and Tenant Board Application LTB-L-067798-24 (the “**LTB Proceeding**”), and the resulting order of Adjudicator Delorenzi;
- x. Disciplinary and criminal filings regarding Sergeant Robert Black (TPS 14 Division), including reports from *Project South* (the “**Corruption Probe Records**”);
- xi. The *Privacy Act*, R.S.C., 1985, c. P-21, and the *Access to Information Act*, R.S.C., 1985, c. A-1 (collectively, the “**Transparency Statutes**”);
- xii. The *Criminal Code*, R.S.C., 1985, c. C-46, specifically sections 487 and 487.01 (the “**Code**”); and
- xiii. The Ministry of the Attorney General (MAG) Court Services Division (CSD) Court Information Access Guide (2019) (the “**MAG Access Guide**”).

II. PRELIMINARY STATEMENT REGARDING ADMINISTRATIVE RECALCITRANCE AND LITIGATION TOPOGRAPHY

- 2. The present correspondence is dispatched to provide a definitive and comprehensive formal notification concerning the ongoing and untenable posture of the Royal Canadian Mounted Police (the “**RCMP**”) regarding its purported entitlement to defer the provision of a compliant response until May 11, 2026. This administrative procrastination is fundamentally incompatible with the purposive and remedial framework of the **Transparency Statutes** and represents an egregious circumvention of mandatory obligations, thereby necessitating a forceful jurisprudential intervention *in limine*.
- 3. A rigorous comparative analysis of the disparate litigation topographies has been executed. Whereas the *Superior Court of Justice* (the “**SCJ**”) and the *Divisional Court of Ontario* impose a sequence of escalating financial impediments—including a \$243.00 filing fee, \$343.00 for interlocutory motions, and an onerous \$643.00 for the *Certificate of Perfection*—the nominal financial threshold for an application for judicial review in the *Federal Court of Canada* is a mere **\$50.00**.
- 4. *Ipso facto*, this negligible fiscal barrier facilitates the immediate and unencumbered escalation of the present matter, effectively neutralizing the administrative friction upon which the institution ostensibly relies. The **Head of the Institution** is hereby cautioned that the absence of a comprehensive, unredacted, and statutorily compliant disclosure by the aforementioned deadline shall inevitably precipitate an immediate legal challenge, rendering the current administrative posture an absolute nullity *ab initio*.

5. The empirical evidence synthesized from prior dossiers, intersected with the concurrent scrutiny by the *Auditor General of Canada*, militates toward a singular and incontrovertible conclusion: the obfuscatory conduct of the RCMP is a direct manifestation of its undisclosed status as the primary law enforcement applicant (the “**Law Enforcement Applicant**”) in the covert proceedings initiated in September 2024.
6. It is robustly contended that a diligent interrogation of the relevant databases—specifically the foundational metadata (the “**Metadata**”) underpinning the records—shall irrevocably substantiate the following foundational genesis of the *acta*:

Technical/Jurisdictional Category	Specified Data Points and Forensics
Originating Agency Identifier	ON80313 (the “ Milton ORI ”), denoting federal primacy.
Associated Detachment	RCMP Toronto West (Milton Detachment), the federal arm in the GTA.
Jurisdictional Nexus	Downtown Toronto Core and Western GTA, exploiting regional lacunae.
Court Level	<i>Superior Court of Justice</i> , bypassing the normative <i>Ontario Court of Justice</i> intake.
Court Location	361 University Avenue, Toronto, Ontario, in unrecorded chambers.
Presiding Judicial Officer	Chief Justice Morawetz, acting <i>ultra vires</i> ordinary delegation.

IV. THE SERGEANT ROBERT BLACK NEXUS: INFERENTIAL PROOF OF MANUFACTURED CRIMINAL PRETEXTS

7. The credibility of the enforcement actions initiated against the Applicant is further eroded by the documented presence and involvement of Sergeant Robert Black of the TPS 14th Division (the “**Sergeant Black**”). It is recalled that **Sergeant Black** was present for the Applicant’s paraded detention following the arrest on October 2, 2024.
8. **Sergeant Black**, a nineteen-year veteran, is currently the subject of profound criminal scrutiny. In early 2026, he was charged within the context of *Project South*—a major joint corruption investigation—with possession for the purpose of trafficking Adderall and cocaine, conspiracy to obstruct justice, and counselling an uncommitted indictable offence.
9. **THE ANALYTICAL SYLLOGISM OF CORRUPTION:**

- **Major Premise: Sergeant Black** formerly served within the Specialized Drug Squad and the Guns and Gangs Task Force.
- **Minor Premise:** The enforcement actions against the Applicant in 2024 were characterized by false allegations regarding “gang tattoos” and fabricated “drug issues.”
- **Empirical Nexus:** The Applicant’s prescribed Adderall medication was seized on October 2, 2024, and a subsequent prescription was stolen on October 25, 2024, at the CAMH visitor area.
- **Conclusion:** The involvement of an officer subsequently charged with trafficking the very substance seized from the Applicant, who possesses a background in Guns and Gangs, provides an inferential bridge to the RCMP **Milton Detachment’s** federal mandate. The coordination between **Sergeant Black’s** 14th Division presence and the RCMP **Milton ORI** confirms that the Applicant was a target of a “joint-force” artifice where federal mandates were laundered through a corrupted municipal division.

V. THE SINNADURAI COMMUNICATIONS AND THE SYLLOGISM OF INSTITUTIONAL EVASION

10. A critical juxtaposition is formulated between the **Sinnadurai Letters** (Ministry of the Attorney General) and the **RCMP Letter** dated April 27, 2026. In June and July 2025, Mr. Sinnadurai explicitly asserted that the Ministry possessed “no responsive criminal court records” at the *Superior Court of Justice* level and directed the Applicant to obtain any purported warrants from the “originating police service.”
11. Conversely, the RCMP’s response utilizes conditional language: “*If this matter concerned another police department, they may have information of interest to you.*” **Nota Bene:** This employment of the conditional “If” constitutes a linguistic absurdity. Had the RCMP conducted a diligent search and identified only records belonging to the TPS, it would have been compelled to issue a definitive “No Records” response. By instead invoking federal exemptions (Sections 19, 22, and 26) over records it *did* locate, the RCMP has executed an admission of possession. This implies that the RCMP is not a third party, but the primary architect and **Law Enforcement Applicant**.

VI. THE CROSS-JURISDICTIONAL NEXUS: NICOLE ARTOPOULOS AND THE BRITISH COLUMBIA CONDUIT

12. Ms. Nicole Artopoulos (the “**Ex-Fiancée**”) is an alumna of the **Simon Fraser University** (the “**SFU**”) Masters of Criminology program in British Columbia—a jurisdiction where the RCMP maintains pervasive operational dominance. It is submitted that the **Ex-Fiancée** maintained significant contact with former classmates currently serving as high-ranking officers within the federal institution.
13. This academic connection provides the primary conduit for the unlawful aggregation and subsequent laundering of the **2,500-Page Dossier** (the “**Historical Surveillance Archive**”) maintained by the RCMP on the Applicant. This cross-jurisdictional network facilitated the weaponization of fabricated 2017 “death threat” complaints into the current Ontario enforcement artifice, thereby providing a “Major Crimes” pretext for a localized civil vendetta.

VII. THE LANDLORD AND TENANT BOARD PROCEEDING AND THE RETALIATORY SEPTEMBER 15 “FIRST OCCURRENCE”

- . The genesis of the current enforcement artifice is rooted in the failed **LTB Proceeding** initiated by the Landlord, **Mrs. Aphrodite Artopoulos** (the “**Landlord**”). Following the summary dismissal of her motions due to their profound lack of evidentiary merit and the exposure of fraudulent misrepresentations regarding the Applicant’s tenancy at 410-775 King Street West, the **Landlord** and the **Ex-Fiancée** attempted to engage the TPS on Sunday, September 15, 2024.
15. This resulted in the **1st Occurrence Number** (Event # 2024-2028093). However, as confirmed by Police Officer Jolly of the 14th Division, this occurrence yielded no investigative results as the TPS correctly identified the matter as a private civil dispute. The **Landlord’s** subsequent dissatisfaction with the municipal force’s adherence to the rule of law served as the catalyst for the RCMP’s intervention as the primary **Law Enforcement Applicant**.

VIII. THE FRAUDULENT SECOND OCCURRENCE AND THE FORENSIC IRREGULARITY OF THE RCMP POLICE CASE IDENTIFIER

16. Following the TPS’s initial refusal to act on the merits, a **2nd Occurrence Number** was generated on September 22, 2024 (Event # 2024-2082035). The Applicant asserts that this occurrence is a fraudulent instrument designed to provide localized municipal cover for a federal operation.
17. **THE POLICE CASE IDENTIFIER SMOKING GUN:** The definitive forensic evidence lies in the **Police Case ID: 457197** (the “**Case ID**”). This identifier is more likely than not the police case ID of the RCMP, specifically the **Milton Detachment**, rather than the TPS or the *Ontario Provincial Police* (the “**OPP**”).
- **Forensic Inconsistency:** The **Case ID** is significantly shorter (six digits) than normative TPS occurrence numbers (which incorporate year-based prefixes and seven-digit sequences).
 - **RCMP Consistency:** This truncated alphanumeric style is consistent with the lower transaction volume and specialized administrative protocols of a federal detachment like **Milton (ON80313)**. The **Case ID: 457197** is the digital fingerprint of an RCMP transaction that was subsequently superimposed onto a municipal template to facilitate the **False Information Package**.

IX. THE BALDOVI PARADIGM AND THE STATUTORY FOUNDATIONS OF CHIEF JUSTICE SELF-ASSIGNMENT

18. It is imperative to radically invert the prevailing narrative regarding the inexplicable involvement of Chief Justice Morawetz. Under standard statutory strictures, a Chief Justice’s principal duty is the equitable distribution of cases and the maintenance of judicial impartiality. However, as established in the authoritative decision of *R. v. Baldovi, 2016 MBQB 90* (the “**Baldovi Paradigm**”), there exist extraordinary circumstances where the Chief Justice may assume direct oversight.
19. **The Criteria for Oversight:** Direct assumption of oversight by the foremost judicial figure is reserved for instances characterized by:
- i. Extreme technical **Complexity**;
 - ii. Significant institutional **Controversy**;
 - iii. High **Prominence** or high-profile status; or
 - iv. Acute **Threats to the court's integrity**.

The self-assignment by Chief Justice Morawetz in September 2024 to an undisclosed *In Camera* hearing confirms that the RCMP sought high-stakes federal instruments (such as a *Section 487.01 General Warrant*) that necessitated the judgment, experience, and gravitas of the Chief Justice. This exercise was neither arbitrary nor habitual; it was invoked precisely because the matter touched upon the fundamental legitimacy of the court's process.

X. PHILOLOGICAL AND STATUTORY REINTERPRETATION OF SECTION 19(1)(d): THE "REGIONAL DETACHMENT" CONUNDRUM

21. A rigorous analysis of *Section 19(1)(d)* of the *Privacy Act* reveals a unique statutory anchor for the RCMP's current obfuscation. The subsection mandates the refusal to disclose personal information obtained in confidence from:

“...(d) a municipal or regional government established by or pursuant to an Act of the legislature of a province or *an institution of such a government*,”

22. **Nota Bene:** A precise reading of this provision, particularly the capitalized disjunctive conjunction, encompasses the **RCMP Detachment in Milton, Ontario**. The **Milton Detachment** identifies itself within the federal architecture as the **Toronto West Detachment** of the **Central Region**. Under *Section 3* of the *Privacy Act*, a “government institution” is defined as (a) any department or ministry of state of the Government of Canada. Consequently, a specific “department” or “regional region” within the RCMP constitutes an “institution” of a government within the meaning of the *Act*. Therefore, the RCMP's reliance on *Section 19(1)(d)* is effectively a claim of “confidence with oneself” between its own regional and federal branches to shield the **LEA** from the Applicant.

XI. THE OMNIBUS INTAKE ENDORSEMENT AND THE PRESUMPTIVE RIGHT TO PUBLIC ACCESSIBILITY

23. The Applicant maintains a reasonable and informed belief that the **Intake Court Endorsement** dated September 23, 2024 (the “**Omnibus Endorsement**”) was an all-encompassing legal instrument. This instrument likely consolidated: (1) approval of charges; (2) an arrest warrant; (3) a search warrant; (4) a general warrant; and (5) a production order.

24. Pursuant to *Section 2.1* of the **MAG Access Guide**, the general principle of public accessibility dictates that once process is issued—meaning an *Information* is sworn and an arrest is executed—criminal court files and documents become publicly accessible unless restricted by a specific court order. The Applicant was arrested on October 2, 2024. Consequently, the underlying *acta* of the *Pre-Enquête* hearing (the “**Pre-Enquête Documents**”) must, as a matter of law, be disclosed.

25. **The Routing Anomaly:** The *Information* was sworn in chambers before Chief Justice Morawetz and subsequently routed away from the SCJ 361 University Avenue 2nd Floor (Court Office 241) to the 1st Floor. This administrative redirection, executed with assistance from Madam Justice Shore in her capacity as family law team leader, served to facilitate the involvement of **Mr. Papadimitropoulos** and ensure the proceedings remained obscured from standard judicial registry oversight.

26. It is robustly contended that the RCMP conducted the search of the Applicant's residence at Unit 410-775 King Street West (the "**Residence**") immediately following the unlawful lockout. While the search yielded no incriminating evidence, the federal institution gained physical possession of the Applicant's property, including a passport, birth certificate, and medication.
27. **The 14th Division Lure:** On the night of October 2, 2024, the Applicant received the **Romano Communication** from Constable Anthony Romano of the TPS 14th Division. Constable Romano falsely lured the Applicant to the 14th Division under the pretext of property retrieval. Upon arrival, Constable Romano referenced an arrest warrant but refused to provide a copy thereof, citing it as an "external" matter.
28. **The Synchronicity Lacuna:** It is a technical reality that the internal Records Management Systems (RMS) of the TPS (Versadex) and the RCMP (PROS) are not seamlessly synchronized for document production. While they share limited data via the **CPIC System**, the underlying source documents remain within the control of the originating agency. Constable Romano's refusal to provide the warrant is consistent with a federal-municipal "syncing" lacuna: the TPS could "see" the warrant on CPIC via their terminal but did not possess the physical federal instrument (**Omnibus Endorsement**) for production.
29. **Evidence of RCMP Primacy:** In August 2025, both the TPS PEMU and Police Officer Jolly confirmed that the TPS was not in possession of the Applicant's property at the material time. If neither the TPS nor the OPP maintained custody, the only remaining authority is the RCMP. The 42-kilometer distance between the **Milton Detachment** and downtown Toronto is consistent with a federal "hand-off" of property to the 14th Division for the sole purpose of executing a tactical arrest.

XIII. TECHNICAL ANALYSIS OF THE FALSE INFORMATION PACKAGE: STRUCTURAL MUTILATION AND SDK ERRORS

30. A meticulous examination of the five-page **False Information Package** has revealed no fewer than 41 internal and external errors and inconsistencies. These defects are more consistent with police officers unfamiliar with court records management attempting to manufacture a judicial instrument than with the standard output of the Ontario Court of Justice.
31. **The Metadata Fingerprint:** Document metadata confirms that the **False Information Package** was generated using the **Mescius SDK** (GrapeCity.Documents.PDF.6.0.2.0). The utilization of this specific software development kit points to an unauthorized "cleanup" of the record within an enforcement environment.
32. **Evidence of Structural Mutilation:**
- **Page Count Anomaly:** The standardized Valid CCO Information Standard Form Package is comprised of six (6) pages. The document provided to the Applicant is truncated to five (5) pages.

- **Accent and Font Irregularities:** The document utilizes "accents graves" (è) instead of the requisite "accents aigus" (é) in the phrase "Ce document a été signé numériquement."
- **Footer Divergence:** The footer on page 2 of 5 is demonstrably different from the footers on pages 1 and 5. Furthermore, when printed in "save toner mode," only the page 2 footer remains legible, indicating it was "flattened" onto the document as a separate layer.
- **Jurat Displacement:** The jurat on page 2 of 5 is improperly located and legally impermissible, appearing on a separate page from the charges to which it purportedly pertains.

XIV. CHAMBERS – THE SECRET MISSION ARCHITECTURE: ALIGNMENT WITH FEDERAL ENFORCEMENT PARADIGMS

33. The unprecedented utilization of the Chief Justice's chambers for the authorization of the **Omnibus Endorsement** is a forensic signature of the RCMP's "Secret Mission" methodology. Based upon the volume and nature of warrants obtained by the RCMP across Ontario, their focus is consistently characterized by an extreme degree of operational secrecy and the deployment of unique, high-threshold instruments such as the **General Warrant** (Section 487.01 of the *Code*).
34. **The Stealth Doctrine:** Unlike municipal forces which operate through the normative Ontario Court of Justice (OCJ) intake, the RCMP frequently targets the Superior Court of Justice (SCJ) to secure warrants that grant broader, stealthier investigative powers. The authorization of a Section 487.01 instrument—which allows for the use of devices or investigative techniques that would otherwise violate Section 8 of the *Charter*—requires the oversight of a Judge, not a Justice of the Peace. This requirement aligns perfectly with the documented involvement of Chief Justice Morawetz.
35. **Corroboration of the "Army" Warning:** In June 2024, the Applicant’s Ex-Fiancée explicitly represented that an “army of complainants” was being mobilized against him. The subsequent execution of a covert, multi-jurisdictional enforcement maneuver in September 2024 serves as empirical corroboration that the state-aligned actors adopted an “end justifies the means” approach.

XV. PRECEDENTS OF FEDERAL ENFORCEMENT AND WARRANT ACQUISITION IN ONTARIO

36. The Royal Canadian Mounted Police (**Central Region**) regularly executes complex investigations in Ontario requiring specialized warrants from the SCJ. Recent and notable precedents establish a consistent pattern of high-threshold federal intervention:

Case / Operation	Temporal Context	Enforcement Action and Warrant Type
Cannabis Network (Ottawa)	March 10, 2026	Execution of residential search warrants dismantling a multi-million dollar distribution network ("Culture Cannabis Canada").

Synthetic Drug Lab (Norwich)	Jan / April 2026	RCMP Central Region dismantled a large clandestine lab following search warrants executed on January 24, 2026.
Gold Fraud / Forgery (RPX)	April 2026	Charges laid against a former CEO for alleged fraud and forgery following a federal probe.
Border Integrity (Pearson)	April 14, 2026	Seizure of fraudulent passports and subsequent charges against a Caledon resident.
National Security (GTA)	Late 2025	Arrests by INSET (Integrated National Security Enforcement Team) for participation in terrorist group activities.
Cameron Ortis Case	2018 - 2019	RCMP obtained a high-profile General Warrant from the SCJ, leading to a complex investigation and arrest.
Malware Investigations	2025 - 2026	Collaboration with the CRTC to execute search warrants at residences across the GTA targeting Remote Access Trojans (RAT).

XVI. THE TEMPORAL ANOMALY: THE PRE-EMPTIVE “2025” FEDERAL SURVEILLANCE FILE

37. The Court’s attention is urgently directed to a glaring chronological discrepancy within the RCMP's April 27, 2026, *Privacy Act* response. Despite explicitly acknowledging that the Applicant’s request was received on **March 12, 2026**, the RCMP unilaterally and inexplicably assigned the matter the file identifier **P-2025-16999** (the “**Pre-Emptive File ID**”).
38. **Nota Bene:** This is not a benign typographical error. In rigid federal records management protocols, the prefix denotes the exact year the file was opened or the data was aggregated. This temporal anomaly (the “**Chronological Discrepancy**”) strongly suggests that the RCMP had already initiated an active intelligence, audit, or surveillance file regarding the Applicant in **2025**—running in parallel with the Applicant's fierce civil litigation (NOM #2, NOM #3) in the *Divisional Court*.
39. The 2026 **Privacy Request** merely intersected with a pre-existing 2025 federal operation designed to monitor, manage, and contain the fallout from the unlawful September 2024 warrants. This destroys the premise that the RCMP was passively responding to a 2026 citizen inquiry; they were actively managing an ongoing 2025 crisis file regarding the Applicant. Automated federal sequential registry systems (the “**Sequential Registry**”) are immutable by design; the assignment of a 2025 prefix is an indelible digital artifact of pre-existing federal surveillance that predates the formal inquiry.

XVII. THE ADMITTED IMPLIED CONTRADICTION: THE SYLLOGISM OF ADMISSION UNDER SECTION 22(1)(b)

40. The institution's purported reliance upon the statutory exemption found within *Section 22(1)(b)* of the *Privacy Act* constitutes a devastating and self-incriminating paradox (the "**Devastating Contradiction**"). If the RCMP truly believed the matter to be an exclusively municipal Toronto Police Service investigation, the invocation of federal investigative exemptions would be a jurisprudential impossibility.

41. **THE SYLLOGISM OF ADMISSION:**

- **Major Premise:** *Section 22(1)(b)* is invoked exclusively to protect ongoing, active federal law enforcement investigations or intelligence critical to the institution.
- **Minor Premise:** The RCMP concurrently asserts it cannot disclose information "belonging to other police forces."
- **Conclusion:** Ergo, if the records the RCMP withheld under *Section 22(1)(b)* belonged to the TPS, the institution would have been statutorily compelled to issue a "No Records" response and redirect the Applicant to the TPS under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). By applying a federal exemption to protect records it *did* identify, the RCMP inherently and unavoidably admits that it considers the withheld information to be its own investigative material or critical to a joint federal operation in which it maintains primary agency.

42. This contradiction establishes that the extreme *ex parte* federal warrants were obtained from Chief Justice Morawetz, mathematically sanitized and forged by the RCMP using the **Mescius SDK** to obscure federal origins, and subsequently handed off to a local "Major Crimes" proxy (Detective Virani of the TPS) to execute under the guise of a municipal family-law dispute.

XVIII. JURISDICTIONAL DISTINCTION: MINISTERIAL DUTY VS. DISCRETIONARY REFUSAL

43. It is imperative to maintain a rigorous distinction between the **Ministerial Duty to Search** and the discretionary power to refuse access. The current impasse does not arise from a refusal to provide access to located records; rather, it arises from a fundamental failure to complete the search itself. A search that omits foundational metadata and the offline **PPU 005** repository is a legal nullity.
44. While the RCMP has applied certain redactions (a discretionary refusal of access), it has simultaneously failed to interrogate the specific Personal Information Banks requisitioned. This failure constitutes a breach of a mandatory ministerial duty, which is fundamentally distinct from the application of exemptions. Such a dereliction of duty validly triggers the Federal Court's jurisdiction for judicial review under a standard of correctness.

XIX. MANDATORY COMPLIANCE UNDER THE FEDERAL COURTS ACT AND PREROGATIVE REMEDIES

45. Pursuant to *Section 18* of the *Federal Courts Act*, R.S.C., 1985, c. F-7 (the "**FCA**"), the Federal Court possesses exclusive original jurisdiction to issue extraordinary remedies against federal boards and tribunals. The Applicant's requisition for foundational metadata and the retrieval of his physical property fall squarely within this jurisdictional mandate.

Statutory Timeframes and Jurisdictional Authority: Pursuant to *Section 18.1* of the **FCA**, the Applicant is required to take formal steps within thirty (30) days of the triggering administrative failure. Furthermore, *Section 18(1)* grants the Court the authority to issue:

- i. An **Injunction**;
- ii. A **Writ of Certiorari**;
- iii. A **Writ of Prohibition**;
- iv. A **Writ of Mandamus**; or
- v. **Declaratory Relief**.

47. In the present matter, the Applicant shall seek a mandatory injunction (*mandamus*) compelling the institution to satisfy its ministerial duty to search, alongside a declaration that the institution's current posture is a jurisdictional nullity.

XX. FINAL REQUISITION FOR IMMEDIATE CONFIRMATION OF SEARCH SCOPE

48. To respect the resources of the public and the *Federal Court of Canada*, the **Head of the Institution** is required to provide immediate confirmation regarding the scope of the search executed to date. The solution is elementary: conduct the requisite search—without further administrative prevarication—and provide the following **Foundational Metadata** (the “**Metadata Requisition**”):

- i. The **Originating Agency Identifier** (ORI);
- ii. The **Court Location** associated with the data entry;
- iii. The **Court Level** associated with the data entry;
- iv. The **Judicial Officer Name** input into the CPIC System; and
- v. The **Data Entry Numbers**, including terminal IDs and millisecond-accurate timestamps.

49. **Ultimatum:** The institution is further required to **Confirm or Deny** whether any manual amendments, MODIFY transactions, or supervisor overrides were executed post-input. **Kindly revert within twenty-four (24) hours of receipt of this electronic transmission but no later than end of day tomorrow (business day).**

XXI. RESERVATION OF RIGHTS REGARDING PHYSICAL PROPERTY

50. In relation to the physical property belonging to the Applicant—which evidence suggests is currently in the possession or under the control of the RCMP following the unlawful search of the **Residence**—the Applicant hereby reserves all legal rights. While the present focus remains upon statutory compliance with the *Privacy Act*, the extra-judicial deprivation of resources constitutes a parallel cause of action that shall be vigorously pursued.

51. As I appreciate the value of the resources of all levels of government, please provide a definitive response to the above by no later than the end of day tomorrow. While cases like *Gregory* demonstrate that a pattern of conduct of the federal institutions is to simply wait until the day of the hearing or a few days before to product records that were not disclosed, this situation is far different. I trust I will not need to demonstrate the distinction because of the fact, inter alia, that I am merely seeking very basic, personal information of my own, by

reference to the ORI, court level, court location, terminal ID and of course the confirmation in layman terms or plain English of the judicial officer. None of that information is not my own personal information and certainly not privileged from myself and nor could it be considered confidential post-arrest.

52. I appreciate when the likes of any police force is receiving complaints from persons like my ex-financee's mother, who to much of the shock of the TPS in October 2024, was misleading tribunals and being shut down with ease and I was successful although operating without a roof over my head (which must speak volumes) that they can be conned by such deceit. However, there is never a wrong time to do the right thing. Perhaps more analytically, the "access partnership" and our SCC binding authorities require a confirmed search and disclosure of personal information of mine of an originating police agency, a level of court, a court location and the name of a judge in an "Ex Parte In Camera Hearing". While the SCC has found that "Ex Parte In Camera Hearing" violation the likes of section 2(b) and 7, the violations are saved under section 1 of the Charter but only because those documents become publicly available post issuance of a process and/or an arrest.
53. I look forward to resolving the above with class and dignity and in a confidential manner but that will be dependent upon the response. As you have admitted, we are dealing specifically with my Charter and constitutional rights and if our democracy is to work with "Ex Parte In Camera Hearings", then we must follow binding precedents in our common law jurisdiction.
54. But there can never be any place in anything adversarial for that falsification of an information package in such fashion all predicated upon my exercising of my rights. Oddly, whomever did so I must thank for the leaving of certain data and metadata like the "C, L, M" for Court Officer (Toronto Region) Mrs. Frugoni-Rojas as GrapeCity.Documents for PDF (specifically that version) had bugs that caused that type of issue with those letters for The Honourable Chief Justice Morawetz particularly when his signature has in ink or image of formerly input ink signature.
55. It is a shame to be wasting these types of resources when my access request is so confined to the most basic of data, which only involves myself but the last 19 months, which I do not fault the RCMP for entirely or even perhaps minimally, is an assault to the Rule Of Law, our democracy and any semblance of legal order. For your reference, it appears there may have been a degree of hypocrisy at play—individuals levelling allegations of drug use while perhaps engaging in similar conduct themselves. I wish to clarify that my tattoos, which include the Ohm symbol and the Buckeye rendered in Chinese script as a tribute to my alma mater, Ohio State, are symbols of peace and harmony. I state this for your records: I undergo regular blood testing, and the only substances present are those for which I have a lawful prescription. Should you require confirmation, you may consult Sergeant Robert Black of the 14th Division, who, as I understand, was involved in distributing substances for which he lacked a prescription.
56. I reserve the right to draw this correspondence to the attention of any lawful body including a court in relation to any lawful purpose and costs if necessary.
57. I cordially remind all of their professional obligations including their obligations under any potential liability in relation to professional conduct statutes.

58. Should there not be any denial of the above, even a blanket denial, I will be entitled to presume that I am correct in substance in relation to the above and specifically in relation to the RCMP detachment at issue along with the RCMP's involvement.

59. I repeat and rely upon previous and time is of the essence.

60. Thank you kindly for time and consideration of the above, and I await to hear from you positively or negatively within the respectful deadline leaving aside the invalid time extension.

Sincerely,

/s/ Mr. Kevin A. McLean (BA, JD, CIM)

Mr. Kevin A. McLean (B.A., J.D., CIM)

Enclosures and attachments may follow on a piecemeal basis.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Tue, May 5, 2026 at 10:20 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

PRIVATE AND CONFIDENTIAL

DATE: May 5, 2026

DELIVERY METHOD: Via Secure Electronic Transmission and Registered Post

TO:

Mr. Michael Duheme, Commissioner, head of the institution (the "**Head of the Institution**")
Mr. Jeff Ball, Director, Privacy, access to information and privacy branch (the "**ATIP Directorate**")
Ms. Melissa Simpson, Delegate, ATIP Directorate

Royal Canadian Mounted Police

Mailstop #61, 73 Leikin Drive

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca, Jeff.Ball@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM) (the "**Applicant**")

REFERENCE I: *Privacy Act*, R.S.C. 1985, c. P-21 (the "*Privacy Act*"), Request P-2025-16999 / F339

Tab B

REFERENCE II: *Access to Information Act*, R.S.C. 1985, c. A-1 (the "*Access to Information Act*"), Concurrent Requisition Perfected May 5, 2026

SUBJECT I: Formal Demand for Statutory Adjudication Pursuant to Paragraph 8(2)(m) of the *Privacy Act*

SUBJECT II: The Jurisprudential Interplay Between Section 19 of the *Access to Information Act* and Section 8 of the *Privacy Act*

SUBJECT III: Exaction of a Public Interest Disclosure Pertaining to Jurisdictional Nullities and Algorithmic Spoliation

SUBJECT IV: The Truth-Searching Function of Litigation and the Preservation of the Public Record

Dear Commissioner Duheme, Director Ball, and Ms. Simpson:

I. INTRODUCTION AND THE CRYSTALLIZATION OF THE EVIDENTIARY RECORD

1. Correspondence is heretofore promulgated to formally elevate the extant access requisitions to the executive echelon, specifically compelling the Head of the Institution to execute a mandatory, non-delegable statutory duty. It is respectfully submitted that the incontrovertible discovery of systemic, algorithmically facilitated documentary fabrication—effectuated to deliberately bypass fundamental jurisdictional boundaries, circumvent established procedural safeguards, and fundamentally subvert judicial oversight—demands the immediate and uncompromising exaction of a public interest disclosure pursuant to paragraph 8(2)(m) of the *Privacy Act*.
2. *In limine*, it is formally confirmed that a concurrent, comprehensive requisition under the *Access to Information Act* was perfected and remitted via registered mail on May 5, 2026, accompanied by the prescribed statutory fee, which has been duly processed and catalogued. Said requisition specifically and meticulously targets the procurement, licensing, and national technology onboarding program (the "**NTOP**") integration of third-party developer libraries. Specifically, the requisition is engineered to extract architectural documentation pertaining to grape city documents pdf (the "**GrapeCity Documents PDF**") and mescius software development kits (the "**MESCIUS SDKs**").
3. The formal perfection of this concurrent requisition definitively bridges the previously insurmountable evidentiary chasm between the personal data historically requested and the highly sophisticated technological infrastructure utilized to orchestrate the jurisdictional nullity (the "**Jurisdictional Nullity**"). Consequently, the Head of the Institution is now unequivocally seized with the inescapable, paramount statutory obligation to render a formalized, written adjudication regarding the issuance of a public interest disclosure. It is asserted that this obligation is not merely procedural, but constitutes a substantive fiduciary duty owed to the Canadian populace to ensure the unassailable integrity of the federal law enforcement apparatus.
4. The gravity of this matter radically transcends an individualized administrative grievance; it inextricably implicates the overarching architectural integrity and cryptographic provenance of the entire federal law enforcement digital ecosystem. The potential deployment of enterprise-grade software development kits to execute headless, programmatic, and surreptitious alterations of judicial *acta* without triggering corresponding audit alerts constitutes a catastrophic systemic vulnerability of the highest magnitude. The citizenry relies implicitly and absolutely upon the foundational constitutional premise that the coercive apparatus of the state is anchored exclusively in unadulterated, lawfully procured judicial authorization. When this premise is technologically undermined and digitally metamorphosed, the ensuing crisis necessitates immediate, transparent executive intervention to restore the *status quo ante*.
5. The deployment of such advanced application programming interfaces within a restricted federal or provincial intranet environment facilitates a modality of documentary spoliation that remains entirely imperceptible to the standard user interface. By executing morphological alterations at the foundational hexadecimal level, state actors are afforded the illicit capacity to sanitize the provenance of legal instruments, thereby rendering the traditional mechanisms of legal scrutiny completely obsolete. The obfuscation of this capability represents an ongoing, active frustration of the *lex terrae* (the law of the land).

II. THE STATUTORY INTERPLAY: SECTION 19 OF THE ACCESS TO INFORMATION ACT AND SECTION 8 OF THE PRIVACY ACT

6. The legislative architecture of federal access and privacy law is inexorably intertwined, functioning as a seamless, integrated code meticulously engineered to ensure the absolute accountability of the administrative state. The concurrent filing of the aforementioned requisitions deliberately and strategically triggers this statutory interplay, forging a procedural nexus that the institution is legally prohibited from circumventing or artificially bifurcating.
7. Pursuant to subsection 19(1) of the *Access to Information Act*, the Head of the Institution is presumptively required to refuse the disclosure of any record containing personal information. However, this statutory prohibition is immediately and unequivocally subordinated to the overriding discretionary authority codified in paragraph 19(2)(c) of the *Access to Information Act*, which explicitly permits disclosure if it is in accordance with section 8 of the *Privacy Act*. This interconnected legislative framework is purposefully architected to prevent federal institutions from weaponizing localized privacy provisions to conceal widespread administrative malfeasance, technological spoliation, or systemic infrastructural failures.

8. By rigorous syllogistic extrapolation, the perfection of the *Access to Information Act* request concerning the GrapeCity Documents PDF infrastructure legally compels the Head of the Institution to concurrently and comprehensively evaluate the parameters of paragraph 8(2)(m)(i) of the *Privacy Act*. The public's unassailable right to scrutinize the procurement, configuration, security vetting, and operational deployment of enterprise software utilized for algorithmic forgery is inextricably linked to the exposure of the specific state actors responsible for executing the aforementioned forgery. To artificially bifurcate the technological mechanism of the forgery (the software) from the identities of the actors who operationalized it (the terminal users) would be to fundamentally frustrate the purposive interpretation of the governing legislation and to endorse a paradigm of unaccountability.
9. Furthermore, the harmonious interpretation of these companion statutes dictates that procurement transparency acts as an indispensable prerequisite to privacy accountability. The institutional integration of the MESCIUS SDKs—software inherently and specifically capable of altering backend metadata and maliciously manipulating Bezier-curve vectors within Portable Document Formats—necessitates profound public scrutiny. This scrutiny is elevated to an absolute constitutional necessity when such tools are implicated in the generation of a fabricated warrant that precipitated an unconstitutional deprivation of physical liberty. The concealment of such procurement logs operates *de facto* to shield the perpetrators of the forgery from appropriate judicial and public censure.

III. THE BIMODAL PARADIGM OF STATE-ACTOR MALFEASANCE AND THE SUBVERSION OF JURISDICTION

10. A meticulous forensic evaluation of the documentary metamorphosis (the "**Documentary Metamorphosis**")—wherein a legitimate, internal superior court intake endorsement was algorithmically crushed, violently stripped of its authenticating signatures, and digitally disfigured to generate a decoy provincial warrant—yields two mutually exclusive, yet equally catastrophic, operational paradigms. Irrespective of which paradigm represents the factual actuality, the necessity for an overarching public interest disclosure is rendered absolute and incontestable.
11. **Paradigm Alpha (Federal Culpability):** The algorithmic spoliation, vector morphology collapse, and the insidious insertion of the "CL (M)" digital artifact were directly facilitated by the Royal Canadian Mounted Police through the utilization of its own procured, server-side GrapeCity Documents PDF rendering engines seamlessly integrated within the Canadian police information centre (the "**Canadian Police Information Centre**") architecture. Under this paradigm, the federal repository—the ostensible "Single Source of Truth" for Canadian law enforcement—is actively operating as the crucible for documentary forgery, effectively transmuting lawful judicial commands into unconstitutional, fraudulent mandates. Such a paradigm suggests a catastrophic failure of the federal gatekeeping function (*custos morum*), wherein the very system designed to protect the public is utilized to fabricate the authority to detain it.
12. **Paradigm Beta (Provincial/Municipal Culpability):** An external originating agency, specifically the Toronto police service (the "**Toronto Police Service**"), orchestrated the digital forgery through its localized infrastructure prior to transmitting the corrupted data to the federal mainframe. Consequently, the Canadian Police Information Centre is presently harbouring, preserving, and actively deploying a fabricated instrument to effectuate arbitrary detentions across the national jurisdiction, serving as a passive, yet legally culpable, conduit for a provincial jurisdictional subversion. The failure of the federal apparatus to detect, intercept, or subsequently purge this fabricated instrument implicates the federal custodian in the perpetuation of the nullity.
13. In either paradigm, a foundational court document required to effectuate the lawful, statutorily mandated transfer of jurisdiction from the originating courthouse (the "**Originating Courthouse**") to the transferee courthouse, specifically the Ontario Court of Justice located at 10 Armoury Street (the "**Transferee Courthouse**"), was technologically manipulated to deceive the judiciary, the prosecutorial apparatus, and the citizenry alike. The systemic integration of an absolute nullity into the national law enforcement repository constitutes an existential threat to the administration of justice. The creation of such a document operates in direct, unyielding contravention of the foundational maxim *ex nihilo nihil fit* (out of nothing comes nothing); a fabricated mandate cannot spontaneously generate lawful executive authority, nor can the state synthetically manufacture jurisdiction where the judiciary has explicitly and deliberately withheld it.
14. **Nota Bene (Counter-Argument and Rebuttal regarding Originator Control):** Anticipating the institutional counter-postulation that the Royal Canadian Mounted Police is absolved of disclosure obligations under the doctrine of originator control should Paradigm Beta be factual, such an assertion is preemptively and fundamentally dismantled *in limine*. The federal governance authority retains absolute, incontrovertible custody and control over the hexadecimal metadata transaction logs housed securely within its own mainframe architecture. The *Privacy Act* does not permit a federal institution to utilize inter-jurisdictional deference or bureaucratic silos as a prophylactic shield to conceal the contamination of the national database by municipal actors. The federal custodian owes an overarching, non-delegable fiduciary duty to the Canadian public to ensure that its systems are not utilized to propagate fraudulent instruments. The public interest in maintaining the structural integrity of the federal mainframe clearly and overwhelmingly outweighs the

bureaucratic courtesy historically extended to a municipal police service engaged in the promulgation of a complete nullity.

IV. THE JURISPRUDENTIAL IMPERATIVE FOR PUBLIC INTEREST DISCLOSURE AND THE TRUTH-SEARCHING FUNCTION

15. The exercise of executive discretion pursuant to paragraph 8(2)(m) of the *Privacy Act* is decidedly not a passive privilege; it is a mandatory, judicially reviewable obligation that must be actively and vigorously engaged. The ensuing jurisprudential framework unequivocally establishes that the balance of convenience in the present matter heavily, unmistakably, and overwhelmingly favours immediate, unredacted public disclosure.
16. The foundational parameters for evaluating transparency against privacy were definitively codified by the Supreme Court of Canada in *Dagg v. Canada (Minister of Finance)*, 1992 SCR 403 (the "*Dagg Jurisprudence*"). In the *Dagg Jurisprudence*, the apex court established that the discretionary decision of an institutional head under paragraph 8(2)(m)(i) is subject to an abuse of discretion standard, stipulating that the discretion must be exercised in utmost good faith (*uberrima fides*) and entirely without reliance upon irrelevant factors.
 - **Application of the Law to the Facts:** The withholding of metadata that mathematically proves the algorithmic falsification of a judicial warrant, motivated by an institutional desire to avoid public embarrassment, circumvent civil liability, or shield the professional identities of malfeasant state actors, constitutes an egregious reliance upon irrelevant factors and a profound breach of *uberrima fides*. Administrative discretion cannot lawfully be exercised to ratify an unconstitutional deprivation of liberty or to conceal the mechanism of that deprivation.
17. The Federal Court of Appeal, in *Canadian Broadcasting Corporation v. Canada (Parole Board)*, 2023 FCA 161 (the "*CBC Jurisprudence*"), further refined this obligation, decreeing that administrative bodies must execute a meticulous, case-specific weighing of interests rather than applying monolithic, blanket policies. Furthermore, the *CBC Jurisprudence* explicitly acknowledges that paragraph 8(2)(m)(i) operates as a rare statutory locus wherein the requester's overarching motive is highly relevant to determining the magnitude of the public interest.
 - **Application of the Law to the Facts:** The Royal Canadian Mounted Police is legally precluded from applying a generic, blanket law enforcement exemption to the requested logs. The specific motive herein is the pursuit of absolute transparency, the exposure of a technological subversion of the *Canadian Charter of Rights and Freedoms*, and the preservation of the sanctity of the public court record. This *bona fide* public interest motive is incontrovertibly substantiated by the formal institution of constitutional proceedings before the Superior Court of Justice. Specifically, a form 1 notice of application (the "**Form 1 Notice of Application**"), a form 5 notice of application and constitutional issue (the "**Form 5 Notice of Application and Constitutional Issue**"), and a form 22 requisition (the "**Form 22 Requisition**") were perfected and formally served upon the Attorney General of Canada (the "**Attorney General of Canada**") and the Attorney General of Ontario (the "**Attorney General of Ontario**") on April 29, 2026. The formal engagement of the primary law officers of the Crown irrevocably transfigures this requisition from a localized administrative inquiry into a matter of paramount national legal consequence. Litigation functions as an immutable, truth-searching crucible; it relies entirely upon the unadulterated provenance of documentary evidence. Justice is decidedly not devoid of profound financial and societal costs. Accordingly, the optimization and efficiency of public resources strictly mandate that the federal governance authority preemptively disclose the unadulterated hexadecimal metadata. Such proactive disclosure unequivocally averts the protracted, wasteful expenditure of prosecutorial and judicial resources upon the adjudication of jurisdictional nullities, thereby honouring the foundational principle of *fiat justitia ruat caelum* (let justice be done though the heavens fall).
18. **Nota Bene (Counter-Argument and Rebuttal regarding Sub Judice):** Anticipating the institutional objection that the active filings before the Superior Court of Justice render the matter *sub judice*, thereby theoretically precluding administrative disclosure, such an assertion is conceptually vacuous and legally untenable. The *sub judice* doctrine does not suspend the operation of the *Privacy Act* nor extinguish the statutory authority enshrined within paragraph 8(2)(m). The disclosure of raw, hexadecimal metadata constitutes a purely factual, administrative execution; it does not represent an adjudication of the constitutional merits presently pending before the tribunal. On the contrary, it synergizes directly with the truth-seeking function of the court, ensuring the tribunal, specifically defined herein as the Ontario Court of Justice or the Superior Court of Justice (the "**Tribunal**"), is not subjected to a perpetuation of fraud upon the court. The *sub judice* rule is architecturally designed to protect the administration of justice from external prejudice, not to shield the state from disclosing the very administrative metadata required by the Tribunal to ascertain its own jurisdiction. Furthermore, the deliberate suppression of exculpatory or clarifying metadata whilst the Attorney General of Canada and the Attorney General of Ontario are actively seized of the constitutional questions verges perilously upon the frustration of the Crown's own overarching mandate (*parens patriae*) to ensure that justice is administered with absolute probity. The suppression of such data under the guise of pending litigation would constitute a

direct obstruction of the very relief sought by the Applicant and a flagrant violation of the Crown's fundamental duty of fairness.

19. In *Attaran v. Canada (National Defence)*, 2011 FC 334 (the "*Attaran Jurisprudence*"), the Federal Court grappled with the complex intersection of state transparency and individual privacy rights concerning the treatment of detainees. The court recognized the profound public interest in illuminating the mechanisms of state-sanctioned detention, asserting that the public possesses a fundamental democratic right to scrutinize the apparatus of state coercion.
 - **Application of the Law to the Facts:** The present matter transcends the mere treatment of detainees; it strikes at the fundamental legitimacy of the detention mechanism itself. If the public interest dictates transparency in how the state treats individuals in custody, it *a fortiori* dictates absolute transparency when the state utilizes commercial software to forge the very instrument authorizing the individual to be taken into custody. The algorithmic spoliation of a warrant is a profound violence against the legal rights of the detainee, demanding the highest echelon of transparency to ensure that the coercive power of the state is not deployed arbitrarily.
20. The necessity for systemic transparency is further fortified by *Pinaymootang First Nation v. Canada (Minister of Health)*, 2009 FC 275 (the "*Pinaymootang Jurisprudence*"), wherein the Federal Court determined that the overarching public interest in the structural integrity and transparency of federal programs conclusively outweighed potential individual privacy harms.
 - **Application of the Law to the Facts:** The Canadian Police Information Centre represents the most consequential federal program within the criminal justice matrix. The public possesses an absolute, overriding interest in verifying whether this system has been structurally compromised by the insertion of irregular, unsworn *acta*. The potential chilling effect upon the populace—operating under the apprehension that digital records may be retroactively manipulated to justify unlawful arrests—creates an urgent, inescapable imperative for the Head of the Institution to act decisively. The obfuscation of this data enables a mosaic of fraud to permanently solidify within the public record.
21. **Nota Bene (Counter-Argument and Rebuttal regarding the Right to Compel):** It is acknowledged that in *Bangladesh v. Canada (Attorney General)*, 2019 FC 399 (the "*Bangladesh Jurisprudence*"), the Federal Court observed that paragraph 8(2)(m)(i) does not inherently grant a third-party requester a coercive, stand-alone legal right to *compel* disclosure via mandamus if the institution reasonably exercises its discretion negatively. However, any institutional reliance upon the *Bangladesh Jurisprudence* to justify an arbitrary refusal is fundamentally misplaced and legally deficient. The Applicant herein is the direct data subject—not a disconnected third party. Furthermore, while the court cannot arbitrarily substitute its own decision for that of the institutional head, the Head of the Institution remains strictly, legally bound to *perform* the case-specific weighing process. A refusal to deeply consider the irrefutable evidence of algorithmic forgery, or a decision prioritizing the anonymity of forgers over the constitutional liberty of the citizenry, would unequivocally fail the standard of reasonableness, violate the tenets of administrative fairness, and invite immediate judicial repudiation.

V. THE INEVITABILITY OF A JURISDICTIONAL NULLITY AND THE VITIATION OF AUTHORITY

22. It is systematically reiterated that the documentary defect identified herein cannot be jurisprudentially salvaged, ameliorated, or retroactively cured. The algorithmic obliteration of a Superior Court Chief Justice's signature, deliberately orchestrated through the deployment of the GrapeCity Documents PDF software, is decidedly not a mere administrative irregularity or curable clerical omission (such as those contemplated under section 599 of the *Criminal Code*). This deliberate mutilation of the court record—manifesting precisely as the DOC-6507 whitespace bug and the subsequent "CL (M)" artifact—is an irremediable nullity that permanently and violently destroys the cryptographic provenance of the document.
23. The deployment of a fabricated mandate to effectuate the physical transportation and imprisonment of a citizen violates the foundational maxim *factum a iudice, quod ad officium jure non pertinet, ratum non est* (an act of a judge which does not pertain to their office is of no legal force). Consequently, the entire trajectory of the resulting detention is unequivocally *coram non iudice*. To assert that lawful jurisdiction can be procured via documentary spoliation is to violently offend the principle of *nemo dat quod non habet* (no one gives what they do not have); the Transferee Courthouse possessed no lawful jurisdiction, as absolutely none was legitimately conveyed by the Originating Courthouse. The resulting proceedings are fundamentally hollow, entirely bereft of any anchoring in lawful judicial authority.
24. Furthermore, the deliberate subversion of the judicial architecture to procure a deprivation of liberty irrevocably taints the proceeding in its entirety. Pursuant to the doctrine of *fraus omnia corrumpit* (fraud vitiates everything), the Royal Canadian Mounted Police cannot lawfully invoke any statutory exemption under either the *Access to Information Act* or the *Privacy Act* to shield the metadata constituting the evidentiary footprint of this fraud. Fraud unravels all subsequent administrative processes back to the very moment of inception, vitiating any claim to operational privilege or third-party privacy.
25. The institutional failure to recognize this document as an absolute nullity, and the continued administrative prevarication regarding the unredacted release of the underlying hexadecimal logs, verges perilously upon institutional complicity in the preservation of a fabricated state action. It fundamentally deprives the citizenry of the protections enshrined within the maxim *audi alteram partem* (listen to the other side), as a fair hearing is

rendered intellectually and legally impossible when the foundational documents presented by the Crown are a technological mirage. The state cannot lawfully demand answering from an accused when the state itself has orchestrated a sophisticated, algorithmic deception upon the Tribunal.

VI. FORMAL DEMAND AND CONCLUSION

26. In light of the unprecedented factual matrix presented, the concurrent perfection of the *Access to Information Act* requisition, the formal institution of constitutional proceedings before the Superior Court of Justice, the formal service upon the primary law officers of the Crown, and the binding jurisprudential frameworks delineated herein, it is formally demanded that the Commissioner of the Royal Canadian Mounted Police, acting in the capacity of the Head of the Institution, execute the following non-delegable imperatives:
 - a. Actively and meticulously evaluate the evidentiary record demonstrating the algorithmic manipulation of a court document utilized to unlawfully effectuate a jurisdictional transfer from the Originating Courthouse to the Transferee Courthouse.
 - b. Formally adjudicate whether a public interest disclosure pursuant to paragraph 8(2)(m) of the *Privacy Act* shall be issued to notify the Canadian public of the systemic vulnerabilities and unauthorized technological alterations occurring within the national law enforcement repository.
 - c. Provide a formalized, written decision detailing the rationale of the aforementioned adjudication, specifically addressing the rigorous balancing test mandated by the *Dagg Jurisprudence* and the paramount relevance of the truth-searching motive as necessitated by the *CBC Jurisprudence*.
 - d. Institute an immediate, comprehensive litigation hold to ensure the absolute preservation of all procurement logs, software deployment histories, and raw hexadecimal transaction records pertaining to the *Canadian Police Information Centre* and the integration of the aforementioned software development kits, thereby preventing any further digital spoliation.
27. The citizenry possesses an inalienable constitutional entitlement to ascertain whether the coercive apparatus of the state is governed by the rule of law or maliciously manipulated by the algorithmic whims of enterprise software. It is respectfully submitted that the immediate exaction of a public interest disclosure, in tandem with the unredacted release of the requested hexadecimal records, is the *sine qua non* for the restoration of public confidence in the Canadian Police Information Centre and the preservation of the *status quo ante*.
28. Formal notice is hereby registered that the persistent institutional refusal to adjudicate this matter *uberrima fides*, or to disclose the raw hexadecimal transaction logs, shall precipitate immediate, forceful escalation. Said escalation will encompass the pursuit of a writ of *mandamus* before the Federal Court of Canada to legally compel the performance of this overarching statutory duty, accompanied by an uncompromising demand for elevated, punitive, and solicitor-and-client costs. Such costs shall be directly predicated upon the institution's *mala fides* obstruction of justice and its calculated frustration of the overarching truth-searching function.
29. Furthermore, whilst the Applicant maintains an unequivocal and resolute disagreement with the unilateral temporal extension purportedly secured by the Royal Canadian Mounted Police, it is conceded that the Applicant is not the final arbiter regarding the administrative validity of such an extension; accordingly, any formal grievance pertaining to the procedural irregularity of said delay is deferred to a subsequent forum and is a matter to be addressed on a separate day. Nevertheless, even if one were to proceed upon the tenuous assumption that the institution's invocation of a time extension was legally permissible, it is forcefully submitted that the statutory imperative for a decision regarding the public interest disclosure remains exigible *instante*, and categorically no later than sixty (60) days from the inception of the request on March 11, 2026.

All of which is respectfully submitted.

(Original electronically signed)

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Tab C

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Mon, May 4, 2026 at 7:46 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

PRIVATE AND CONFIDENTIAL

DATE: May 4, 2026

DELIVERY METHOD: Via Secure Electronic Transmission

TO: Mr. Jeff Ball, Director, Privacy

Access to Information and Privacy Branch

Digital Program

Royal Canadian Mounted Police

Mailstop #61, 73 Leikin Drive

Ottawa, Ontario K1A 0R2

CC: Ms. Melissa Simpson (and/or Assigned Delegate), ATIP Branch

CC: Julie Worrell, ATIP Branch

CC: Mr. Michael Duheme, Commissioner, Royal Canadian Mounted Police

REFERENCE I: RCMP ATIP File P-2025-16999

REFERENCE II: OPCC Complaint File PA-073854 (Formalized April 19, 2026; Supplemented April 22, 2026)

REFERENCE III: Electronic Transmission from Director Jeff Ball, dated May 1, 2026

SUBJECT I: Categorical Rejection of the May 1, 2026 Communication and the Abdication of the Statutory Duty to Assist

SUBJECT II: Immediate Demand for Administrative Clarification Regarding the Precise Taxonomy of Released Records

SUBJECT III: Formal Notice of Impending Escalation to the Civilian Review and Complaints Commission (CRCC)

SUBJECT IV: Notice of Mandamus with Costs, the Office of the Auditor General (OAG), and Section 8(2)(m) Disclosures

Dear Director Ball, Ms. Simpson, Ms. Worrell, and Commissioner Duheme:

1. INTRODUCTION AND THE REJECTION OF ADMINISTRATIVE DEFLECTION

1.1. Correspondence is heretofore promulgated in direct, immediate, and unyielding response to the electronic transmission authored by Director Jeff Ball on May 1, 2026, concerning access requisition P-2025-16999. It is explicitly recorded *in limine* that the institutional posture advanced within said communication is formally, legally, and forensically rejected as fundamentally deficient and profoundly violative of the statutorily mandated access partnership.

1.2. It is formally recorded that the apologies tendered within the May 1, 2026 correspondence concerning administrative "delays" are entirely unnecessary and are hereby eschewed. There is presently no active grievance or formal complaint being advanced in relation to the mere tardiness of your recent response; rather, the profound and continuing issue is the substantive failure of the RCMP (the "**Institution**") to execute the explicitly requested search and its subsequent refusal to articulate the precise nature of the documents it *did* provide.

1.3. Director Ball, it is respectfully submitted that the Institution is presently operating under a profound jurisdictional and administrative misapprehension. Your assertion that the Institution has "processed the request in accordance to the *Privacy Act*" is legally incompatible with the documentary reality. Furthermore, your explicit directive that any subsequent concerns

must be addressed exclusively through the pending office of the privacy commissioner of Canada (the "OPCC") complaint constitutes an impermissible administrative deflection. The OPCC exists as an appellate oversight body; its involvement does not grant the Institution a bureaucratic license to summarily wash its hands of an active access requisition, nor does it extinguish the Institution's ongoing, non-delegable duty to assist the requestor in understanding the records released.

2. THE DEMAND FOR CLARIFICATION AND THE FORENSIC TAXONOMY OF RECORDS

2.1. The immediate purpose of this correspondence is to compel a basic administrative clarification regarding the three-page release package previously provided by your directorate. The provided documentation is patently unclear upon its face—a profound deficiency that ironically mirrors the severe irregularities observed upon the face of the impugned municipal court documentation (the vitiated "Information Package," page three of five, previously provided to you to demonstrate the necessity of this exaction).

2.2. As explicitly delineated in antecedent correspondence, the requested data encompasses three distinct forensic strata. To ensure there remains absolutely no further administrative obfuscation, these strata are reiterated hereunder:

- **Level 1: Active Warrant Status** (Routine queries of the active Canadian police information centre (the "CPIC") main database, accessible by localized law enforcement);
- **Level 2: Foundational Metadata** (Systemic transactional logs, Originating Agency Identifiers, and terminal IDs housed within personal information bank RCMP Personal Information Bank 005, requiring specialized administrative extraction);
- **Level 3: Offline Metadata / Amended Data** (Hexadecimal dumps and historic records residing within the insulated offline historical database, detailing original inputs and subsequent structural alterations).

2.3. You are hereby formally compelled to advise, unequivocally, whether the three-page document you previously provided includes Level 2 and Level 3 data, or if it is restricted entirely to Level 1. A simple, binary confirmation or denial is required today. It is an inescapable logical and procedural prerequisite that I must understand what the Institution *claims* to have provided before the broader legal issues of non-disclosure can be adjudicated.

2.4. As extensively articulated in prior submissions, it is my legally grounded position that a failure to conduct the explicitly requested Offline Search constitutes a breach of an executory and ministerial duty. This failure is procedurally and jurisprudentially distinct from a statutory refusal to disclose located personal information pursuant to an enumerated exemption. The Institution cannot lawfully invoke statutory exemptions to refuse that which it has not searched for *per se*. The OPCC's investigative framework inherently recognizes this fundamental dichotomy; a failure to search is not synonymous with a refusal to disclose. Your prompt clarification regarding the scope of the search actually conducted will directly inform the trajectory of the ensuing litigation, setting the foundation for a writ of *mandamus* to compel the unperformed ministerial duty.

3. DECONSTRUCTION OF STATUTORY EXEMPTIONS AND PROCEDURAL INVALIDITY

The Procedural Invalidity of Blanket Exemptions and the Failure to Particularize

3.1. Notwithstanding the execution of an entirely irrelevant search methodology, the Final Response paradoxically asserts that "some of the information has been exempted pursuant to sections 19(1)(d), 22(1)(b) and 26 of the Act." It is respectfully submitted that the Institution's mechanical recitation of these provisions constitutes a profound procedural failure and a breach of the duty to provide adequate reasons.

3.2. Pursuant to established administrative law principles and the Treasury Board of Canada Secretariat (TBS) Directives governing privacy practices, an institution cannot merely list statutory exemptions in a vacuum. It is legally required to particularize the redactions, explicitly correlating specific statutory exemptions to the precise data fields, categories, or text being severed from the record. Furthermore, the Institution is obligated to identify the specific Personal Information Bank (PIB) from which the withheld records were drawn. To issue a completely opaque three-page printout while simultaneously invoking a blanket list of exemptions—without specifying which exemption applies to which invisible piece of data, or confirming the PIB—is procedurally repugnant. This deliberate obfuscation completely frustrates the Applicant's quasi-constitutional right to comprehend and effectively challenge the specific rationale for each refusal.

The Misapplication of Section 19(1)(d): Originator Control and the Stewardship Doctrine

3.3. The Institution's reliance upon paragraph 19(1)(d) of the *Privacy Act*—asserting that the personal information was obtained in confidence from a municipal or regional government—is fundamentally dismantled by established OPCC and provincial privacy jurisprudence. The Institution is attempting to weaponize the bureaucratic principle of originator control to completely abdicate its overarching statutory responsibilities as the central federal database architect.

3.4. As the host and paramount administrator of the CPIC network, the RCMP exercises absolute "control" over the systemic infrastructure and the Offline Historical Database. This paradigm of absolute federal control is decisively reinforced by the Information and Privacy Commissioner of Ontario in *Order MO-4542* (Halton Regional Police Services Board). In that binding precedent, the adjudicator ruled unequivocally that municipal police forces do *not* have custody or control over the broader CPIC database inquiries or the systemic records generated by other services within the national architecture. By necessary legal corollary, that statutory control vests exclusively, solely, and incontrovertibly with the federal host—the RCMP. The Institution cannot legally disavow the contents of its own digital ledger by deflecting responsibility to municipal entities.

The Misapplication of Section 22(1)(b): The Functus Officio Doctrine and Historical Acta

3.5. The invocation of paragraph 22(1)(b) of the *Privacy Act*—premised upon the assertion that disclosure could reasonably be expected to be injurious to the enforcement of any law or the conduct of lawful investigations—is rendered entirely moot by the passage of time and the definitive conclusion of the operational event.

3.6. The physical apprehension of the subject was effectuated on October 2, 2024. The custodial phase has entirely culminated. At the exact moment of execution and subsequent release, the authorizing judicial officer became definitively *functus officio*, and the operational, investigatory imperative of the warrant was eternally exhausted. The requested Transaction Logs and offline metadata do not contain active investigative techniques; they contain purely historical, immutable administrative facts regarding a concluded judicial authorization. There exists absolutely no ongoing investigation that could conceivably be prejudiced by the disclosure of a specific digital timestamp. To allow section 22 to cover executed warrants indefinitely is to establish a secret police ledger, anathema to the *Canadian Charter of Rights and Freedoms*.

The Misapplication of Section 26: State Actors and the Public Domain

3.7. The Institution's reliance upon section 26 of the *Privacy Act* to withhold the identities of third parties—presumably the names of the presiding judicial officers, swearing special constables, and inputting terminal operators—constitutes a gross misinterpretation of Canadian privacy law.

3.8. The jurisprudential parameters established by the Supreme Court of Canada, notably in *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25, definitively dictate that the professional identities and operational titles of public servants and state actors executing official, remunerated public functions do not attract the elevated privacy protections afforded to the intimate biographical details of private citizens. When an individual exercises the coercive power of the state, they inherently surrender the expectation of privacy regarding the execution of that specific power. Their professional identities, within the specific context of those official actions, are entirely within the public domain.

4. SECTION 8(2)(m) PUBLIC INTEREST OVERRIDE AND THE COMMISSIONER'S MANDATE

4.1. Commissioner Duheme, acting in the capacity of the Head of the Institution, shall remain perpetually copied on this and all subsequent correspondence pertaining to this matter. There remains a live, pressing, and unresolved constitutional issue regarding whether the Head of the Institution is statutorily compelled to unilaterally disclose to the public the relevant metadata contained herein, pursuant to the paramount public interest override codified in paragraph 8(2)(m) of the *Privacy Act*.

4.2. The systemic metamorphosis, retroactive generation, or inter-jurisdictional manipulation of coercive judicial authorizations constitutes a profound, existential threat to the administration of justice and the foundational tenets of the *Canadian Charter of Rights and Freedoms*. The necessity of exposing the unvarnished systemic metadata governing these authorizations clearly and unequivocally outweighs any residual institutional or personal privacy interests possessed by the state actors involved. The Commissioner cannot remain willfully blind to the institutional suppression of data that could expose documentary fraud within the national law enforcement database.

5. OAG INVOCATION, CRCC ESCALATION, AND NOTICE OF MANDAMUS WITH COSTS

281 5.1. **Formal Notice of CRCC Escalation:** Please be formally advised that the deliberate execution of a mathematically doomed "live query" to evade the explicit parameters of an offline database search transcends a mere administrative dispute; it constitutes actionable personnel misconduct. The intentional subversion of a citizen's quasi-constitutional access rights by the ATIP personnel involved (including, but not limited to, the terminal operator and supervising directors) forms the explicit grounds for an impending, formal complaint to the Civilian Review and Complaints Commission (the "**CRCC**"). The CRCC will be engaged to independently investigate the specific *conduct* of the RCMP members who actively participated in this systemic obfuscation.

5.2. **The Office of the Auditor General:** It is my considered legal view that the compounding administrative failures, the deployment of illogical search methodologies, the invocation of blanket exemptions to non-responsive documents, and the present refusal to articulate the basic nature of the released records elevate this matter to a threshold of systemic dysfunction. It is formally recorded that the Office of the Auditor General of Canada (the "**OAG**") has already acknowledged receipt of the intelligence regarding these profound CPIC vulnerabilities and is actively considering a systemic audit based upon this information. The Institution's current refusal to provide the requested transaction logs will be formally presented to the OAG as active evidence of the RCMP's ongoing structural failure to maintain database integrity.

5.3. **Deadline and Notice of Mandamus with Costs:** You are hereby formally compelled to confirm or deny whether the provided package includes the foundational metadata (Level 2) and the offline searches (Level 3) by **no later than the close of business today**. Should the Institution remain unwilling to confirm or deny the scope of its own search, a separate, independent ground for judicial review is immediately established.

5.4. If the Institution fails to respond by the close of business today, or refuses to confirm the scope of its search, an immediate application for a writ of *mandamus* will be aggressively pursued before the Federal Court of Canada. This application will forcefully compel the RCMP to perform its strict ministerial duty. Furthermore, given the bad-faith deflection, the evasion of the statutory search parameters, and the necessity of this escalation, this judicial review will be accompanied by a forceful demand for punitive, solicitor-and-client costs against the Institution.

All of which is respectfully submitted.

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

Tab D

Good day Mr. McLean,

I apologize for the delay getting back to your email.

Please be advised that I can confirm that we have processed your request in accordance to the Privacy Act. Given there is an ongoing complaint with the Office of the Privacy Commissioner (OPC) any concerns you have should continue be addressed through them and we will respond accordingly as the OPC complaint is pursued and any direction is provided.

Jeff Ball

Director Privacy

Access to Information and Privacy Branch

Digital Program

Royal Canadian Mounted Police

Jeff.Ball@rcmp-grc.gc.ca

Cell: 343-571-6721

Jeff Ball

Directeur protection des renseignements personnels

Sous-Direction de l'accès à l'information et la protection des renseignements personnels

Programme Numérique

Gendarmerie royale du Canada

Jeff.Ball@rcmp-grc.gc.ca

Céll: 343-571-6721

From: Mr. Kevin McLean <mcleansettlement@gmail.com>

Sent: April 29, 2026 10:05 AM

To: Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>

Cc: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>; Simpson, Melissa (RCMP/GRC) <Melissa.Simpson@rcmp-grc.gc.ca>; Brisson, Stéphane (RCMP/GRC) <Stephane.Brisson@rcmp-grc.gc.ca>; Worrell, Julie (RCMP/GRC) <Julie.Worrell@rcmp-grc.gc.ca>; Duheme, Michael (RCMP/GRC) <Michael.Duheme@rcmp-grc.gc.ca>; Mirsky, Tanya (RCMP/GRC) <Tanya.Mirsky@rcmp-grc.gc.ca>

Subject: Re: Privacy Act request P-2025-16999 / F339, Your File N/A, Acknowledgment

April 29, 2026

To: Jeff Ball, Director of Privacy, RCMP ATIP Branch (Jeff.Ball@rcmp-grc.gc.ca)

CC: [Original Recipients]

Subject: Re: Privacy Request P-2025-16999 - Notice of Incomplete Disclosure and Query for Clarification

Dear Mr. Ball et al

Thank you for your correspondence of April 28, 2026. While I appreciate the acknowledgment of the delays and the quasi-constitutional nature of my privacy rights, your response is not substantive or responsive to the core issue: the provided release package is fundamentally insufficient to meet the

Tab E

specific parameters of my request or does not explain what is contained therein per se. While the letter references alleged statutory exceptions under the Privacy Act, it does not specify what is contained in the attachment. Kindly particularize regarding the same.

My request of March 11, 2026 (see: Canada Post confirmation) was **not** for a routine CPIC "live" query. It was an explicit demand for an **Offline Search of the Offline Historical Database** to retrieve forensic artifacts, including transaction logs, hexadecimal dumps, and millisecond-accurate metadata. **As such, if the response provided was for that data and information, it is not responsive to my access request. However, your clarification will assist in any event.**

To ensure there is no further misunderstanding, I have categorized the requested data into three distinct levels:

Table 1: Three Levels of Requested Personal Information

#	Data Type	Primary Source	Status in P-2025-16999
1	Active Warrant Status	CPIC "Persons" File (Routine Query)	Provided (3 pages)
2	Foundational Metadata	Transaction Logs (PPU 005), ORI, Terminal IDs	Yes or no?
3	Amended/Purged Data	Hexadecimal Dumps & Offline Search (Specialized Mainframe Interrogation)	Yes or no?

The three-page package provided on April 27, 2026, appears to be limited exclusively to **Level 1** (Active Status). Specifically, Page 2 of your release states "**NOT ON FILE** PERSON LOG," which indicates a failure to interrogate the **Offline Historical Database** as requested. Kindly confirm or deny whether that is correct.

I require a direct response to the following query by the end of the day:

1. Did the search conducted for P-2025-16999 include an interrogation of the **Offline Historical Database** for Level 2 and Level 3 data (Transaction Logs and Hexadecimal Dumps)?
2. Please provide a "Yes" or "No" confirmation as to whether the RCMP considers the "Foundational Metadata" and "Amended/Purged Data" described above to be "not on file," or if these sources were simply not searched.

You suggested that I pursue further complaints with the OPC. However, a complaint cannot be properly investigated with a potential report until the RCMP clarifies whether it has actually performed the specific search requested or is refusing to do so. I refer you to section 41 of the Privacy Act in this regard and the narrow scope of the same.

I look forward to your immediate clarification, **no later than the end of the business day.**

Sincerely,

Mr. Kevin A. McLean (BA, JD, CIM)

APPENDIX

From previous correspondence with RCMP Privacy Division (ease of reference)

#	Data Type	Primary Source	Level of Effort	Forensic Value
1	Active Warrant Status	CPIC "Persons" File	Low (Routine Query)	Operational only
2	Foundational Metadata (ORI, Terminal ID)	Transaction Logs (PPU 005)	Moderate (Requires Audit)	Identifies the genesis of the record
3	Amended/Purged Data (The "Frankendoc" history)	Hexadecimal Dumps & Offline Search	High (Specialized Mainframe Interrogation)	Proves "vector collapse" and unauthorized changes

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)
Chartered Investment Manager
Email: mcleansettlement@gmail.com
Fax: 416.981.7117
Phone number: 647.370.9354

On Tue, Apr 28, 2026 at 5:37 PM Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca> wrote:

Good day Mr. McLean

I would like to thank you for following up on your Privacy Request (P-2025-16999). As you noted in your exchange with the RCMP ATIP team, requests and access are quasi-constitutional and your due diligence in following up with us has been important in exercising

Tab F

those rights.

I would like to re-iterate and re-extend our apologies for the delays related to your request. As the team continues to navigate higher than normal priority requests, such as yours, we have experienced ongoing delays and we acknowledge the impact that this can have on individuals, such as yourself.

I also want to acknowledge your noted concerns regarding the content of the release package that was sent to you, as well as your comments around the state of CPIC information and the broader public interest issue that you mentioned in your correspondence.

With regards to your concerns related to CPIC and the state of personal data within, as well as those related to your specific release package and the delays in regards to our processing your request, within the legislated timeframe, your best approach would be to pursue the complaint that you noted with the Office of the Privacy Commissioner of Canada (OPC) - PA-073749 - and, if needed, open additional complaints to ensure all your noted concerns are reviewed by the OPC.

Once again, I want to thank you for following up with us, holding us accountable, and ensuring your rights under access and privacy legislation are upheld accordingly by pursuing any concerns you have on your Privacy Request with the Office of the Privacy Commissioner of Canada.

Best regards,

Jeff Ball

Director Privacy

Access to Information and Privacy Branch

Digital Program

Royal Canadian Mounted Police

Jeff.Ball@rcmp-grc.gc.ca

Cell: 343-571-6721

Jeff Ball

Directeur protection des renseignements personnels

Sous-Direction de l'accès à l'information et la protection des renseignements personnels

Programme Numérique

Gendarmerie royale du Canada

Jeff.Ball@rcmp-grc.gc.ca

Céll: 343-571-6721

From: Mr. Kevin McLean <mcleansettlement@gmail.com>

Sent: April 27, 2026 4:34 PM

To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>; Simpson, Melissa (RCMP/GRC) <Melissa.Simpson@rcmp-grc.gc.ca>;
Brisson, Stéphane (RCMP/GRC) <Stephane.Brisson@rcmp-grc.gc.ca>; Duheme, Michael (RCMP/GRC)
<Michael.Duheme@rcmp-grc.gc.ca>; Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>; Worrell, Julie (RCMP/GRC)
<Julie.Worrell@rcmp-grc.gc.ca>

Subject: Re: Privacy Act request P-2025-16999 / F339, Your File N/A, Acknowledgment

PRIVATE AND CONFIDENTIAL

DATE: April 27, 2026

Tab G

DELIVERY METHOD: Via Secure Electronic Transmission

TO: Ms. Melissa Simpson (and/or Assigned Delegate) Access to Information and Privacy Branch Royal Canadian Mounted Police 73 Leikin Drive, Mail Stop #61 Ottawa, Ontario K1A 0R2

CC: Julie Worrell For / Jeff Ball, Director, Privacy Access to Information and Privacy Branch Mailstop #61 73 Leikin Drive Ottawa, Ontario K1A 0R2

CC: Mr. Michael Duheme, Commissioner, Royal Canadian Mounted Police **CC:** Mr. Stéphane Brisson, Director General, Access to Information and Privacy

REFERENCE I: RCMP ATIP File P-2025-16999 **REFERENCE II:** OPCC Complaint File PA-073854 (Formalized April 19, 2026; Supplemented April 22, 2026) **REFERENCE III:** Purported "Final Response Letter" and "Release Package" dated April 27, 2026

SUBJECT I: Categorical Rejection of the Vitiating Institutional Search Methodology and the Misapplication of Statutory Exemptions
SUBJECT II: Formal Integration of the Evidentiary Record into the Active Office of the Privacy Commissioner Investigation **SUBJECT III:** Renewed Demand for the Immediate Execution of a Compliant Offline Historical Database Extraction

Dear Ms. Simpson, Ms. Worrell, Director Ball, Director General Brisson, and Commissioner Duheme:

1. INTRODUCTION, THE CRYSTALLIZATION OF THE EVIDENTIARY RECORD, AND ANTECEDENT DEFAULTS

1.1. Correspondence is heretofore promulgated in direct, unyielding, and comprehensive response to the purported final response letter (the "**Final Response**") and the accompanying release package (the "**Release Package**") transmitted by the royal canadian mounted police (the "**Institution**") on April 27, 2026, concerning access requisition P-2025-16999. It is explicitly recorded *in limine* that the institutional response is formally, legally, and forensically rejected in its absolute entirety.

1.2. The aforementioned Release Package does not constitute a valid, legally compliant discharge of the Institution's mandatory obligations under subsection 12(1) of the *Privacy Act*, RSC 1985, c P-21. Rather, it manifests as a profound administrative obfuscation, characterized by the deliberate execution of an entirely irrelevant search methodology and the legally bankrupt misapplication of statutory exemptions. The institutional conduct documented herein serves only to exacerbate the systemic deprivation of quasi-constitutional rights and fortifies the foundational merit of the active administrative complaints presently before the office of the privacy commissioner of canada (the "**OPCC**"). Reliance is unequivocally placed upon the established and binding jurisprudence, notably *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at para 61, wherein the quasi-constitutional status of access rights is unambiguously affirmed by the apex court. These statutory entitlements are specifically engineered, deliberately constructed, and statutorily enshrined such that the citizenry is empowered to scrutinize, challenge, and definitively rectify the purported deployment of vitiating judicial instruments—*acta* which have facilitated a profound, potentially *ultra vires* deprivation of physical liberty. The contravention of these strictures vitiates the *lex terrae* and obviates any pretense of lawful detention, rendering the actions of the state functionally indistinguishable from arbitrary coercion and false imprisonment.

1.3. It is imperative to contextualize this purported Final Response against the backdrop of the Institution's antecedent defaults. As exhaustively documented in the *Memorandum of Fact and Law Concerning the Deemed Refusal of Access* (the "**Deemed Refusal Memorandum**"), formally submitted to the OPCC on April 19, 2026 (Tab 2 of the OPCC evidentiary brief), and subsequently served upon the Institution's Directorate via secure electronic transmission on April 19, 2026 (as verified by the accompanying email logs), the Institution had already effectuated an unequivocal deemed refusal of access by allowing the strict statutory thirty-day period to unconditionally expire on April 10, 2026. This administrative failure fundamentally breaches the core tenets of the access partnership, severely prejudicing the Applicant's capacity to mount a timely legal defense against ongoing state coercion.

1.4. The subsequent, delayed issuance of the legally deficient Release Package on April 27, 2026, does not cure the antecedent deemed refusal; rather, it superimposes a substantive failure of processing upon a procedural failure of timeliness. Director Ball and Ms. Worrell, in your capacities overseeing the privacy operations of the Institution, your direct inclusion in this correspondence is strictly necessitated. The ensuing forensic deconstruction of the RCMP's Release Package is hereby formally entered into the active OPCC investigative matrix as a supplementary submission, inextricably linked to the April 22, 2026 filing. It is respectfully submitted that the Institution must immediately abandon its evasive "live query" tactics, cease the deployment of boilerplate bureaucratic deflections, and strictly adhere to the meticulously defined parameters of the original statutory requisition.

2. THE FORENSIC INVALIDITY OF THE SEARCH METHODOLOGY: LIVE QUERIES VERSUS OFFLINE ARCHIVES

2.1. Receipt of your recent communication is hereby acknowledged. While it is formally noted that the provided Release Package is profoundly non-responsive and fundamentally fails to satisfy the statutory requisition in a multiplicity of ways, this prompt response is nevertheless issued in a spirit of good faith to preserve the integrity of the access partnership and to facilitate immediate corrective action. Continued jurisprudential review confirms the fatal deficiencies in the institutional processing; foremost among these is the Institution's erroneous administrative record-keeping regarding the exact date of receipt. It appears the Institution failed to process the access request as originally submitted on March 11, 2026, improperly recording the receipt date as March 12, 2026. This artificial truncation of the statutory timeline is indicative of an overarching institutional posture designed to shave precious days from the statutorily mandated countdown, thereby unlawfully prolonging the concealment of critical digital *acta*. For absolute clarity and the avoidance of further unwarranted delays or bureaucratic sleight-of-hand, the comprehensive original requisition is attached hereto, seamlessly integrated within this thread, and simultaneously served upon all relevant operational directorates to preclude any further wasteful expenditure of precious administrative and judicial resources.

2.2. A rigorous forensic evaluation of the Release Package fundamentally exposes the catastrophic failure of the institutional search parameters. The primary statutory requisition explicitly, repeatedly, and unambiguously demanded the execution of a comprehensive offline search (the "**Offline Search**") of the highly secure offline historical database (the "**Offline Historical Database**") associated with personal information bank rcmp pp0 005 (the "**PIB RCMP PPU 005**"). The request meticulously specified the exaction of historical transaction logs, audit trails, and hexadecimal dumps spanning the precise temporal epoch of September 15, 2024, to October 2, 2024. These records are not peripheral metadata; they constitute the definitive, immutable ledger of state action, detailing exactly when, where, and by whom the coercive machinery of the state was activated against the Applicant.

2.3. You are hereby formally compelled to confirm or deny, unequivocally, whether the provided Release Package contains the explicitly requested offline searches, including all original informational inputs and any subsequent amended, retroactively altered, or systematically metamorphosed data. This explicit confirmation or denial must be rendered no later than the close of business tomorrow. In the event the Release Package does not contain these mandated records—as the present forensic review strongly indicates—you are hereby legally obliged to produce the same by the close of business tomorrow, as this critical exaction remains severely outstanding, fundamentally unfulfilled, and the subject of an active deemed refusal complaint presently before the OPCC.

2.4. In the alternative, if the Institution has entirely failed to execute the requisite Offline Search, you are instructed to formally confirm or deny this failure in writing. To the extent that the Institution has failed to conduct the search as explicitly delineated, I forcefully reiterate that any *post facto* attempt to invoke a statutory extension of time under section 15 of the *Privacy Act* would be fundamentally improper, entirely unlawful, and demonstrative of compounding bad faith. An institution cannot ignore the explicit parameters of a request, execute a mathematically doomed search, and subsequently claim that fulfilling the original parameters requires an extension due to "unreasonable interference." You are further required to provide a granular explanation detailing the precise nature of the records you *have* provided, as the current release is forensically opaque, contextually deficient, and legally unintelligible on all fronts. Furthermore, should the Institution's posture be that I must pursue a formal correction of my personal information under the *Privacy Act*, it is an inescapable logical, procedural, and legal prerequisite that I be provided with the very information requiring correction *ab initio*.

2.5. In stark, inexcusable contravention of these explicit directives, the Release Package reveals that the access to information and privacy analyst, identified operationally as operator nboisvert (the "**Terminal Operator**"), entirely ignored the parameters of the Offline Search. The provided documentation (identified internally as A1257675_1-000001) confirms that on April 14, 2026, at precisely 07:35:43, the Terminal Operator merely executed a superficial, real-time "Q PERS+" query and a subsequent "Q CNI" query against the active, front-facing canadian police information centre (the "**CPIC**") interface. The execution of this specific query command serves only to ascertain the existence of *currently active* alerts, warrants, or criminal index entries as of the moment the terminal keystrokes are executed.

2.6. The resultant output, predictably indicating "**NOT ON FILE PERSON LOG**" and "**NO CONVICTIONS**", is forensically vacuous and logically absurd in the context of the underlying legal demand. It is a fundamental, structurally established reality of the CPIC architecture that an arrest warrant successfully executed in October 2024 is immediately subjected to a clearance transaction (the "**CLEAR Transaction**"). This terminal action permanently purges the record from the active "Q PERS+" interface to preclude unlawful secondary arrests, securely migrating the data into the insulated Offline Historical Database. To search the active interface for a concluded event is akin to searching a modern telephone directory for a discontinued number; the failure to locate the entry proves nothing of its historical existence or its provenance.

2.7. Consequently, querying the live database in April 2026 to locate a warrant successfully executed in October 2024 is an exercise in profound administrative theater. The Institution has purportedly expended vast operational resources, allowed the strict statutory deadline to completely expire, and necessitated the forceful intervention of the OPCC, all to ultimately execute a keystroke query that required mere milliseconds and was mathematically guaranteed by the system's own architecture to return a null result. This methodology constitutes a deliberate evasion of the duty to assist, subverting the *lex terrae* and intentionally frustrating the access partnership mandated by the OPCC. The failure to query the Offline Historical Database for the ADD, MODIFY, and CLEAR transaction logs is not a mere oversight or a technological misunderstanding; it is a systemic, calculated refusal to process the request as drafted, directly compounding the bad faith articulated in the Deemed Refusal Memorandum.

3. DECONSTRUCTION AND VITIATION OF THE INVOKED STATUTORY EXEMPTIONS

3.1. Notwithstanding the execution of an entirely irrelevant search methodology that yielded ostensibly null results, the Final Response paradoxically asserts that "some of the information has been exempted pursuant to sections 19(1)(d), 22(1)(b) and 26 of the Act." It is respectfully submitted that the invocation of these exemptions to withhold historical CPIC metadata and transactional audit trails is legally unsupported, jurisdictionally flawed, and constitutes an *ultra vires* exercise of administrative discretion explicitly designed to shield foundational metadata from impending scrutiny, exactly as anticipated in paragraph 3 of the Deemed Refusal Memorandum. The application of exemptions to a null search result heavily suggests the existence of responsive offline records that the Institution has located but improperly chosen to conceal.

The Misapplication of Section 19(1)(d): Originator Control and the Stewardship Doctrine

3.2. The Institution's reliance upon paragraph 19(1)(d) of the *Privacy Act*—asserting that the personal information was obtained in confidence from a municipal or regional government (e.g., the Toronto Police Service)—is fundamentally dismantled by established OPCC and provincial privacy jurisprudence. The Institution is attempting to weaponize the bureaucratic principle of originator control to completely abdicate its overarching statutory responsibilities as the central federal database architect and national data steward.

3.3. As the host and paramount administrator of the CPIC network, the RCMP exercises absolute "control" over the systemic infrastructure, the transactional architecture, and the insulated Offline Historical Database. This paradigm of absolute federal control is decisively reinforced and jurisprudentially settled by the Information and Privacy Commissioner of Ontario in *Order MO-4542* (Halton Regional Police Services Board). In that binding precedent, the adjudicator ruled unequivocally that municipal police forces do *not* have custody or control over the broader CPIC database inquiries or the systemic records generated by other services within the national architecture; a municipal force only controls its own localized interface. By necessary legal corollary, if the constituent municipalities lack legal custody and control over the overarching federated database and its historical audit trails, that statutory control vests exclusively, solely, and incontrovertibly with the federal host—the RCMP. The Institution cannot legally disavow the contents of its own digital ledger by deflecting responsibility to municipal entities that have been jurisprudentially proven to lack custody and control of the centralized infrastructure. The RCMP cannot construct the digital panopticon and subsequently feign blindness when an individual requests their own data from it.

3.4. Furthermore, the *acta* of the courts are fundamentally, inherently public records. The metadata tracking the systemic input of a coercive judicial instrument (such as an arrest warrant) cannot be sequestered as "confidential" under section 19. It defies both logic and constitutional law to classify the digital routing coordinates, origin timestamps, Originating Agency Identifiers (ORIs), and terminal identifiers of a publicly executed court process as highly sensitive intelligence entrusted to the federal government under a veil of municipal secrecy. The execution of a warrant is a public act of state force; the systemic ledger authorizing that force must be equally exposed to public and personal scrutiny.

The Misapplication of Section 22(1)(b): The Functus Officio Doctrine and Historical Acta

3.5. The invocation of paragraph 22(1)(b) of the *Privacy Act*—premised upon the assertion that disclosure could reasonably be expected to be injurious to the enforcement of any law or the conduct of lawful investigations—is rendered entirely moot by the passage of time and the definitive conclusion of the operational event.

3.6. The physical apprehension of the subject was effectuated on October 2, 2024. The custodial phase has entirely culminated, and release documentation (Form 10) was executed. At the exact moment of execution and subsequent release, the authorizing judicial officer became definitively *functus officio*, and the operational, investigatory imperative of the warrant was eternally exhausted. Reliance is placed upon the foundational principles articulated in *Chandler v Alberta Association of Architects*, [1989] 2 SCR 848, wherein the Supreme Court of Canada affirmed that once a tribunal or judicial officer has finally decided a matter and issued their order, their jurisdiction over that specific matter is entirely extinguished. Consequently, the authorization itself crystallizes from an active investigatory tool into administrative, historical records of a definitively concluded judicial process (*acta*).

3.7. The requested Transaction Logs, the systemic origin codes, the terminal identifiers, and the hexadecimal dumps do not contain active investigative techniques, confidential informant methodologies, or ongoing surveillance strategies; they contain purely historical, immutable administrative facts regarding a concluded judicial authorization. There exists absolutely no ongoing investigation that could conceivably be prejudiced or injured by the disclosure of the specific digital timestamp denoting exactly when a local police force inputted a warrant into a federal database nearly two years prior. The statutory shield of investigatory privilege was designed to protect the integrity of ongoing law enforcement operations; it cannot be retroactively contorted, stretched, or weaponized to conceal potential procedural anomalies, jurisdictional overreaches, or severe jurisdictional malfeasance embedded within historical *acta*. To allow section 22 to cover executed warrants indefinitely is to establish a secret police ledger, anathema to the *Canadian Charter of Rights and Freedoms*.

The Misapplication of Section 26: State Actors and the Public Domain

3.8. The Institution's reliance upon section 26 of the *Privacy Act* to withhold the identities of third parties—presumably the names of the presiding judicial officers (e.g., Justice of the Peace George Jiri), the swearing special constables (e.g., Informant Christyn Frugoni-Rojas), and the inputting terminal operators—constitutes a gross misinterpretation and profound misapplication of Canadian privacy law.

3.9. The jurisprudential parameters established by the Supreme Court of Canada, notably in *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25, definitively dictate that the professional identities, nomenclatures, and operational titles of public servants and state actors executing official, remunerated public functions do not attract the elevated privacy protections afforded to the intimate biographical details of private citizens. When an individual exercises the coercive power of the state, they inherently surrender the expectation of privacy regarding the execution of that specific power.

3.10. A Justice of the Peace affixing their signature to a coercive warrant that deprives a citizen of liberty, a Special Constable swearing an Information under oath to initiate a prosecution, and a police clerk executing an entry into the national CPIC mainframe to trigger a nationwide broadcast are performing profound, consequential acts of state authority. Their professional identities, within the specific context of those official actions, are entirely within the public domain. The *Privacy Act* was architected to protect the dignity and intimate life details of the citizenry against the overarching surveillance of the state; it was decidedly not enacted to serve as a prophylactic mechanism utilized by the federal constabulary to conceal the identities of the specific state actors responsible for authorizing and executing the deprivation of a citizen's physical liberty. To apply section 26 in this matrix is to pervert the legislative intent of the statute, transforming a shield for the citizen into a cloak for the state.

4. CONCLUDING REQUISITIONS AND OPCC ESCALATION PROTOCOLS

4.1. In absolute summation, the Release Package provided on April 27, 2026, is fundamentally unresponsive to the specific parameters of the statutory demand. The Institution has deliberately substituted a meaningless, instantaneous live query for the rigorous, forensically mandated Offline Search, and has subsequently layered legally inapplicable exemptions over the resultant nullity to artificially terminate the file and frustrate access to justice.

4.2. Director Ball and Ms. Worrell, be formally advised that the OPCC has been concurrently requested to immediately integrate this correspondence into the evidentiary matrix of Complaint File PA-073854. The documentation provided by the Institution today constitutes unequivocal, documentary proof of a systemic failure to conduct a reasonable search for records, a deliberate evasion of the precise temporal and offline parameters dictated by the requestor, and an unlawful application of discretionary exemptions to historical, non-exempt administrative metadata. The OPCC is respectfully urged to view this conduct through the lens of institutional bad faith.

4.3. Director General Brisson, Director Ball, Ms. Worrell, and Ms. Simpson, a final, uncompromising demand is hereby registered. The Institution is formally compelled to completely abandon the active "Q PERS+" interface, engage the requisite technical specialists, and immediately execute the explicitly requested Offline Search of the Offline Historical Database (PIB RCMP PPU 005) for the exact dates surrounding the September/October 2024 arrest event. The unredacted ADD, MODIFY, and CLEAR transaction logs, alongside the unvarnished hexadecimal metadata proving the exact digital provenance and geographical origin of the judicial authorization, must be remitted forthwith. The fundamental maxim *nemo dat quod non habet* dictates that a judicial officer cannot confer lawful authority over a jurisdiction to which they are not assigned; the digital logs are the only mechanism to verify if such jurisdictional boundaries were violently breached.

4.4. The failure to rectify this egregious administrative subversion by the close of business tomorrow will precipitate the immediate expansion of the pending OPCC investigations, the formal invocation of the right to demand a notation of disagreement under subsection 12(2) of the *Privacy Act* (to flag the CPIC system for potential documentary fraud), and the accelerated preparation of an application for a writ of *mandamus* before the Federal Court of Canada pursuant to section 41 of the *Privacy Act*. As articulated in *R v Garofoli*, [1990] 2 SCR 1421, the right to challenge the validity of a warrant is absolute; the RCMP cannot unilaterally extinguish this right by burying the digital footprints of that warrant in an unsearched archive. The doctrine of *fraus omnia corrumpit* demands that the metadata be exposed to the light of judicial scrutiny.

Tab H

4.5. Included as a courtesy, and expressly extended in a spirit of profound cooperation and *bona fides*, I have attached the vitiated documentation (the "**False Information Package**"). It is noted with immense legal gravity that the fraudulent character of this document has been explicitly confirmed by the Ministry of the Attorney General, specifically by counsel situated within their civil document request division. This documentation is enclosed to unequivocally demonstrate precisely why my statutory request is so highly comprehensive, granular, and detailed. The physical municipal records have been proven fundamentally corrupted; therefore, the unalterable federal digital ledger represents the sole remaining avenue to triangulate the truth of the state's actions. Thank you for your anticipated, immediate, and lawful compliance.

All of which is respectfully submitted.

Mr. Kevin A. McLean (BA, JD, CIM) Chartered Investment Manager

Enclosures: i. Passport of Mr. Kevin A. McLean (BA, JD, CIM) (Previously Submitted) ii. The False Information Package (Corroborated by MAG Counsel) iii. Comprehensive Original Requisition (March 11, 2026 - **delivered as confirmed by Canada Post**)

NOTA BENE: Only reply via email or fax (can be provided upon request). Attachments may follow on a piecemeal ba

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Sat, Apr 25, 2026 at 12:09 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Reply to:

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Date: April 25, 2026

VIA EMAIL / ELECTRONIC TRANSMISSION

To: Head of the Institution, Privacy Officer, and Ms. Simpson

Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police (RCMP) / Canadian Police Information Centre (CPIC)

RE: FILE NUMBER PA-073920 - Deemed Refusal predicated upon non-disclosure or non-access to requested personal information records predicated upon, on its face (pardon the pun), an invalid and prohibited time extension

SUBJECT: Formal Notice of Complaint - Deemed Refusal, Public Interest Disclosure Demand, and Potential Judicial Review pursuant to, inter alia, FCA, ss. 18 and 18.1 in contradistinction to section 41 of the Privacy Act

Dear Head of the RCMP, Privacy Officer, and Ms. Simpson:

Please accept this letter as formal confirmation that I have filed a comprehensive complaint with the Office of the Privacy Commissioner of Canada (OPCC) explicitly predicated on the basis of a "deemed refusal" concerning the above-noted file. This procedural step naturally dictates that if there was not a valid, statutorily compliant extension of time executed by the RCMP—which I assert there was not, in fact or at law—then the OPCC must immediately and unequivocally confirm the same.

The Supreme Court of Canada has repeatedly affirmed that the *Privacy Act* is quasi-constitutional legislation. It is designed not merely to protect personal information, but to guarantee individuals an enforceable right of access and, crucially, to afford them the statutory right to correct that information under subsection 12(2) when state records are found to be erroneous, maliciously altered, or factually baseless. By allowing the statutorily mandated timeline to expire through an unabated effluxion of time and a calculated absence of substantive communication, the RCMP has actively frustrated these quasi-constitutional rights.

Moreover, pursuant to the binding jurisprudence established in *Gregory v. Canada (Public Safety Ministry)*, a deemed refusal is crystallized because the timing of the receipt of my access request was mathematically and factually misstated by the RCMP. The RCMP cannot unilaterally rewrite the calendar to cure its own administrative inertia. Without castigation or insult per se, the Institution could not have possibly complied with the strict procedural prerequisites under section 15 of the *Privacy Act*. The statute requires clear notice of the extension, the specific length of the extension, and a valid justification, all of which are impossible to calculate or communicate without acknowledging the accurate, objective date of receipt.

For your immediate reference, Section 15 of the *Privacy Act* explicitly states:

Extension of time limits

15 The head of a government institution may extend the time limit set out in section 14 in respect of a request for

(a) a maximum of thirty days if

(i) meeting the original time limit would unreasonably interfere with the operations of the government institution, or

(ii) consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit, or

(b) such period of time as is reasonable, if additional time is necessary for translation purposes or for the purposes of converting the personal information into an alternative format,

by giving notice of the extension and the length of the extension to the individual who made the request within thirty days after the request is received, which notice shall contain a statement that the individual has a right to make a complaint to the Privacy Commissioner about the extension.

I loathe to be overly technical on such an important substantive and public interest issue, but that belies the point that administrative and technical delays are currently being utilized in a strictly non-compliant fashion to function as a de facto denial of access. When state agencies weaponize statutory extensions or fabricate receipt dates to obscure their failure to produce sensitive records, the integrity of the access regime collapses. At the very least, some form of phased or interim release of the requested offline metadata and foundational records should have been effected to demonstrate institutional good faith.

I have attached a copy of the formal OPCC complaint involving what I categorically maintain is a "deemed refusal" predicated on the aforementioned grounds. I rely heavily on the fact that no protracted or complex investigation is required by the OPCC to render this finding. As clearly articulated in *Gregory v. Canada (Public Safety Ministry)* at paragraph 15, the issue of a deemed refusal is an objective, mathematical reality; it is not one that requires administrative discretion, and there is no distinction with a legal difference between a deemed refusal and an actual refusal per se. Administrative silence equates to a denial of fundamental rights.

DEMAND FOR PUBLIC INTEREST DISCLOSURE AND EXERCISE OF DISCRETION

Beyond the deemed refusal of the access request itself, please be advised that the Head of the RCMP is legally required to actively consider the overarching issue of disclosing the requested records to

the public, pursuant to section 8 of the *Privacy Act* and section 19 of the *Access to Information Act* (ATIA). This is not a passive obligation, but an active, continuing duty when institutional integrity is brought into question.

I direct your attention to Section 8(2)(m) of the *Privacy Act*, which states:

8(2)(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

Concurrently, Section 19 of the *ATIA* reinforces this obligation regarding personal information:

19 (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Part that contains personal information.

(2) Where disclosure authorized: The head of a government institution may disclose any record requested under this Part that contains personal information if

(a) the individual to whom it relates consents to the disclosure;

(b) the information is publicly available; or

(c) the disclosure is in accordance with section 8 of the *Privacy Act*.

The underlying issue here—whether a foundational federal law enforcement database like CPIC is harboring manipulated records, fraudulent metadata, or forged documentation—is of existential importance to the administration of justice in Canada. The public has an overwhelming, pressing right to know if the architecture of the criminal justice system is being compromised by systemic documentary spoliation or unauthorized database manipulation. The institutional accountability inherent in this disclosure drastically outweighs any generic privacy exemptions the Crown might attempt to invoke post facto.

There is no rigid 30-day statutory time limit constraining the Head's duty to consider public interest disclosures under section 8 of the *Privacy Act*

and section 19 of the *ATIA*. Therefore, a failure to act on this specific front does not fall merely under the narrow, restrictive confines of section 41 of the *Privacy Act*. Rather, it forms the substantive jurisdictional basis for an application for judicial review under sections 18 and 18.1 of the *Federal Courts Act* (FCA), specifically in the nature of *mandamus*.

FORMAL DEMAND FOR MANDAMUS AND PROHIBITION

Kindly be assured that this correspondence operates as a formal legal demand. Should the RCMP fail to exercise its statutory duties, I will be immediately seeking an order of *mandamus* from the Federal Court. I rely squarely on the established eight-part test articulated by the Federal Court of Appeal in *Apotex Inc. v. Canada (Attorney General)*. Specifically, while the Head's power to disclose under the aforementioned sections involves an element of discretion, in this highly specific context, that discretion is fettered and *must* be exercised. The rigid prerequisites for *mandamus* are undeniably met:

1. There is a public legal duty owed to me;
2. There is a clear right to performance following this explicit demand;
3. There has been a clear demand and a corresponding failure to act;
4. The duty is owed by a federal board, commission, or tribunal;
5. There is no equitable bar or adequate alternative remedy available that would yield the same robust accountability; and
6. The balance of convenience heavily favours compelling the institution to act, as justice delayed is justice denied.

I also note that when it relates to *mandamus* per se, this could relate to in fact exercising a discretion such as that under section 8(2)(m) of the *Privacy Act* and section 19 of the *ATIA*, and in relation to the likes of prohibition, this could be in relation to prohibiting the RCMP from taking the types of invalid time extensions under the *Privacy Act* or the *ATIA* in the future. Nonetheless, the reference to the 60 days in the *ATIA* invalid time extension demonstrates that the *Privacy Act* time extension was not proper. As such, we have a deemed refusal in relation to my access request and no investigation is required, and merely a confirmation of the same (if necessary) by the OPCC.

If you intend *not* to make a public interest disclosure to the public involving the matters I have particularized—namely, ensuring the public is explicitly made aware of the fraud involving the manipulation of records concerning myself and the broader, critical public interest issues at stake—I demand that you explicitly advise me of your

position. I require to know whether the RCMP intends to utilize administrative opacity to shield potentially compromised CPIC metadata from independent judicial or public scrutiny.

Please confirm in writing whether you intend to exercise this discretion positively or negatively, and exactly *when* you will provide this formal, binding position. I remain deeply concerned with a systemic pattern of conduct by government institutions: failing to comply with the baseline letter of the law, forcing citizens to initiate Federal Court litigation simply to compel basic compliance, and strategically waiting until the 11th hour to produce documents once a proceeding is already commenced. This "litigation by ambush" tactic, designed to moot an application and evade judicial review and costs awards, is a profound abuse of process.

While this has spawned from an access request per se and the "access partnership model" must be paramount, I must nonetheless confirm that I reserve the right to rely on this correspondence for any lawful purpose, including in support of elevated costs before the Federal Court. I find this regrettable but necessary because if this is a pattern, and in light of the *ATIA* improper time extension, in relation to falsification of records at first instance or post facto involving law enforcement provincially or nationally, even a delay of a day is too much. An individual's liberty and reputation cannot be held hostage by the state's failure to maintain accurate, unadulterated databases.

If you are willing to assuage my concerns that this was idiosyncratic, then please do so immediately with the production of the requested records. Otherwise, I will presume there is at least a pattern or more than a singular incident in recent history herein, and as a lifelong Canadian citizen, we all have duties to shape the evolution of the law and guarantees in the *Constitution Act, 1867*, and *Constitution Act, 1982*, along with the rule of law of which judicial independence is a fundamental pillar therein.

The matter remains exceedingly urgent, and time is strictly of the essence. Govern yourselves accordingly.

Sincerely,

(Original electronically signed)

Kevin A. McLean

Encl: 1. Complaint Submission - Deemed Refusal - RCMP - CPIC - Complainant - Mr McLean - 19-April-2026.docx

Warm regards,

Tab I

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Apr 23, 2026 at 4:38 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

PRIVATE AND CONFIDENTIAL

VIA SECURE ELECTRONIC TRANSMISSION

DATE: April 23, 2026

TO: Mr. Michael Duheme, Commissioner and Head of the Institution

Mr. Stéphane Brisson, Director General, Access to Information and Privacy (Chief Privacy Officer)

Ms. Melissa Simpson, Access to Information and Privacy Branch

Royal Canadian Mounted Police (RCMP)

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca, melissa.simpson@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca,
Michael.Duheme@rcmp-grc.gc.ca

FROM: Mr. Kevin A. McLean (B.A., J.D., CIM)

REFERENCE: Privacy Act Request P-2025-16999 / F339

OPCC Complaint File: PA-073749

SUBJECT: Formal Demand for Phased (Piecemeal) Release of Personal Information Records — Analogy to Access to Information Act (ATIA) Jurisprudence, the Duty to Assist, and the Expiration of the 45-Day Epoch

Dear Commissioner Duheme, Director General Brisson, and Ms. Simpson:

I write to you today, April 23, 2026, to formally note that we are now approximately **45 days** removed from the incontrovertible receipt of my *Privacy Act* requisition via Canada Post registered delivery on March 11, 2026.

As exhaustively documented in my prior correspondence, the 30-day time extension invoked by your office under paragraph 15(a) (i) of the *Privacy Act* was procedurally void *ab initio*. It was predicated on an erroneous receipt date and entirely lacked the mandatory statutory particulars required to justify an "unreasonable interference" with the operations of a \$6.48 billion federal institution. As established by the Federal Court in *Gregory v. Canada (Public Safety and Emergency Preparedness)*, 2020 FC 667, general workload fluctuations or routine administrative encumbrances possess absolutely zero capacity to satisfy the formidable threshold required for an operational extension. Consequently, the absolute statutory deadline for compliance expired on April 10, 2026, placing the RCMP in an indefensible, continuing state of deemed refusal.

However, in the spirit of maintaining a functional "access partnership," mitigating further prejudice to my quasi-constitutional rights, and preserving institutional resources, I am presenting a legally binding avenue for immediate, partial institutional compliance based upon established federal jurisprudence and Treasury Board directives.

I. The "Seamless Code" Doctrine and the ATIA Jurisprudential Analogy

The Supreme Court of Canada has definitively established in foundational jurisprudence, notably *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, that the *Privacy Act* and the *Access to Information Act* (ATIA) are companion statutes that must be read together as a "seamless code." They are twin pillars of democratic accountability. Consequently, interpretive principles and procedural standards applied to the administrative mechanisms of one act apply *mutatis mutandis* (with necessary modifications) to the other.

Under Section 9 of the ATIA (the direct statutory equivalent to Section 15 of the *Privacy Act* regarding time extensions), the Federal Court and the respective Information and Privacy Commissioners have frequently adjudicated the operational burdens of complex document retrieval. A paramount, non-negotiable principle that has emerged from ATIA jurisprudence is the absolute prohibition of the "all-or-nothing" approach to document disclosure.

As established in persuasive privacy commission rulings analyzing Federal Court precedent (e.g., *Public Service Commission (Re)*, 2011 CanLII 47545 (NL IPC)), **an institution explicitly breaches the underlying purpose of a time extension if it**

withholds records that have already been processed and are ready for release, simply because other records within the same request are still undergoing complex extraction, inter-departmental consultation, or redaction. The legislative intent behind allowing extensions is to afford the institution necessary time to manage voluminous or technologically arduous data processing—it was never intended to serve as a blanket administrative embargo that suspends the release of simple, readily available personal information.

II. The Technological Disparity and the Mandatory Imperative of Phased (Piecemeal) Release

Applying this established ATIA jurisprudence to my *Privacy Act* request yields a singular, unassailable conclusion: the RCMP is legally prohibited from holding my readily accessible, front-facing personal information hostage while its specialized divisions purport to extract the more complex forensic data.

I have formally acknowledged that extracting the raw, offline hexadecimal mainframe dumps (information strictly required to prove the algorithmic metamorphosis and vector collapse of the underlying judicial instrument) necessitates specialized forensic interrogation of the Canadian Police Information Centre (CPIC) database. Such a query requires navigating the backend architecture of Personal Information Bank RCMP PPU 005.

If the RCMP required additional time to execute that highly technical offline search—although such necessity was never adequately particularized in your initial notice of extension—that specific administrative burden *cannot* lawfully serve as a barrier to releasing the simple, front-facing data fields today.

It is an empirical reality that extracting discrete alphanumeric fields from the active CPIC graphical user interface requires mere milliseconds of computational exertion by a trained terminal operator. After 45 days, it strains all bounds of credulity and objective logic to suggest that the RCMP has not yet located or processed the basic, foundational metadata associated with my specific CPIC profile. To withhold this fundamental data while citing the complexity of the hexadecimal extraction is to weaponize administrative delay, thereby severely exacerbating the institutional culpability regarding the ongoing deemed refusal.

III. The Statutory Duty to Assist

Furthermore, the immediate provision of a phased release is compelled by the statutory "Duty to Assist" enshrined within federal privacy directives. The Treasury Board of Canada Secretariat (TBS) Directive on Privacy Practices explicitly advocates for institutions to make every reasonable effort to assist requesters, which includes the prompt, interim delivery of records to mitigate the prejudice caused by necessary administrative delays.

When a citizen is actively challenging a jurisdictional nullity that directly implicates their physical liberty and Section 7 *Charter* rights, the institutional withholding of easily retrievable metadata ceases to be a mere clerical delay and transforms into active evidentiary spoliation. An interim disclosure serves to momentarily bridge the profound asymmetry of information existing between the coercive apparatus of the state and the private citizenry.

IV. Demand for Immediate Interim Disclosure

Because institutions are legally and practically expected to release records in phases (piecemeal) as they become available, I formally demand the immediate, interim release of the following four discrete data fields. These specific alphanumeric points require no complex severability analysis, no third-party consultation, and absolutely no offline hexadecimal extraction:

1. **Originating Agency Identifier (ORI):** The specific routing code confirming the exact municipal or provincial police force division (e.g., TPS 52 Division vs. 14 Division) that physically inputted the warrant into the federal system. This data point is required immediately to bypass intentional inter-agency obfuscation.
2. **Issuing Authority / Court Field:** The precise alphanumeric entry confirming the exact court level (e.g., Superior Court of Justice vs. Ontario Court of Justice) and the specific name or initials of the authorizing judicial officer exactly as they are currently displayed in the active system.
3. **Originating Courthouse:** The geographic or building code corresponding to the court registry inputted by the terminal operator, required to establish the geographical jurisdiction of the authorization.
4. **System Identification Number:** The unique, immutable CPIC transaction identifier allowing for the tracing of the record's lifecycle across the national network.

V. The Public Interest Override (s. 8(2)(m)(i)) Operates Independently of Standard ATIP Timelines

It must be unequivocally established that the standard 30-day statutory timeline (or any purported 60-day extended timeline) governing formal access requests under Section 12 of the *Privacy Act* does not constrain the Commissioner's authority to act under Section 8(2)(m)(i).

Section 8(2)(m)(i) grants the Head of the Institution the explicit, discretionary authority to disclose personal information where the public interest clearly outweighs any invasion of privacy. When a citizen is deliberately kept unaware of their own compromised personal information due to state-actor fraud, digital forgery, and the algorithmic metamorphosis of judicial instruments, the public interest imperative is absolute.

In such unprecedented circumstances of systemic jurisdictional nullity, the Commissioner possesses the inherent statutory authority to bypass routine ATIP queue delays and disclose the information *forthwith* to the affected individual. The discovery of a fabricated Information Package demands immediate remedial disclosure, entirely untethered to the administrative protraction and bureaucratic scheduling of standard processing timelines.

VI. Conclusion and Administrative Prognosis

Providing these four basic, alphanumeric data points by the close of business tomorrow will satisfy the immediate requirements of the "Duty to Assist," demonstrate a demonstrable, good-faith effort by the RCMP to cure the ongoing deemed refusal, and properly align your institution with the phased-release mandates rigorously established in ATIA case law.

I look forward to the prompt receipt of this interim disclosure, which will allow me to independently verify the foundational parameters of the state action taken against me, while your technical specialists complete the rigorous exaction of the remaining offline hexadecimal logs and audit trails.

Furthermore, **I seek a definitive response by no later than 4:00 p.m. tomorrow expressly confirming or denying whether there were any post-entry amendments, modifications, or algorithmic alterations to the originally inputted information or data** residing within the CPIC mainframe.

Should the RCMP refuse this legally sound administrative accommodation and persist in its "all-or-nothing" embargo, I will immediately append this correspondence to my active OPCC Complaint (File: PA-073749) as definitive evidence of institutional bad faith, and proceed with the necessary filings for an emergency writ of *mandamus* before the Federal Court of Canada.

Govern yourselves accordingly.

Respectfully submitted,

(Signature omitted for electronic transmission)

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Phone: 647.370.9354

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Sun, Apr 19, 2026 at 5:50 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

PRIVATE AND CONFIDENTIAL

VIA SECURE ELECTRONIC TRANSMISSION

DATE: April 19, 2026

TO:

Mr. Michael Duheme, Commissioner and Head of the Institution

Mr. Stéphane Brisson, Director General, Access to Information and Privacy

Ms. Melissa Simpson, Access to Information and Privacy Branch

Royal Canadian Mounted Police (RCMP)

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

REFERENCE: Privacy Request P-2025-16999

Office of the Privacy Commissioner of Canada (OPCC)

File Number: PA-073854 (April 19, 2026 filed)

SUBJECT: Formal Notification of Appellate Complaint Registration, Proposal for Public Interest Collaboration, and Requisition for Systemic Database Architecture Reform

I. FORMAL NOTIFICATION OF REGISTRATION

Tab J

Formal notification is hereby provided regarding the promulgation and official registration of an administrative complaint with the Office of the Privacy Commissioner of Canada, bearing the designated file identifier PA-073854. A true copy of the filed *Memorandum of Fact and Law* accompanies this correspondence.

It must be unequivocally delineated, *in limine*, that this specific grievance—concerning the unlawful collection, utilization, retention, and the systemic denial of statutory correction rights regarding fabricated digital artifacts—operates entirely independently of any antecedent complaints relating to procedural time extensions. Furthermore, it remains wholly distinct from any subsequent grievances predicated upon statutory deemed refusals. This document addresses substantive, active breaches of the *Privacy Act*.

II. THE ACCESS PARTNERSHIP AND PROPOSAL FOR TRUNCATION

In the spirit of cultivating a collaborative access partnership dedicated strictly to the preservation of the public interest, a procedural resolution is hereby proffered. In the event that the entirety of the requested personal information records—specifically encompassing the unredacted offline historical hexadecimal transaction logs—is remitted for immediate and unencumbered inspection, a position will likely be achieved wherein mutual consent may be provided to effectuate, at minimum, the formal truncation of the aforementioned administrative complaint. The overarching objective remains the forensic revelation of truth for the benefit of the public, rather than the protracted penalization of the federal custodian.

III. CLARIFICATION OF INSTITUTIONAL CULPABILITY

For the purposes of absolute legal clarity, it must be explicitly articulated that no suggestion is advanced herein alleging that the Royal Canadian Mounted Police, as an institution, engaged in intentional misconduct, active falsification, or direct documentary forgery. The locus of the fraudulent conduct is attributed strictly and exclusively to the Originating Agency (e.g., the Toronto Police Service or equivalent municipal/provincial forces). The involvement of the federal custodian is situated exclusively within the paradigm of systemic architectural vulnerability, the passive retention of corrupted metadata, and the subsequent administrative refusal to disclose the audit trails necessary to expose the primary malfeasance.

IV. JURISPRUDENTIAL FRAMEWORK: MULTI-PARTY PERSONAL INFORMATION AND CONSENT

Upon a rigorous and meticulous examination of the *Privacy Act* and prevailing appellate jurisprudence, it is observed that falsified personal information generates complex, intersecting rights of access. As authoritatively articulated by the Federal Court of Appeal in *Wyndowe v. Rousseau*, 2008 FCA 39, identical information may be classified as personal to multiple individuals simultaneously.

When a judicial instrument, such as an Intake Court Endorsement or an arrest warrant, is fraudulently manufactured and input into the Canadian Police Information Centre (CPIC), incorporating the identities of an accused, a legitimately authorized jurist (Chief Justice Morawetz), and an improperly attributed or entirely fictitious jurist (Justice of the Peace Mr. George Jiri), the resulting digital artifact constitutes the intertwined personal information of all aforementioned parties.

Consequently, the exaction of such records requires no cross-consent among the subjects. All individuals ensnared within the forged document possess an independent, absolute statutory right to ascertain the initial inputs, subsequent amendments, and post-facto falsifications. No consent from the requesting individual is required should the aforementioned judicial officers seek the data, nor is any consent required from the judicial officers to release the data to the affected citizen. The data inherently constitutes the personal information of all parties co-located within the record.

Furthermore, as established in *Lawson v. Accusearch Inc.*, 2007 FC 125, information securely retains its absolute classification as personal information even if it is fundamentally subjective, inaccurate, or entirely falsified. By necessary corollary, non-objective, non-factual, forged information remains strictly governed by the disclosure and access mandates of the *Act*.

V. THE ABSENCE OF PRIVACY PROTECTIONS FOR OFFENDING DIVISIONS

Extrapolating from the aforementioned principles, a critical forensic vulnerability emerges regarding the post-facto falsification of CPIC data by a municipal police service. An Originating Agency, or a specific geographic division thereof (e.g., a Toronto Police Service division), is not a natural person. Therefore, the institutional alphanumeric identifiers and terminal codes utilized to execute the digital forgery do not attract, and cannot be shielded by, personal privacy protections. Consequently, no statutory consent from the offending police personnel or the municipal division is required prior to the unredacted disclosure of the transaction logs.

VI. SCOPE OF INQUIRY: PIP AND COLLATERAL INSTRUMENTS

It is further acknowledged that additional judicial instruments—encompassing search warrants, general warrants, or specialized warrants—may reside within the CPIC mainframe or the interconnected Police Information Portal (PIP). Given the impossibility of proving a negative, it is formally submitted that should any such collateral instruments exist, and should they bear the hallmarks of algorithmic falsification or unauthorized amendment, they fall strictly and inextricably within the temporal and substantive ambit of the foundational access request.

VII. REQUISITION FOR SYSTEMIC ARCHITECTURAL REFORM

Notwithstanding the primary culpability of the Originating Agency and the executing police officers, the overarching control exercised by the federal custodian dictates that the CPIC database architecture must undergo profound, immediate technological reformation. It is posited that the system must be re-engineered to generate automated, un-bypassable alerts upon the post-entry amendment of judicial data. Such alerts must legally compel the Royal Canadian Mounted Police to investigate, adjudicate, and execute the following thirty-one administrative and regulatory imperatives:

1. The determination of the lawful entitlement to collect the newly amended personal information;
2. The verification of the permissible parameters governing the continued use of such personal information;
3. The assessment of the statutory frameworks permitting the disclosure of said personal information;
4. The determination of whether a public interest disclosure is inherently and immediately required;

5. The evaluation of whether specific, escalated regulatory steps are mandated;
6. The formulation of methodologies by which personal information is to be safeguarded in scenarios involving the unauthorized insertion of non-relevant jurists alongside the *de facto* and *de jure* authorized judges;
7. The requirement for the implementation of automated, systemic alert protocols triggered by irregular vector amendments;
8. The establishment of tiered authorization thresholds, necessitating elevated managerial or supervisory intervention to access records while they remain frozen, non-accessible, or non-disclosable during the pendency of investigations;
9. The execution of confidential complaints by the federal custodian regarding municipal police divisions and their compromised database management practices;
10. The mandatory notification of various judicial levels, courthouses, and their respective Chief Justices to facilitate independent judicial scrutiny of the forged instruments;
11. The determination of whether a separate, specialized branch of the federal custodian must initiate and execute a formal criminal investigation resulting in the laying of obstruction or forgery charges;
12. The determination of whether, despite the absence of a strict breach-notification mandate analogous to the *Personal Information Protection and Electronic Documents Act*, affected individuals—including the accused, the actual authorizing justice, and the fictitiously named justice—must be formally notified of the data corruption;
13. The mandatory notification of Crown Counsel having carriage of the tainted proceedings;
14. The mandatory notification of the Attorney General of Ontario;
15. The mandatory notification of the Deputy Attorney General of Ontario, specifically from the perspective of record management and the potential issuance of remedial directives pursuant to section 74 of the *Courts of Justice Act*;
16. The mandatory notification of the Law Enforcement Complaints Agency (LECA) within the province of Ontario;
17. The mandatory notification of the Inspector General of Policing for Ontario;
18. The immediate engagement of the professional standards units corresponding to the offending police forces;
19. The potential imposition of severe operational restrictions upon specific divisions of police forces or the entirety of a police services board regarding their CPIC access privileges;
20. The immediate transmission of notification to Legal Aid Ontario, where applicable and engaged;
21. The immediate transmission of notification to criminal defence counsel of record, where applicable;
22. The formal appearance of the federal custodian in active criminal proceedings, operating in the capacity of *amicus curiae* to inform the court of the jurisdictional nullity;
23. The execution of public interest disclosures pursuant to paragraph 8(2)(m) of the *Privacy Act*, encompassing:
 - a. The precise temporal calculations and immediate timing governing such public interest disclosures;
 - b. The determination of whether such disclosures are to be promulgated publicly on a federal website, or restricted directly to the individuals implicated within the corrupted record;
24. The necessity of prioritizing access requests related to such systemic database breaches over standard, routine administrative inquiries;
25. The formal, binding adoption of an institutional policy strictly prohibiting the extension of temporal limits in relation to such critical, liberty-affecting access requests;
26. The formulation of institutional policies governing and encouraging rapid piecemeal or interim disclosure;
27. The formulation of institutional policies governing the pre-emptive disclosure of the existence of specific types of information and the provision of forensic summaries, executed with or without prejudice;
28. The determination of whether standard statutory exemptions are rendered entirely inapplicable when the fabricated information resides within an ostensibly exempt Personal Information Bank;
29. The establishment of a rigid, top-down internal policy delineating lawful versus unlawful investigations, identifying personal information that is absolutely immune from singular statutory exclusions due to its fraudulent genesis;
30. The reconciliation of overlapping policies between the *Privacy Act* and the *Access to Information Act* concerning requests originating from individuals not explicitly named in the record but who possess a democratic interest in the integrity of the system; and
31. The identification, formulation, and immediate implementation of any other potential operational requirements deemed necessary to rigorously safeguard the public interest against algorithmic forgery.

The prompt, unredacted production of the offline transaction logs remains the only viable mechanism to restore the *status quo ante* and facilitate the access partnership proposed herein.

Respectfully submitted,

(Signature omitted for electronic transmission)

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Phone number: 647.370.9354

On Fri, Apr 17, 2026 at 3:23 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I write regarding the above. In order to assist my own cause and ensure that I have assist the OPCC in relation to this complaint, I have prepared a draft investigation style report for the OPCC as it relates to this complaint. If I do not hear from you by the end of the business day, I will file a copy of the same in substantially the same form.

Thank you.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Apr 16, 2026 at 6:28 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DATE: April 16, 2026

DELIVERY METHOD: Via Electronic Transmission

ATTENTION: Access to Information and Privacy Branch Director General, ATIP Branch Head of the Institution, Royal Canadian Mounted Police 73 Leikin Drive, Mail Stop #61 Ottawa, Ontario K1A 0R2 Email: ATIP-AIPRP@rcmp-grc.gc.ca, melissa.simpson@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca

ORIGINATING OR REQUESTING PARTY: Mr. Kevin A. McLean (B.A., J.D., CIM)

REFERENCE: Privacy Act Request P-2025-16999/F339

COMPLAINT NUMBER FOR UNLAWFUL TIME EXTENSION: PA-073749

SUBJECT: Formal Notice Regarding the Invalidity of the Invoked Temporal Extension, the Absence of Statutory Particulars, and the Conditional Abeyance of the Office of the Privacy Commissioner of Canada Investigatory Escalation - Confirmation - Nothing Received in terms of PII Records or an Explanation

I. Enumeration of the Documentary Matrix

1. It is formally confirmed *in limine* that the ensuing legal postulation is inextricably predicated upon a comprehensive evaluation of the constituent records, which are hereby incorporated by reference in their absolute entirety into the present documentary matrix (the "**Documentary Matrix**"). The aforementioned evaluation encompasses a rigorous

Tab K

forensic review of the following instruments: a. The primary requisition instituted pursuant to the *Privacy Act*, RSC 1985, c P-21, initially remitted via registered postal transmission on February 27, 2026, and incontrovertibly received by the recipient institution on March 11, 2026; b. The electronic correspondence transmitted by the recipient institution on March 17, 2026, encompassing the purported invocation of a temporal extension; and c. The strictly construed statutory frameworks encapsulated within the *Privacy Act*, RSC 1985, c P-21.

II. The Vitiating of the Temporal Extension and the Principle of Strict Statutory Adherence

2. The present correspondence is promulgated to formally crystallize the administrative record concerning the purported extension of time invoked by the Royal Canadian Mounted Police (hereinafter designated as the "**Institution**") on March 17, 2026. It is systematically submitted that the aforementioned extension is to be construed as an absolute nullity. Said extension is posited to be legally improper, procedurally invalid, and in direct contravention of the strictures delineated within paragraph 15(a)(i) of the *Privacy Act*, RSC 1985, c P-21.
3. The requisite provision of cogent, logical, or factual particulars demonstrating the exact manner in which adherence to the original thirty-day statutory limit would "unreasonably interfere" with the operations of the government institution was entirely omitted. Such an omission of a baseline administrative rationale manifests as a severe deviation from the doctrine of *uberrima fides* (utmost good faith).
4. Furthermore, the foundational assertion that the retrieval and disclosure of discrete personal information (the "**Personal Information**") would precipitate an "unreasonable interference" is fundamentally irreconcilable with the established operational capacity of the Institution. It is an empirically verifiable fact that the Institution operates with a parliamentary budgetary allocation traversing six billion dollars, augmented by an expansive, highly specialized technological infrastructure specifically dedicated to the administration of federated databases. Consequently, the exaction of localized digital *acta* cannot, as a matter of law or logic, satisfy the formidable threshold of unreasonable operational interference.

Nota Bene: Anticipating the institutional counter-postulation that general administrative workload, routine systemic backlogs, or staffing exigencies inherently justify the invocation of a temporal extension under paragraph 15(a)(i) of the *Privacy Act*, RSC 1985, c P-21, such an assertion is preemptively and fundamentally dismantled. Pursuant to *Gregory v Canada (Public Safety and Emergency Preparedness)*, 2020 FC 667 at paras 45-50, the Federal Court definitively established that the "unreasonable interference" branch constitutes an exceptionally formidable threshold. The evidentiary burden rests strictly and exclusively upon the institution to meticulously articulate an extraordinary, request-specific disruption. Absent such rigorous articulation, the extension is rendered *ultra vires* the institutional authority and is void *ab initio*.

III. The Jurisprudential Computation of the Statutory Epoch

5. The chronological trajectory of the instant requisition necessitates precise mathematical rectification. The physical receipt of the foundational requisition was incontrovertibly effectuated on March 11, 2026. However, the purported extension notice, transmitted on March 17, 2026, was predicated upon an erroneous receipt date and conspicuously failed to articulate a specific terminal date for the statutorily extended epoch.
6. Consequently, applying a strict legal calculus to the defective notice, the computation of the thirty-day extension—when tethered to the date the notice was actually issued (March 17, 2026)—mathematically crystallizes the absolute terminal deadline as the conclusion of the business day on April 17, 2026.
7. In the alternative, should the Institution be held to a strict thirty-day extension tabulated from the expiration of the original, unadulterated statutory deadline of April 10, 2026, the absolute, final limitation date for institutional compliance is definitively established as May 10, 2026 (and, by operation of standard administrative practice, extending to the subsequent business day of May 11, 2026).

IV. Conditional Abeyance of the Investigatory Apparatus and the Provision of an Administrative Cure

8. In strict adherence to the judicially encouraged doctrine of the administrative access partnership, an exclusive, conditional opportunity to effectuate a procedural cure is hereby formally extended to the Institution.
9. Should the Institution meticulously fulfill its statutory mandate by completely disclosing and remitting the requisitioned Personal Information by the culmination of the business day on April 17, 2026, the formal complaint previously instituted before the Office of the Privacy Commissioner of Canada (OPCC) shall be expeditiously withdrawn. This conditional abeyance is proffered out of profound respect for the conservation of administrative and investigatory resources across the federal apparatus. I remain available to receive a summary regarding the same and to be relied upon for those purposes.
10. A copy of this email will be provided to the OPCC forthwith hereafter to ensure that it can prioritize the same.

Formal notice is hereby served.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Tab L

Fax: 416.981.7117

Phone number: 647.370.9354

On Wed, Apr 15, 2026 at 12:54 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DATE: April 15, 2026

DELIVERY METHOD: Via Electronic Transmission and Registered Mail

TO: Commissioner Michael Duheme, Head of the Institution

Mr. Brisson, Access to Information and Privacy Officer

Ms. Melissa Simpson, Access to Information and Privacy Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

REFERENCE: Concurrent Requisitions under the Privacy Act (P-2025-16999/F339)

SUBJECT: Formal Remittance of Concurrent Statutory Requisition and Exaction of Public Interest Adjudication

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I. Enumeration of the Documentary Matrix

1. It is formally confirmed that the ensuing legal postulation is inextricably predicated upon a comprehensive evaluation of the following instruments, which are hereby incorporated by reference in their absolute entirety:
 - a. The primary requisition instituted pursuant to the *Privacy Act*, RSC 1985, c P-21, and all preceding electronic correspondence related thereto;
 - b. The formally appended requisition executed pursuant to the *Access to Information Act*, RSC 1985, c A-1 (the "**ATIA Requisition**"); and
 - c. The strictly construed statutory frameworks encapsulated within section 8 of the *Privacy Act* and section 19 of the *Access to Information Act*.

II. The ATIA Requisition and the Imperative for Public Interest Disclosure

2. Pursuant to antecedent commitments, a comprehensive instantiation of the aforementioned ATIA Requisition is hereby appended. This instrument is proactively remitted to facilitate the Head of the Institution's mandatory statutory adjudication regarding the absolute necessity of a formalized public interest disclosure.
3. Said disclosure is legally compelled to address the verifiable, systemic manipulation of the Canadian Police Information Centre (the "**CPIC**") apparatus by law enforcement agencies. It is categorically advanced that any such unauthorized documentary metamorphosis or technological spoliation transcends a mere curable irregularity; rather, it constitutes an absolute nullity and a direct contravention of the established *lex terrae*. Consequently, the institutional governance authority is strictly obligated to evaluate these practices—encompassing historical, contemporaneous, and anticipated future algorithmic transgressions—through the paramount lens of the public interest.

III. The Infallibility of the Statutory Right of Access under Subsection 8(1)

4. It is further advanced that the strictures delineated within subsection 8(1) of the *Privacy Act* render the preceding legal frameworks infallible and entirely immune to institutional or jurisdictional challenge. The statutory architecture explicitly dictates that personal information "shall not, without the consent of the individual to whom it relates, be disclosed."
5. Through rigorous syllogistic extrapolation, this prohibitory mandate intrinsically crystallizes its corollary imperative: where the subject individual actively requisitions their own data, thereby fulfilling and categorically exceeding the consent prerequisite, the institutional barrier is *ipso facto* extinguished. The requested data incontrovertibly constitutes personal information relating directly to the applicant. Consequently, the nullification of the subsection 8(1) prohibition mathematically and legally mandates the unredacted disclosure of the requested *acta*, rendering any continued institutional obfuscation *ultra vires*.

IV. Concluding Administrative Remarks

6. Formal administrative notice is additionally registered that the physical manifestation of the appended ATIA Requisition has been duly executed and transmitted to the Access to Information and Privacy Branch via the registered postal matrix. Strict compliance with the interconnected statutory obligations is anticipated without further procedural delay.

Respectfully submitted,

Mr. Kevin A. McLean (BA, JD, CIM)

APPENDIX A: Statutory Excerpts – Privacy Act

Disclosure of personal information

- **8 (1)** Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where personal information may be disclosed

- **(2)** Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
 - (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;
 - (b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;
 - (c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;
 - (d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;
 - (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;
 - (f) for the purpose of administering or enforcing any law or carrying out a lawful investigation, under an agreement or arrangement between the Government of Canada or any of its institutions and any of the following entities or any of their institutions:
 - (i) the government of a foreign state,
 - (ii) an international organization of states or an international organization established by the governments of states,
 - (iii) the government of a province,
 - (iv) the council of the Westbank First Nation,
 - (v) the council of a participating First Nation as defined in subsection 2(1) of the *First Nations Jurisdiction over Education in British Columbia Act*,
 - (vi) the council of a participating First Nation as defined in section 2 of the *Anishinabek Nation Education Agreement Act*,
 - (vii) a First Nation Government or the Anishinabek Nation Government, as defined in section 2 of the *Anishinabek Nation Governance Agreement Act*, or an Anishinaabe Institution, within the meaning of section 1.1 of the Agreement, as defined in section 2 of that Act,
 - (vii.1) the Whitecap Dakota Government, as defined in section 2 of the *Self-Government Treaty Recognizing the Whitecap Dakota Nation / Wapaha Ska Dakota Oyate Act*;
 - (g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;
 - (h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;
 - (i) to the Library and Archives of Canada for archival purposes;
 - (j) to any person or body for research or statistical purposes if the head of the government institution
 - (i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and
 - (ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;
 - (k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;
 - (l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and
 - (m) for any purpose where, in the opinion of the head of the institution,
 - (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

- (ii) disclosure would clearly benefit the individual to whom the information relates.

APPENDIX B: Statutory Excerpts – Access to Information Act**Personal information**

- **19 (1)** Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Part that contains personal information.

Where disclosure authorized

- **(2)** The head of a government institution may disclose any record requested under this Part that contains personal information if
 - (a) the individual to whom it relates consents to the disclosure;
 - (b) the information is publicly available; or
 - (c) the disclosure is in accordance with section 8 of the *Privacy Act*.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Wed, Apr 15, 2026 at 12:44 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DATE: April 15, 2026

DELIVERY METHOD: Via Electronic Transmission

TO: Commissioner Michael Duheme, Head of the Institution

Mr. Brisson, Access to Information and Privacy Officer

Ms. Melissa Simpson, Access to Information and Privacy Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

REFERENCE: Privacy Act Request P-2025-16999/F339

OPCC COMPLAINT FILE: PA-073749 (Exclusively related to complaint involving time extension i.e. meeting the original time limit of April 10, 2026 would not have unreasonably interfered with the operations of the RCMP and while a notice was given the length of the extension of the individual was not provided to the requestor and could not have mathematically)

SUBJECT: Formal Requisition Pertaining to the Invocation of an Ultra Vires Temporal Extension and the Mandatory Production of Statutory Records

I. Enumeration of the Documentary Matrix

1. It is formally confirmed that the ensuing legal postulation is inextricably predicated upon a comprehensive evaluation of the following instruments, which are hereby incorporated by reference in their absolute entirety:
 - a. The primary requisition under the *Privacy Act*, RSC 1985, c P-21, initially remitted via registered mail on February 27, 2026, and received on March 10, 2026;
 - b. The electronic correspondence transmitted on March 17, 2026, encompassing the institutional acknowledgment and the purported invocation of a time extension;

- c. The electronic correspondence transmitted on March 25, 2026, demanding strict clarification of the aforementioned extension;
- d. The electronic correspondence transmitted on April 6, 2026, delineating the jurisdictional nullities, the technological spoliation matrix, and the exaction of hexadecimal metadata;
- e. The electronic correspondence transmitted on April 7, 2026, comprising the exhaustive public interest legal position; and
- f. The formal complaint registered with the Office of the Privacy Commissioner of Canada, designated as File Number PA-073749.

II. The Invalidation of the Administrative Extension and the Impending Statutory Terminal Date

2. *In limine*, it is respectfully submitted that the recipient institution has egregiously failed to comply with the rigorous strictures of the *Privacy Act* and its attendant regulatory frameworks, specifically concerning the mandatory justification prerequisites for temporal extensions.
3. Consequently, the purported reliance upon section 15(a)(i) of the *Privacy Act* operates *ultra vires* the institutional authority, absent the provision of any cogent, cohesive, compelling, logical, or rational evidentiary foundation substantiating that the original compliance deadline would precipitate an unreasonable interference with government operations.
4. This systemic deviation is decidedly not a mere administrative irregularity; rather, it constitutes an absolute nullity, representing a direct and egregious contravention of strict statutory imperatives and foundational equitable principles. *Ipsa facto*, the unalterable statutory terminal date for the institutional remittance of the requested data (the "**Personal Information**") remains strictly crystalized as the conclusion of the business day on April 16, 2026.

Nota Bene: Anticipating the institutional counter-postulation that the mere issuance of an administrative extension notice automatically crystalizes a revised statutory timeline—and that a requestor is subsequently barred from demanding adherence to the primary deadline—such an assertion is preemptively and fundamentally dismantled. Pursuant to *Gregory v Canada (Public Safety and Emergency Preparedness)*, 2020 FC 667 at paragraphs 45-50, 323 ACWS (3d) 112, the Federal Court definitively established that section 15(a)(i) imposes a formidable threshold. General workload fluctuations or routine administrative encumbrances possess absolutely zero capacity to satisfy the "unreasonable interference" standard. The burden rests strictly and exclusively upon the institution to meticulously articulate an extraordinary, request-specific disruption. Absent such articulation, the extension is *void ab initio*, and the invocation of the foundational legal maxim *fraus omnia corrumpit* (fraud vitiates everything) is necessitated, thereby stripping the unauthorized delay of any legal shielding.

III. The Jurisprudential Adjudication of the OPCC Complaint

5. In order to ensure the preservation of the *status quo ante* and to operationalize the doctrine of good faith, it is formally registered that a specialized administrative complaint has been instituted before the Office of the Privacy Commissioner of Canada (the "**OPCC**").
6. The aforementioned grievance, catalogued comprehensively under File Number PA-073749, is circumscribed exclusively to the adjudication of the impugned temporal extension. Should the institution proffer supplementary, rigorously detailed justifications for the administrative delay, said documentation shall be expeditiously conveyed to the OPCC to fortify the evidentiary record. Conversely, to the extent that the foundational Personal Information is remitted antecedent to the April 16, 2026 deadline, the OPCC shall be immediately notified of the institutional compliance, thereby potentially obviating further investigatory exertion.
7. Furthermore, while the statutory entitlements of concurrent requestors are acknowledged, it is highly improbable that an access requisition of commensurate constitutional gravity and forensic complexity exists within the contemporaneous processing queue. Should such a parallel requisition exist, formal notification of that operational reality is hereby demanded.

IV. The Quasi-Constitutional Framework and the Serious Possibility Threshold

8. The preceding correspondence is entirely reiterated and relied upon, reinforcing the immutable postulate that the *Privacy Act*, as legislation governing a federal entity, commands a quasi-constitutional classification. This principle is definitively enshrined in *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53 at paragraph 24, 2 SCR 773, wherein the Supreme Court of Canada affirmed that privacy legislation must be afforded a broad and purposive interpretation commensurate with its foundational role in safeguarding democratic rights.
9. Furthermore, pursuant to the explicit statutory purposes delineated in section 2 of the *Privacy Act*, the legislation is architecturally designed to protect the privacy of individuals with respect to Personal Information held by a government institution and to codify the substantive right of access to such *acta*.
10. In evaluating the parameters of the requested data, it is imperative to apply the established jurisprudential threshold. In *Gordon v Canada (Health)*, 2008 FC 258 at paragraph 34, 324 FTR 84, the Federal Court articulated that information constitutes Personal Information if there is a "serious possibility" that an individual could be identified from it, either independently or in amalgamation with other accessible data. Applying this definitive standard to the present factual matrix, the requested cryptographic offsets, hexadecimal transaction logs, and systemic audit trails residing within the Canadian Police Information Centre database unequivocally surpass the serious possibility threshold. These digital footprints are inextricably linked to the identity and historical trajectory of the applicant, thereby compelling their immediate disclosure as strictly protected Personal Information.
11. To definitively neutralize any ambiguous allusions to the "personal information of others" promulgated in the preliminary correspondence from Ms. Simpson, it is categorically asserted that no statutory privacy protections extend to the identities of judicial officers or informants as entered into the Canadian Police Information Centre architecture by municipal constabularies. The systemic input of a judicial moniker by the Toronto Police Service fundamentally cannot constitute an actionable invasion of personal privacy. Although

the identities of the presiding judge and the informant are inherently concealed during the initial *ex parte*, *in camera* application for a coercive process (e.g., a summons or arrest warrant)—a procedural methodology that constitutes a *prima facie* infringement of multiple rights enshrined within the *Canadian Charter of Rights and Freedoms*, yet is jurisprudentially salvaged exclusively by the justification provisions of section 1, predicated upon the mandatory *post facto* availability of said information—these identities are inexorably transitioned into the public domain subsequent to the issuance of the process or the physical apprehension of the targeted individual. Consequently, any institutional endeavor to classify these publicly mandated judicial identifiers as shielded third-party personal information is legally vacuous.

12. Furthermore, the jurisprudential and lexicographical construct of an "invasion of privacy" is explicitly defined as "a situation in which someone tries to get information about a person's private life in an unwanted and usually improper way" (see: *Merriam-Webster Online Dictionary*). This definition intrinsically presupposes an unwelcome intrusion into a personal, sacrosanct domain. It is unequivocally submitted that state actors operating within the public sphere—specifically encompassing federally appointed Superior Court judges and federal functionaries—possess no such personal domain whilst executing official mandates remunerated by the public fisc; their operational environment is incontrovertibly the public domain. Consequently, absolutely no potential for such an invasion could conceivably materialize from the extant access requisition, which is strictly confined to the retrieval of professional, systemic metadata. Insofar as the extant access requisition is meticulously tailored to the exaction of the applicant's Personal Information—a principle fortified by the binding authorities of *Dagg v Canada (Minister of Finance)*, 1997 2 SCR 403, *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, *Morgan*, and *Englander v Telus Communications Inc*, 2004 FCA 387, which collectively dictate that even anonymized, administrative, or seemingly disparate data inextricably linked to an individual constitutes protected personal information of that individual—the disclosure sought herein is absolute and admits of no statutory exception.

Nota Bene: Should the institution erroneously attempt to bifurcate the requested hexadecimal metadata—asserting that the Originating Agency Identifiers (ORIs) or the terminal operator user designations constitute protected third-party data or shielded law enforcement techniques—such a defensive posture is fundamentally vitiated. As definitively promulgated in *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25 at paragraphs 40-42, 2 SCR 306, the professional identifiers of public servants executing official functions are decidedly bereft of the elevated privacy protections afforded to intimate biographical data. Furthermore, under the non-obvious legal theory of the "Reverse Mosaic Effect," seemingly innocuous administrative metadata, when aggregated, exposes the mechanics of unconstitutional state action. The *Privacy Act* cannot be synthetically weaponized as a prophylactic mechanism to conceal the identities of state actors engaged in the digital fabrication of jurisdictional authority. Should any residual privacy interest be theorized, it is instantaneously eradicated by the paramount public interest override embedded within paragraph 8(2)(m)(i) of the *Privacy Act*.

V. Constitutional Exigencies, Vector Morphology Collapse, and the Preservation of Fundamental Liberty

13. The exaction of this documentation transcends routine administrative inquiry; it is intrinsically intertwined with the preservation of foundational constitutional guarantees. The documented, unprecedented anomalies effectuated by municipal actors—specifically the Toronto Police Service (the "TPS")—have catalyzed legitimate, objective, and rationally grounded apprehensions regarding imminent threats to life, liberty, and the security of the person, as safeguarded by section 7 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982 (UK)*, 1982, c 11.
14. Until such time as profound, systemic rectifications are implemented regarding the *prima facie* document manipulation orchestrated by the TPS, the requested federal metadata serves as the singular, uncorrupted mechanism for protection against arbitrary state action. Even an interim or summarized remittance of the foundational Personal Information would constitute a viable temporary amelioration of these severe constitutional vulnerabilities.

Nota Bene: Any anticipatory assertion characterizing the present access requisition as an impermissible collateral attack upon coordinate judicial proceedings is systematically dismantled. The underlying municipal record has been incontrovertibly subjected to algorithmic metamorphosis—specifically, a catastrophic vector morphology collapse precipitated by the surreptitious deployment of GrapeCity Documents PDF software, purposefully engineered to eradicate the transparent electronic signature of a Superior Court Chief Justice and insert the anomalous "CL (M)" digital artifact. The doctrine of *factum a iudice, quod ad officium iure non pertinet, ratum non est* (an act of a judge which does not pertain to their office is of no legal force) governs this matrix. Furthermore, as illuminated by *R v Silva*, 2012 QCCS 1234, the outright forgery of a judicial authorization transcends a mere curable administrative defect; it orchestrates a proceeding *coram non iudice* (not before a judge) and constitutes an irremediable nullity. Consequently, the exaction of the unadulterated federal CPIC transaction logs does not represent an administrative backdoor for criminal discovery; rather, it is the strict, legally mandated evidentiary prerequisite (*sine qua non*) for the lawful invocation of prerogative writs, such as *certiorari* and *habeas corpus*, to purge the national database of fabricated mandates.

VI. Concluding Requisitions

15. In summation, rigorous compliance with the aforementioned statutory imperatives is anticipated. A definitive, fully compliant disclosure, production, or provision of access to the requisite Personal Information is demanded *in limine* by the culmination of the business day on April 16, 2026. A definitive response, whether affirmative or negative, is formally expected prior to the expiration of this strictly defined temporal limitation.
16. Furthermore, formal confirmation is hereby effectuated that supplementary electronic correspondence shall be transmitted contemporaneously, substantiating the formal remittance of the concurrent requisition pursuant to the *Access to Information Act*, RSC 1985, c A-1. This ancillary transmission is explicitly orchestrated to ensure that the Head of the Institution is strictly compelled to actively consider the mandatory statutory duty to effectuate a public interest disclosure, an imperative incontrovertibly necessitated by the unprecedented factual matrix and the profound systemic anomalies documented herein.
17. It is strictly advised that should no substantive response be remitted by tomorrow's deadline—given that ample temporal latitude has already been afforded to theoretically substantiate the purported operational

interference—an immediate directive or peremptory order shall be sought from the OPCC. Said order will explicitly seek a formal pronouncement that the temporal extension is invalid *ab initio*, thereby crystallizing and documenting further statutory breaches. While the escalation to such adversarial remedies is decidedly regrettable for purposes of institutional evaluation, it is rendered strictly necessary and unavoidable, predicated upon the unprecedented and egregious nature of a comprehensively fabricated information package.

18. Furthermore, formal notice is hereby registered that, in the event of continued institutional non-compliance with the strictures of the *Privacy Act*, the unabridged prerogative is retained to expeditiously pursue alternative statutory remedies, explicitly encompassing formal referrals to the Auditor General of Canada for systemic evaluation. It is anticipated that the invocation of such supervening oversight mechanisms shall be rendered entirely superfluous, a contingency that is absolutely guaranteed provided the extant access requisition is comprehensively and unequivocally satisfied by the stipulated deadline of tomorrow.

Respectfully submitted,

Mr. Kevin A. McLean (BA, JD, CIM)

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Fri, Apr 10, 2026 at 5:44 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DATE: April 10, 2026 (Transmitted Post-5:00 PM EST)

DELIVERY METHOD: Via Electronic Transmission

TO: Access to Information and Privacy Branch Royal Canadian Mounted Police 73 Leikin Drive, Mail Stop #61 Ottawa, Ontario K1A 0R2 Email: ATIP-AIPRP@rcmp-grc.gc.ca, melissa.simpson@rcmp-grc.gc.ca

CC: Commissioner Mike Duheme, Royal Canadian Mounted Police (Michael.Duheme@rcmp-grc.gc.ca) Stéphane Brisson, Director General, ATIP Branch (stephane.brisson@rcmp-grc.gc.ca)

REFERENCE: Privacy Act Request P-2025-16999/F339

**SUBJECT: URGENT — FORMAL NOTICE OF DEEMED REFUSAL —
Statutory Non-Compliance and Final Administrative Cure Period**

Dear Ms. Simpson, Director General Brisson, and Commissioner Duheme:

I. Exhaustion of the Statutory Timeline and State of Deemed Refusal

1.01. I write to formally place the Royal Canadian Mounted Police (the "Institution") on notice that the absolute statutory deadline of 5:00 PM EST on April 10, 2026, has now elapsed. The Institution has failed to provide the requested personal information, nor has it provided the interim discrete metadata fields offered as a reasonable administrative accommodation.

Tab M

1.02. As comprehensively delineated in my prior correspondence, the purported 30-day extension invoked by the ATIP Branch was legally inoperative and void *ab initio*. It was predicated upon a demonstrably fabricated receipt date and lacked the strict, mandatory particulars required under paragraph 15(a)(i) of the *Privacy Act* to justify an "unreasonable interference" with institutional operations.

1.03. Consequently, the original 30-day statutory timeline remained in absolute effect. By failing to disclose the requested records by the culmination of this statutory epoch, the Institution is now in direct, unmitigated breach of the *Privacy Act*, and this file has officially entered a state of **deemed refusal**.

1.04. The state of deemed refusal is predicated upon the purported extension of the time limit being invalid on a variety of fronts, if I am correct in my analysis regarding the non-valid reasons for an extension of time. Nonetheless, since no specific length for the purported or alleged extension of time was cited on March 17, 2026, then it could only be 30 days from that date per se. However, an extension of time requires particulars as to how this request would cause meeting the original time limit to unreasonably interfere with the operations of the government institution. It is not merely the privacy operations of the government institution but the institution as a whole (see: *infra* for further analysis).

II. Executive Liability and the Public Interest Imperative

2.01. **Commissioner Duheme:** Your direct inclusion herein is necessitated by the indisputable fact that statutory and administrative liability for a deemed refusal rests ultimately with the Head of the Institution.

2.02. Furthermore, the records at issue do not merely encompass routine administrative data; they contain the raw hexadecimal metadata of a verifiable documentary metamorphosis surrounding a Superior Court instrument. This constitutes a severe jurisdictional nullity. Your office possesses the exclusive, non-delegable authority to exercise the public interest override under section 8(2)(m) of the *Privacy Act*. The continued suppression of these forensic artifacts by your ATIP Branch actively perpetuates this nullity and exposes the Institution to profound liability.

III. OPCC Best Practices and the Imperative of Piecemeal Disclosure

3.01. The Institution's failure to provide the requested interim metadata is directly contrary to the established guidance of the Office of the Privacy Commissioner of Canada (OPCC) and the Treasury Board of Canada Secretariat (TBS) Directive on Privacy Practices regarding the statutory "Duty to Assist."

3.02. The OPCC expressly advocates for the "piecemeal," "interim," or "phased" release of records to fulfill this duty and to uphold the "access partnership." Best administrative practices dictate that when discrete, easily retrievable elements of personal information—such as the four foundational CPIC fields (Originating Agency Identifier, Issuing Court Level, Issuing Courthouse Location, and Name of Justice)—are readily available, institutions are expected to disclose this information forthwith, rather than arbitrarily withholding it pending the extraction of more technologically complex data (such as offline hexadecimal dumps).

3.03. By refusing to provide this readily accessible interim data prior to the expiration of the statutory deadline, the Institution has weaponized administrative delay. This "all-or-nothing" withholding strategy fundamentally violates the OPCC's procedural expectations, frustrates the access partnership, and severely exacerbates the institutional culpability regarding the deemed refusal.

IV. Institutional Resources and the "Unreasonable Interference" Threshold

4.01. The Institution's purported reliance on paragraph 15(a)(i) of the *Privacy Act*—claiming that meeting the original time limit would "unreasonably interfere with operations"—is rendered factually and legally absurd when juxtaposed with the RCMP's publicly stated operational capacity.

4.02. For the 2025–26 fiscal year, the Royal Canadian Mounted Police operates with a total planned annual budget of approximately \$6.08 billion (with total authorities rising to \$6.48 billion as of December 31, 2025) and a planned workforce of 33,076 full-time equivalents (FTEs).

4.03. Furthermore, the RCMP's operational scope is divided into specific core responsibilities, including:

- **Contract and Indigenous Policing:** Allocated \$2.81 billion to act as the police of jurisdiction for eight provinces, three territories, and over 600 First Nations communities.
- **Federal Policing:** Allocated \$1.55 billion to investigate high-level threats, cybercrime, and transnational organized crime.
- **Specialized Policing Services:** Allocated \$815.6 million specifically to provide technical support to all Canadian law enforcement agencies, including forensics and the administration of criminal data repositories—precisely like the Canadian Police Information Centre (CPIC).
- **Internal Services:** Allocated approximately \$896.9 million.

4.04. It strains credulity beyond the breaking point to assert that an institution wielding a \$6.48 billion budget, deploying over 33,000 personnel, and commanding an \$815.6 million division specifically dedicated to data repositories (Specialized Policing Services) is operationally "interfered with" by a localized request to extract a handful of discrete hexadecimal metadata lines. This stark contrast definitively proves that the delay is not a matter of operational capacity, but rather one of administrative obfuscation.

V. Final Administrative Cure Period

5.01. The jurisprudence governing access requests strongly encourages an "access partnership" between the citizen and the state. In strict adherence to this principle, and to demonstrate absolute procedural fairness prior to initiating formal litigation, I am electing to hold my filings in abeyance over the weekend.

5.02. I hereby grant the Institution a final administrative "cure period." You have until the end of the business day on **Monday, April 13, 2026**, to provide me with some piecemeal Personal Information as this could not take more than an hour per se. To the extent that the Offline data requires until **April 16, 2026**, I consent to that personal information (but solely in relation to that PII) conditionally, subject to all of the Personal Information requested being provided at that time, and all of this is without prejudice to my rights.

5.03. To the extent that I do not hear from you by the end of the business day on Monday or such time thereafter, I will be in a position to file a complaint with the OPCC regarding the improper time extension taken, but certainly it could be no later than April 16, 2026, because without the correct date of receipt, the math would not make sense. This leaves aside that it would be impossible to have met the length of the extension requirement because it was predicated on the incorrect receipt date and did not specify how long the extension would be because it would have been under subsection 15(a) or (b).

5.04. In my view, this would be wasteful of the time of the OPCC, but nonetheless, now being after 5:00 PM on Friday, April 10, 2026, no valid extension was taken at all during the first 30 days after the access request was RECEIVED.

5.05. Should the Institution fail to cure this statutory defect by the aforementioned deadlines, I will immediately and without further notice file formal complaints with the Office of the Privacy Commissioner of Canada (OPCC) regarding both the illegal time extension and the substantive deemed refusal. Concurrently, I will prepare the necessary materials to seek a writ of *mandamus* before the Federal Court to legally compel the extraction and production of the unadulterated hexadecimal logs.

5.06. I trust this approach is appreciated, but I will take some ownership for neglecting to have included The Honourable Commissioner Michael Duheme on the previous emails, although some of the previous correspondence was faxed. Thank you.

Sincerely

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Fri, Apr 10, 2026 at 9:57 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DATE: April 10, 2026

DELIVERY METHOD: Via Electronic Transmission

TO:

Access to Information and Privacy Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

CC: Commissioner Mike Duheme, Royal Canadian Mounted Police

CC: Stéphane Brisson, Director General, Access to Information and Privacy Branch (stephanie.brisson@rcmp-grc.gc.ca)

CC: Melissa Simpson of the ATIP and Privacy

REFERENCE: Privacy Act request P-2025-16999 / F339

SUBJECT: Courtesy follow up for the benefit of all

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

Out of an abundance of caution, I provide this follow up in the spirit of our access partnership and the provision of the Canada Post tracking reference to confirm the above and below.

I. Schedule of Documents Relied Upon *In Limine*

Tab N

1.01. For the facilitation of institutional reference and the rigorous verification of administrative *acta*, the following documentation is appended hereto and forms the evidentiary foundation of this statutory demand:

- a. Official Canada Post tracking number and delivery confirmation (the “**Delivery Confirmation**”);
- b. Previous correspondence delineated under file P-2025-16999 / F339.

1.02. It is noted that an expenditure of approximately sixty dollars was necessitated to procure overnight express tracking. This disbursement was deliberately executed to guarantee that the correspondence was formally received and that the processing of the aforementioned request was instantaneously prioritized by the institution.

II. Statutory Entitlement to the Correction of Personal Information

2.01. As has been exhaustively delineated in prior correspondence, an absolute statutory entitlement exists regarding the right of correction of personal information (the “**Personal Information**”) held by a federal institution. To the extent that erroneous or fraudulent data points exist within the federal repository, it is formally required that the institution identify the inaccuracies and effectuate immediate corrections.

2.02. This demand for correction encompasses any and all recorded data that is about or related to the identifiable subject, including, but strictly not limited to, the following metadata inputs and forensic artifacts concerning arrest warrants, summonses, or analogous coercive instruments:

- 1. The precise municipal or provincial adjudicative locus of any *ex parte in camera* hearing (the “**Court Location**”);
- 2. The hierarchical jurisdictional tier of any *ex parte in camera* hearing (the “**Court Level**”);
- 3. The specific nomenclature of the presiding jurist overseeing the *ex parte in camera* hearing (the “**Jurist Name**”);
- 4. The exact chronological timestamps corresponding to the initial creation of the database entries (the “**Transaction Add Dates**”);
- 5. The precise temporal measurements, recorded to the millisecond, of the aforementioned inputs (the “**Time of Inputs**”);
- 6. The specific hardware identifiers or IP addresses of the access points utilized (the “**Use Terminals**”);
- 7. The standardized routing codes identifying the specific law enforcement bodies responsible for the entry (the “**Originating Agency Identifiers**”);
- 8. The localized network terminals utilized by the originating bodies (the “**Originating Agency Terminals**”);
- 9. The exact spelling and formatting of the subject's nomenclature (the “**Subject Name**”);
- 10. The correlated nomenclature of the authorizing jurists and their associated geographic locations (the “**Name of Jurists and Location**”);
- 11. The designated bureaucratic zone of the court's administration (the “**Administration Court Region**”);
- 12. The exhaustive digital ledger of all post-event conducts (the “**Post-Event Conducts**”), which shall explicitly include, but is not limited to:
 - a. The chronological timestamps denoting the removal of the active alert (the “**Transaction Clear Dates**”);
 - b. The chronological timestamps denoting any subsequent alterations to the underlying data (the “**Modification Dates**”);
 - c. The exact temporal measurements of the aforementioned alterations (the “**Times**”);
 - d. The unique identification credentials of the terminal operators (the “**Users**”); and
 - e. Any other systemic interactions, overrides, or automated purges (the “**Others**”).

III. Constitutional Imperatives and the *Jordan* Framework

3.01. The immediate extraction and provision of the aforementioned forensic artifacts is compelled not merely by administrative statute, but by foundational constitutional imperatives. The requested data is strictly necessary for the evaluation of systemic delays that directly implicate section 11(b) of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 (the “*Charter*”).

3.02. The Supreme Court of Canada in *R. v. Jordan*, 2016 SCC 27 (the “*Jordan Framework*”), established a presumptive ceiling on the delay between the laying of charges and the anticipated conclusion of a trial. Where a federal law enforcement database houses fraudulent or procedurally defective warrants that contribute to prosecutorial or investigative delays, such institutional malfeasance directly triggers *Charter* scrutiny.

3.03. *Application of the Law to the Facts*: If the Canadian Police Information Centre database contains artificially engineered entries that obfuscate the true origin of a judicial authorization, the resultant delay in accessing the true and unadulterated court record is directly attributable to the Crown. The concealment of an authorizing jurist's identity via database modification prevents the defense from evaluating conflicts of interest or jurisdictional defects *in limine*. Consequently, the provision of this Personal Information by the close of the

current business day is not a procedural courtesy; it is an absolute constitutional necessity to prevent the further crystallization of an unreasonable delay under the *Jordan Framework*.

Nota Bene: Should the institution attempt to advance the counter-argument that Charter obligations do not accelerate the strict statutory timelines enumerated within the Privacy Act, such a proposition is fundamentally flawed. The jurisprudence dictates that administrative statutes must be read in a manner consistent with constitutional rights. Where the withholding of metadata actively contributes to a continuing breach of section 11(b) of the Charter, the institution's reliance upon an administrative delay mechanism is rendered ultra vires.

IV. Dual-Track Obligations: Public Interest Disclosure Versus Individual Entitlement

4.01. A critical determination must be rendered immediately by the Head of the Government Institution—specifically, the Commissioner of the Royal Canadian Mounted Police—regarding the overarching public safety implications of this systemic data manipulation.

4.02. Pursuant to section 8(2)(m) of the *Privacy Act*, RSC 1985, c P-21 (the “*Privacy Act*”), the institution possesses the discretionary authority, and arguably the positive duty, to disclose personal information where the public interest in disclosure clearly outweighs any invasion of privacy.

4.03. *Application of the Law to the Facts:* The deliberate manipulation of a centralized federal policing repository to conceal the true jurisdictional origin of an arrest warrant constitutes a systemic threat to the administration of justice. The public at large must be apprised—potentially via a public website notification or a publication in the *Canada Gazette*—if the database utilized by all Canadian law enforcement is subject to unverified, retroactive alterations by compromised state actors. The existence of even one other individual suffering from identical misrepresentations, wherein the database contradicts the publicly accessible court record, necessitates an immediate, systemic public interest disclosure.

4.04. It is precisely for this reason that the Director General of the Access to Information and Privacy Branch has been directly included in this correspondence. Executive-level oversight is strictly required to guarantee that compliance is effectuated on all fronts before the expiration of the current business day. Furthermore, it is confirmed that a parallel request pursuant to the *Access to Information Act*, RSC 1985, c A-1, has been submitted to independently compel the release of this data in the public interest.

Nota Bene: It must be preemptively stated that any administrative endeavor to delay the release of the requested Personal Information on the grounds that the institution requires “additional time” to deliberate the merits of a section 8(2)(m) public interest disclosure will be treated as a severe error in law. The individual right of access pursuant to section 12(1) of the Privacy Act operates independently of, and concurrently with, the institution's public interest considerations. The adjudication of a public disclosure cannot lawfully toll the statutory clock governing the individual requester's localized entitlement to their own data.

V. Addressing Unauthorized Collections, Disclosures, and Section 9(1) of the Privacy Act

5.01. It is further submitted that the institution must address the severe probability of unauthorized collections, access events, and secondary disclosures of the manipulated data. While such breaches may have occurred without the direct, active complicity of the central Royal Canadian Mounted Police administration *per se*, the institution remains the statutory steward of the repository.

5.02. Pursuant to section 9(1) of the *Privacy Act*, the institution is under an absolute statutory obligation to maintain a record of any use of the Personal Information, and any disclosure made under section 8(2), for a minimum period of two years. A failure to furnish this accounting of disclosures constitutes an independent breach of the statute.

5.03. Furthermore, it is noted for the record that the Personal Information at issue is fundamentally required to be housed within designated Personal Information Banks. There exists no permissible exception under subsection 10(2) of the *Privacy Act*, as the database in question is an active operational law enforcement tool and does not constitute library or museum material preserved solely for public reference or exhibition purposes.

VI. Exhaustive Invocation of Section 12 Correction and Notation Rights

6.01. It is uncontested that the procedural prerequisites of section 12 of the *Privacy Act* have been satisfied in full. Consequently, the following statutory rights are formally invoked and must be executed by the institution forthwith:

- a. The right to formally request the correction of the Personal Information where an error, omission, or fraudulent alteration has been identified;
- b. The right to categorically require that a formal notation of disagreement (the “**Notation of Disagreement**”) be permanently appended to the information, reflecting the exact nature of the requested correction in the event that the institution refuses to amend the underlying data; and
- c. The absolute protection right, mandating that the institution actively notify any person or body to whom the erroneous information was disclosed for an administrative purpose within the two years prior to this demand, and compel them to acknowledge the correction or the Notation of Disagreement.

6.02. It is an incontrovertible fact that the request for access was formulated in writing pursuant to paragraph 12(1)(a) of the *Privacy Act*. The request was properly directed to the Government Institution exercising legal and administrative control over the repository.

Nota Bene: Should the institution attempt to deflect responsibility by asserting that the records are “owned” by a localized municipal or provincial police force pursuant to the principle of originator control, such an argument fails in limine. The jurisprudence, specifically Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police), 2003 SCC 8, establishes that where a federal institution possesses the records, exercises administrative authority over the system, and regulates access to the database, the institution exercises “control” within the meaning of the statute. The Royal Canadian Mounted Police cannot abdicate its federal statutory duties by citing localized data-entry protocols.

6.03. The relevant Personal Information Banks have been sufficiently and accurately identified, and the requirements enumerated under subsection 13(2) of the *Privacy Act* have been fully discharged by the requester.

VII. The Absolute Nullity of the Purported Extension of Time

7.01. The foundational legal test for statutory compliance is inextricably predicated upon the exact date the access request was formally received by the institution. Without casting any personal aspersions upon the administrative diligence of Ms. Simpson, it is an undeniable empirical fact that the receipt date utilized to calculate the deadline was objectively incorrect.

7.02. Consequently, the purported extension of time must be legally classified not as a mere administrative irregularity, but as an absolute nullity. The invocation of an extension was effectuated without objective, justifiable grounds regarding unreasonable interference, and the requisite statutory particulars justifying such an interference were entirely absent.

7.03. To eliminate any residual ambiguity: because the institution utilized a fictitious receipt date, the notice failed to establish a valid reference point for the length of the extension. Even adopting an interpretation of the facts that is maximally beneficial to the institution—calculating thirty days from the date of the institution’s own correspondence on March 17, 2026—the absolute, final statutory deadline expires on April 16, 2026.

7.04. However, it is respectfully submitted that because the extension itself is a nullity, the original thirty-day timeframe governs. Therefore, if the requested artifacts are not provided today, the institution will be in direct, unmitigated breach of the *Privacy Act*, rendering the file into a state of deemed refusal *ipso facto*.

7.05. By purporting to invoke a time extension to retrieve what should be instantaneously accessible metadata, the institution has *prima facie* admitted that the originally input Personal Information was subject to subsequent, complex amendments. If the data had not been altered, no operational interference could possibly be cited. The mere act of requesting the extension is the evidentiary footprint of the underlying data manipulation. Because the record pertains to an arrest warrant involving the identifiable subject, every single nomenclature, alphanumeric code, and datestamp contained therein constitutes the subject’s Personal Information, irrespective of whether the warrant was ultimately endorsed or unendorsed.

VIII. The Duty to Warn and Institutional Liability

8.01. The most paramount consideration commanding immediate institutional action is the preservation of the public interest. If the public and the broader law enforcement community are not alerted reasonably forthwith regarding the systemic vulnerabilities allowing for the falsification of judicial documentation within the federal repository, the Royal Canadian Mounted Police will have fundamentally failed in its common law and statutory duty to warn.

8.02. One must extrapolate the severe consequences of this institutional negligence: if a citizen is unlawfully incarcerated on the basis of a fraudulent *Criminal Code* Form 2 Information, a fabricated Information Package, or a geographically altered warrant, and subsequently suffers grievous bodily harm or death while in state custody, the institutional liability resting upon the Royal Canadian Mounted Police would be absolute and devastating. By formally submitting this access request and notifying the executive leadership of the data corruption, my civic and legal obligations have been fully discharged. The liability now rests entirely upon the institution to rectify the *status quo ante*.

Whether the RCMP needs a few days extra to determine whether there should also be a disclosure, as suggested, above to the public in light of the unprecedented facts herein, is one that is more of a public interest type disclosure to the public issue as opposed to my entitlement to my Personal Information.

I rely on the communications previously but should you need copies, I can provide them anytime tomorrow or you can seek the same from Ms. Simpson. Thank you.

I look forward to hearing from you by no later than the end of the business day. I trust that I will not need to make a complaint solely at this time about an improper time extension which would carry over in any event of the disclosures made to me even if they were perfectly compliant with the *Privacy Act* and its binding jurisprudence. As the adage goes, “justice delayed is justice denied” and so too is, “access delayed, access to justice denied” along with “reportage delayed and reportage denied”.

Sincerely,

Tab O

Mr. Kevin A. McLean (BA, JD, CIM)

Enclosures

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Apr 9, 2026 at 10:12 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DATE: April 10, 2026

DELIVERY METHOD: Via Electronic Transmission

TO: Melissa S.

Access to Information and Privacy Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

CC: Commissioner Mike Duheme, Royal Canadian Mounted Police

CC: Stéphane Brisson, Director General, Access to Information and Privacy Branch (stephanie.brisson@rcmp-grc.gc.ca)

REFERENCE: Privacy Act request P-2025-16999 / F339

SUBJECT: Formal Notice of Invalid Time Extension, Demand for Immediate Requirement, and the Impending Escalation Regarding Statutory Non-Compliance

Dear Ms. Simpson, Director General Brisson, and the RCMP Access to Information and Privacy Branch:

I rely on the communications previously but should you need copies, I can provide them anytime tomorrow or you

can seek the same from Ms. Simpson. Thank you.

I write to you today regarding the purported "extension of time" recently invoked by your office in relation to my quasi-constitutional access rights under the *Privacy Act* (Canada). In strict accordance with the Office of the Privacy Commissioner of Canada's (OPC) published guidance on *Tips for raising your privacy concern with a federal government institution*, I am attempting to resolve this matter directly with the ATIP Coordinator by being crystal clear, thorough, and setting firm, reasonable timelines before formally engaging the Commissioner.

Director General Brisson, your direct inclusion in this correspondence is intentional, strategic, and highly consequential. As the executive head of the Access to Information and Privacy Branch, the ultimate statutory liability for the RCMP's compliance with the *Privacy Act* rests squarely upon your desk. I am escalating this matter directly to your level because you possess the absolute executive authority to immediately intervene, direct your internal colleagues, and definitively order the provision of my requested personal information. The deliberate inclusion of your office ensures that this highly sensitive file can no longer languish in the procedural bottlenecks, mathematical errors, or stalling tactics of lower-level analysts.

You have the direct administrative power to instruct Ms. Simpson and her counterparts to immediately execute the CPIC Offline Search and release the requested data, thereby curing this glaring statutory defect before it triggers severe institutional penalties. I fully expect you to exercise that authority upon review of this correspondence. The Access to Information and Privacy regime was designed to bridge the vast power imbalance between the individual citizen and the state apparatus. It was never intended to be wielded as an adversarial shield to protect the institution from the disclosure of its own internal systemic failures.

I am putting the institution on formal notice that the extension is fundamentally invalid, procedurally defective,

and serves only as further circumstantial evidence of the very systemic irregularities my request seeks to expose. The arbitrary delay of a citizen's personal information, particularly when it pertains to matters of physical liberty, is not a mere clerical oversight—it is a substantive breach of administrative fairness.

Furthermore, I am acutely aware that ATIP departments, and specifically their Directors General, are heavily penalized in their annual reporting to Parliament for having files fall into "deemed refusal." By proving that your receipt date calculation is demonstrably false via Canada Post tracking, and by establishing that your extension is legally hollow under the stringent *Gregory* framework, this notice effectively strips away your administrative cover. An invalid extension means the original 30-day statutory deadline remains in effect. Consequently, the RCMP is currently teetering on the edge of an indefensible deemed refusal—a failure metric that is heavily tracked, publicly reported to Parliament by the OPC, and reflects exceedingly poorly on institutional competence and executive leadership. A deemed refusal is not simply a missed deadline; it is a statutory failure that flags the institution for elevated parliamentary oversight.

Access to one's personal information—particularly when that information pertains directly to the deprivation of liberty via the execution of an arrest warrant—is not a trivial administrative privilege; it is a quasi-constitutional right repeatedly enshrined and vigorously defended by the Supreme Court of Canada. The *Privacy Act* serves as a critical mechanism of transparency and accountability, ensuring that the state cannot compile, alter, or act upon clandestine dossiers without the affected individual's knowledge. When an institution leverages procedural mechanisms to delay the release of highly specific, localized forensic data, it directly prejudices the requester's ability to vindicate their Charter rights, specifically under Sections 7, 8, and 9. Administrative delays in these precise circumstances create a cascading effect of prejudice, effectively paralyzing my ability to correct the record of my own unlawful detention and to

hold the originating actors accountable before statutory limitation periods expire.

1. The Mathematical and Procedural Invalidity of the Time Extension

To begin with the most basic of administrative facts, your office has formally recorded the receipt date of my request as March 12, 2026. This is demonstrably false, and the reliance upon this fabricated date renders your subsequent timeline mathematically moot and legally void. I have attached the official Canada Post tracking documentation (Tracking No. 0105952990142328), which categorically proves that the physical package was delivered to, and officially accepted at, your Ottawa facility on **March 11, 2026, at 10:33 a.m. EST.**

Because the statutory clock under Section 14 of the *Privacy Act* is triggered by the actual date of receipt, any extension invoked by your institution based on the incorrect March 12 date is inherently flawed, legally inoperative, and void *ab initio*. You cannot claim an extension under Section 15 of the *Act* when your fundamental record-keeping regarding the commencement of the statutory timeframe is completely inaccurate. The strict interpretation of the 30-day mandate does not afford government institutions the luxury of manipulating the calendar to suit their internal mail-routing delays or administrative convenience, nor does it allow them to artificially lengthen their response windows by simply ignoring validated courier delivery timestamps.

In addition to the above, because your notice of extension failed to explicitly specify a valid period of time and was based on an incorrect receipt date, on the RCMP's absolute "best day," it would have to be calculated as 30 days from the date of your correspondence (March 17, 2026). Even granting this erroneous premise and bending the statutory interpretation entirely in the institution's favor, the absolute latest deadline would be April 16, 2026.

However, as established by the strict requirements of the *Gregory* test, there were no legal or operational grounds for a time extension to begin with. The Federal Court in

Gregory explicitly held that Section 15(a)(i) sets out a stringent two-pronged framework, and the "unreasonable interference" branch is an exceptionally high bar that institutions rarely clear. Institutions cannot rely on this provision simply because they are busy, because a request requires effort, or to accommodate ordinary workload fluctuations, systemic backlogs, and staffing shortages. The default state of any federal institution is "busy"; allowing routine operations to justify extensions renders the 30-day statutory limit entirely meaningless and subverts the legislative intent of the *Privacy Act*.

Under the Act, the Head of the Government Institution—RCMP Commissioner Mike Duheme—would ultimately be faulted for this failure. The institution is legally required to provide specific particulars as to exactly what aspects of this targeted request would "UNREASONABLY interfere" with the operations of the government institution. Given that your notice already implicitly admitted that no extensive external consultations were necessary to comply with the request (by grounding the delay solely in operational burden), you are legally required to provide particulars regarding the alleged interference. Blank administrative assertions, boilerplate template responses, and vague references to "workload" are legally insufficient to trigger a Section 15 extension. A failure to provide these particulars not only renders the extension invalid but also demonstrates a profound disregard for the procedural rights of the requester and the statutory obligations imposed upon the institution.

Without demonstrating with specific, empirical evidence that my highly targeted, clearly delineated request imposes an *extraordinary burden* on your operational capacity, your reliance on this provision is a blatant abuse of process. In light of the enormous failings in both the legal justification and the rudimentary mathematical calculation of that extension, there are absolutely no valid grounds for delay, period. I am strategically sending this correspondence at this hour to ensure that the administrative record is permanently crystallized. The time

to "clean up" or retroactively amend your notice of extension to cover these fatal procedural defects has definitively passed.

2. The Inherent Contradiction of the Extension and the Admission of Complexity

By invoking an extension based on the premise that meeting the original time limit would "unreasonably interfere" with operations, the RCMP has effectively made a crucial and deeply damaging admission. You have inadvertently conceded that retrieving what should be highly standardized, easily accessible CPIC data requires high-level technical expertise and extraordinary operational intervention.

The Canadian Police Information Centre (CPIC) database is structurally engineered for high-availability, instantaneous, real-time retrieval by frontline officers, border services, and judicial officials across the country. It is a system built entirely on the premise of rapid, infallible data extraction. If this were a routine, legitimate warrant—entered lawfully, authorized by a competent court of proper jurisdiction, and existing without subsequent manipulation—pulling the offline database logs would take a trained CPIC analyst mere milliseconds. The architecture of the Offline Historical Database is specifically designed to be audited precisely for circumstances such as this. It is a system built for transparency and accountability, not for obfuscation and delay.

The fact that the RCMP requires a statutory extension to produce four basic fields of personal information strongly implies that the systemic non-repudiation artifacts have indeed been fraudulently metamorphosed. If the CPIC database had not been blatantly and fraudulently amended to alter the court level (e.g., executing an unprecedented geographic and jurisdictional swap between the Toronto Superior Court of Justice and the Brampton Ontario Court of Justice), geography, and the issuing judicial officer, there would be zero operational necessity to seek a 30-day delay.

The delay itself is the forensic footprint of the forgery. When an institution requires a full month to locate basic metadata that should be instantly available via a simple query of my personal identifiers, it speaks volumes about the condition of those records. Administrative friction is, in this instance, a glaring proxy for institutional obfuscation. It suggests that time is required not to *retrieve* the data, but to formulate a strategy on how to handle the explosive anomalies contained within it, or worse, to find a way to sever the hexadecimal data to hide the tampering. A raw hexadecimal dump bypasses user-interface masking; it shows the binary reality of the database entry. Producing it is not operationally burdensome; it is simply politically inconvenient. The refusal to produce this raw data immediately is an active decision to prioritize institutional protection over public accountability.

3. Targeted Escalation to the OPCC and Institutional Context

I am acutely aware of the tendency for federal institutions to rely heavily on the "deemed refusal" mechanism, comfortable in the cynical knowledge that complaints to the Office of the Privacy Commissioner of Canada (OPCC) often languish in administrative doldrums for years. Let me disabuse you of any notion that I will simply file a broad, generalized complaint to gather dust in a queue while my Charter rights continue to be actively prejudiced.

It is not my primary interest to file a formal complaint simply to force more oversight onto the RCMP. However, Director General Brisson, your branch is already operating under intense, unprecedented scrutiny from the OPC. As highlighted in the OPC's 2024-2025 Report to Parliament, the RCMP generated the highest volume of federal privacy complaints (274 complaints, or 21% of the federal total). Your branch is already the single largest violator of privacy timelines in the federal public service.

Your institution's recent track record before the Commissioner is defined by systemic failures to protect personal information, verify the legality of its data practices, or maintain basic data integrity. This includes

the damning Special Report on *Project Wide Awake* regarding unauthorized open-source intelligence gathering, the OPC findings regarding your negligent loss of unencrypted USB storage devices, the opaque utilization of Mobile Device Forensic Tools (MDFT) without proper Privacy Impact Assessments, and the highly critical investigation into the RCMP's use of Clearview AI, where the OPC explicitly found that the RCMP "failed to take any active steps to verify the legality of the collection of the information of Canadians." These repeated, high-profile failures demonstrate a pattern of disregard for the *Privacy Act* and the fundamental rights of Canadians.

If the RCMP so fundamentally failed to verify the legality of its biometric collections, and if it cannot secure an unencrypted physical USB drive, it strains credulity to believe it has properly verified the legality of the manipulated CPIC warrant data in my file. Should you fail to rectify this immediate breach of the Act, my complaint to the OPCC will be exceptionally narrow and laser-focused *solely* on the improper extension of time, the failure to perform basic mathematical calculations regarding receipt dates, and the procedural invalidity of your notice. I will invite the Commissioner to place an extra, high-powered microscope exclusively on the RCMP ATIP branch's administrative competence, adding the suppression of CPIC forgery logs to your institution's rapidly expanding, heavily criticized OPC dossier. I pose the question directly to you: Do we really need more eyes, a formal investigation from the Privacy Commissioner, and the associated public institutional embarrassment on this specific, easily avoidable procedural failure?

4. The Chief Justice Morawetz Correlation

Given the meticulously documented irregularities in this file, I do not view the timing of your correspondence as a coincidence. I find the exact timing of your initial email on March 17, 2026, to be profoundly interesting, and highly indicative of external considerations driving this ATIP process. That date marks exactly two months prior to the first day that Chief Justice Morawetz will be out of office.

Given the wealth of evidence I have already compiled regarding the conflict of interest, the bizarre misdirection between the Toronto Region Superior Court of Justice (SCJ) and the Brampton Ontario Court of Justice (OCJ), and the purposeful obscuring of the authorizing judge's identity, it is increasingly apparent that the RCMP is aware of the true identity of the issuing judicial officer. The separation of powers and the constitutional firewall between different levels of the judiciary are not mere suggestions; they are the bedrock of the Canadian justice system. Swapping a Superior Court marker for an Ontario Court marker within a federal database to mask a judicial conflict of interest is a catastrophic breach of that bedrock. It is an action that strikes at the very heart of judicial independence and the integrity of the administration of justice.

The stalling tactics currently being deployed appear designed not for administrative convenience, nor for necessary inter-agency consultation, but specifically to shield this fact until the judicial officer in question has safely retired and is beyond the reach of certain immediate disciplinary mechanisms or media scrutiny. This calculated delay is not merely an administrative failure; it is an active complicity in the suppression of crucial evidence.

I assure you, the database metadata does not retire. The offline transaction logs, the hexadecimal dumps, and the originating agency identifiers remain immutable. They cannot be aged out of existence, nor can they be politely ignored. Delaying the inevitable disclosure only compounds the institutional liability of the RCMP and implicates the federal repository as an active accessory in the provincial manipulation of judicial records. Aiding in the concealment of a forged judicial authorization by hiding behind the *Privacy Act* timeline provisions is a deeply dangerous and legally perilous posture for the national police force to maintain.

5. Public Interest Disclosure vs. Personal Release

We are rapidly approaching a critical juncture regarding Section 8(2)(m) of the *Privacy Act*, which allows for the

disclosure of personal information where the public interest in disclosure clearly outweighs any invasion of privacy. The manipulation of a federal database to effectuate a fraudulent arrest warrant—and the subsequent inter-jurisdictional cover-up of the issuing authority—is not merely a personal grievance; it is a profound matter of urgent, pressing public interest.

The integrity of the CPIC system is the absolute bedrock of Canadian law enforcement. Every police officer, border guard, and crown attorney relies on the unassailable truth of CPIC data. If local police forces, vindictive third parties, or compromised judicial officers can fraudulently amend warrants within the federal system without leaving an accessible, transparent audit trail, the liberty of every single Canadian citizen is at risk. It compromises every background check, border crossing, and roadside stop in the country. The public has an absolute right to know if the national policing database is vulnerable to retroactive manipulation by local actors attempting to cover up malicious prosecutions. The potential for systemic abuse is vast, and the implications for public trust are devastating.

I am once again reminding the RCMP that a critical choice must be made: we can either address this through a highly publicized, targeted public interest disclosure to the public at large concerning the systemic vulnerabilities and unauthorized, untracked manipulation of the CPIC system under s. 8(2)(m), or we can resolve it quietly, efficiently, and lawfully via a localized release of my personal information directly to me.

6. II. General Interpretations by the Courts

To preempt any administrative attempt to sever or withhold the requested CPIC transaction logs, hexadecimal dumps, or judicial metadata on the spurious grounds that they do not constitute my "personal information," I direct you to the binding jurisprudence governing this institution. The Federal Court and Supreme Court of Canada have left no room for bureaucratic evasion on this matter.

Drawing from jurisprudence in the federal public sector, the definition of personal information must be given a broad, highly expansive interpretation (*Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R., dissenting, 403 at para 68; *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66, 2003 SCC 8, at para 23). The Supreme Court has actively pushed back against narrow administrative readings of what constitutes personal data, recognizing the profound power dynamics at play and the inherent need for transparency.

Personal information is information “about” an identifiable individual. “About” means that the information is not just the subject of something but also relates to or concerns the subject (*Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157). The manipulated CPIC metadata, the ORI routing codes, and the hexadecimal dumps surrounding the warrant for my arrest intrinsically relate to me and the direct, physical deprivation of my liberty. It is impossible to separate the technical metadata from the profound personal impact of the warrant itself.

Information will be about an “identifiable individual” where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information (*Gordon v. Canada (Health)*, 2008 FC 258). The system IDs and audit logs associated with a warrant bearing my name easily meet the “serious possibility” threshold. Information need not be explicitly recorded for it to constitute personal information. It is sufficient that the information be about an identifiable individual even if the information is not in a traditionally recorded form, such as oral conversations, biological samples and real time video surveillance. While the absence of a recording may go to the issue of collection, it does not change the fact that the information is inherently personal information (*Morgan v. Alta Flights Inc.* (2006) FCA 121, affirming (2005) FC 421).

The same information can be personal to more than one individual, where, for example, it contains the views of one individual about another individual, or where the same information reveals something about two identifiable individuals (*Wyndowe v. Rousseau*, 2008 FCA 39).

Therefore, the identity of the judicial officer who signed the warrant, and the Originating Agency Identifier (ORI) of the police force that entered it, are unequivocally intertwined with my personal information and cannot be severed under any reasonable interpretation of the Act.

Information will still be personal information even if it is publicly available within the meaning of the regulations, and is exempt from applicable consent requirements (*Englander v. TELUS Communications Inc.*, 2004 FCA 387).

Finally, subjective information about an individual may still be personal information even if it is not necessarily true or accurate. In this case, the fraudulently altered judicial records, while legally and factually false, still constitute my personal information under the Act because they were maliciously generated and permanently attached to my identity within the CPIC database. The falsity of the information is precisely why access is required—to correct the record and vindicate my rights.

7. Demand for Immediate Requirement, Access Partnership, & Executive Directive

This is the exact type of access request that unequivocally requires the provision of the requested personal information today. While noting that retrieving extensive personal information can be operationally demanding in some complex, multi-jurisdictional cases, any information regarding an arrest warrant executed against me—and every single data field, hexadecimal dump, or audit log therein—is unequivocally my personal information as defined by the Federal Court of Appeal and the Supreme Court of Canada. The failure to provide this information is a continuing violation of my quasi-constitutional rights.

In the spirit of the "access partnership" heavily encouraged by Canadian courts, which mandates that institutions and requesters work collaboratively to facilitate access, my primary focus is on working together, advancing the public interest, and ensuring this serves as a profound learning experience for all involved so the public ultimately benefits from greater transparency. I am providing you with a clear, immediate lifeline and a collaborative off-ramp from this procedural quagmire. The goal here is not conflict, but clarity, the restoration of systemic integrity, and the mutual benefit of a functional, accountable ATIP system. This "access partnership" is not a one-way street; it requires active cooperation and a genuine commitment to the principles of transparency.

I kindly refer to the above points regarding the absolute necessity of the Offline Search. To reiterate, the RCMP's extension was invoked entirely without reasonable grounds or required particulars regarding any actual interference with RCMP operations. However, even applying the RCMP's flawed calculations on their absolute "best day," the statutory limit still expires tomorrow.

Director General Brisson, I am directly calling upon your executive mandate to resolve this matter today. By actively stepping in and ordering your internal colleagues to fulfill this immediate requirement, you provide the ATIP analyst with a highly incentivized, easy way out of an untenable position. **Most importantly, you help the RCMP completely avoid two distinct and severe OPC complaints—one for an illegal extension, and one for an indefensible deemed refusal—when, in reality, it would not take a trained CPIC analyst more than two hours to simply run the query, pull the offline hex dump, package the data, and provide it.** Two hours of standard operational effort can prevent years of institutional headaches, media scrutiny, and federal court litigation. You possess the unilateral ability to bypass the administrative paralysis, mandate the quick extraction of the four basic fields below via the Offline Search, pacify a

highly litigious file, and restore the collaborative access partnership that the Privacy Act demands. Your failure to act will be viewed not as an administrative oversight, but as a deliberate executive decision to withhold critical information.

I demand that the RCMP—under the direct instruction of the Director General—fulfill this immediate requirement consisting *only* of the four discrete personal-information elements I have previously identified:

1. **Originating Agency Identifier (ORI)** - Confirming the exact municipal or provincial police force that inputted the warrant into the federal system.
2. **Issuing Authority / Court Field** - Confirming the exact court level (SCJ vs. OCJ) and the specific name of the authorizing judicial officer.
3. **Narrative / Remarks Field** - Completely unredacted, showing the exact parameters, limitations, and specific text of the authorization.
4. **System Identification Number** - The unique, immutable identifier for the mainframe transaction.

Providing these four highly specific, binary data points requires no complex consultation, no severability analysis, no translation, and definitively no unreasonable interference with your operations. They are raw, factual data points belonging exclusively to my file.

Because the deemed date of receipt is definitively proven to be March 11, 2026, the original 30-day statutory limit expires tomorrow. If the records are not produced, your invalid extension falls away entirely, and the file immediately enters a state of deemed refusal. Trusting that all is in order for the immediate provision of my personal information under the direct, collaborative oversight of the Director General, please provide the requested data by return email to cure this defect.

I look forward to receiving these specific records and confirming receipt by no later than 4:59 p.m. tomorrow.

Whether the RCMP needs a few days extra to determine whether there should also be a disclosure, as suggested,

above to the public in light of the unprecedented facts herein, is one that is more of a public interest type disclosure to the public issue as opposed to my entitlement to my Personal Information.

I rely on the communications previously but should you need copies, I can provide them anytime tomorrow or you can seek the same from Ms. Simpson. Thank you.

Govern yourselves accordingly.

Sincerely,

Mr. Kevin A. McLean (BA, JD, CIM)

Appendix: Extension of time limits

15 The head of a government institution may extend the time limit set out in section 14 in respect of a request for

(a) a maximum of thirty days if

(i) meeting the original time limit would unreasonably interfere with the operations of the government institution, or

(ii) consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit, or

(b) such period of time as is reasonable, if additional time is necessary for translation purposes or for the purposes of converting the personal information into an alternative format,

by giving notice of the extension and the length of the extension to the individual who made the request within thirty days after the request is received, which notice shall contain a statement that the individual has a right to make a complaint to the Privacy Commissioner about the extension.

R.S., 1985, c. P-21, s. 151992, c. 21, s. 35

Warm regards,

Tab P

Mr. Kevin A. McLean (BA, JD, CIM)
Chartered Investment Manager

On Tue, Apr 7, 2026 at 7:11 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear RCMP (Privacy Division) (particular attention: Ms. Simpson):

To ensure I have articulated my request as clearly as possible, please consider the proof-of-concept below. If you provide the memory offsets and hexadecimal values, I am fully capable of decoding the text, which I expect will closely match the following output (and will likely include my date of birth, March 25, 1983). As such, this will save operational resources and I can then confirm my decoded text while or before you provide it to me. In this regard, I hope I have done my small part in being respectful of the public purse and your operations along with providing a middle ground – interim or permanent so that decoding is not required per se.

My best to you over the next couple of days.

Thank you.

Mr. Kevin A. McLean (BA, JD, CIM)

Block A: Initial Systemic Entry (Authorized Parameters) – September 23, 2024

Offset (Memory Address)	Hexadecimal Values (Binary Representation)	Decoded Text (ASCII / EBCDIC)
00000000	54 52 41 4E 53 3A 41 44 44 20 44 41 54 45 3A 32	TRANS:ADD DATE:2
00000010	30 32 34 30 39 32 33 20 54 49 4D 45 3A 31 33 31	0240923 TIME:131
00000020	30 30 31 20 55 53 45 52 3A 54 50 53 35 32 44 49	001 USER:TPS52DI
00000030	56 20 54 45 52 4D 3A 54 52 30 30 34 31 00 00 00	V TERM:TR0041...
00000040	4F 52 49 3A 4F 4E 33 30 32 34 37 30 30 30 20 20	ORI:ON30247000
00000050	4E 41 4D 45 3A 4D 43 4C 45 41 4E 2C 4B 45 56 49	NAME:MCLEAN,KEVIN
00000060	4A 55 44 47 45 3A 47 42 4D 20 28 43 49 29 20 20	JUDGE:GBM (CJ)

00000070	52 45 47 3A 54 4F 52 4F 4E 54 4F 20 20 20 20 20	REG:TORONTO
00000080	43 52 54 3A 53 43 4A 20 20 20 20 20 20 20 20 20	CRT:SCJ

Block B: Systemic Clearance / Execution (Arrest Event) – October 2, 2024

Offset (Memory Address)	Hexadecimal Values (Binary Representation)	Decoded Text (ASCII / EBCDIC)
000000A0	54 52 41 4E 53 3A 43 4C 52 20 44 41 54 45 3A 32	TRANS:CLR DATE:2
000000B0	30 32 34 31 30 30 32 20 54 49 4D 45 3A 30 38 34	0241002 TIME:084
000000C0	35 30 31 20 53 54 41 54 3A 45 58 45 43 55 54 45	501 STAT:EXECUTE

Block C: Post-Execution Algorithmic Amendment (Interrogated Parameters) – November 11-12, 2024

Offset (Memory Address)	Hexadecimal Values (Binary Representation)	Decoded Text (ASCII / EBCDIC)
00000100	54 52 41 4E 53 3A 4D 4F 44 20 44 41 54 45 3A 32	TRANS:MOD DATE:2
00000110	30 32 34 31 31 31 31 20 54 49 4D 45 3A 30 39 31	0241111 TIME:091
00000120	35 30 31 20 55 53 45 52 3A 54 50 53 35 32 44 49	501 USER:TPS52DI
00000130	4F 4C 44 5F 52 45 47 3A 54 4F 52 4F 4E 54 4F 20	OLD_REG:TORONTO
00000140	4F 4C 44 5F 43 52 54 3A 53 43 4A 20 20 20 20 20	OLD_CRT:SCJ
00000150	4E 45 57 5F 52 45 47 3A 43 45 4E 54 20 57 45 53	NEW_REG:CENT WEST

Tab Q

00000160	4E 45 57 5F 43 52 54 3A 4F 43 4A 20 28 42 52 41	NEW_CRT:OCJ (BRA)

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)
Chartered Investment Manager
Email: mcleansettlement@gmail.com
Fax: 416.981.7117
Phone number: 647.370.9354

On Tue, Apr 7, 2026 at 6:42 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DATE: April 7, 2026
DELIVERY METHOD: Via Electronic Transmission
TO: Ms. Melissa Simpson Access to Information and Privacy Branch
Royal Canadian Mounted Police 73 Leikin Drive, Mail Stop #61 Ottawa,
Ontario K1A 0R2 Email: ATIP-AIPRP@rcmp-grc.gc.ca
FROM: Mr. Kevin A. McLean (B.A., J.D., CIM)
REFERENCE: *Privacy Act*, RSC 1985, c P-21, Request P-2025-16999 / F339
SUBJECT: Confirmation of Facsimile Transmission: File P-2025-16999 / F339 — Public Interest Legal Position & Formal Demand for Interim Statutory Release (Statutory Limitation Date: April 9, 2026)

Dear Ms. Simpson,

1. In strict adherence to comprehensive legal drafting protocols, it is hereby confirmed that the following documentation has been rigorously reviewed and synthesized in the preparation of this correspondence: the preliminary electronic correspondence transmitted on April 7, 2026; the facsimile transmission directed to the Commissioner of the Royal Canadian Mounted Police on April 7, 2026; the analytical treatise entitled "Accessing Warrant Information Via Privacy Request"; and the constituent components of the privacy requisition designated as File P-2025-16999 / F339.
2. Further to preceding communications, formal confirmation is hereby effectuated that the legal memorandum enumerating the public interest position (**the Public Interest Legal Position**), accompanied by its corollary appendices and the concurrent statutory access requisition promulgated pursuant to the *Access to Information Act*,

RSC 1985, c A-1 (**the ATIA Requisition**), has been successfully transmitted via facsimile to the Office of the Commissioner of the Royal Canadian Mounted Police and the Ontario Headquarters.

3. Furthermore, physical instantiations of the aforementioned documentation are presently in transit via registered post, directed specifically to the attention of the Commissioner. The utilization of manifold secure transmission channels is effectuated to guarantee the absolute inviolability of the institutional record and to precipitate the immediate forensic evaluation necessitated by the documentary metamorphosis (**the Documentary Metamorphosis**) delineated in prior submissions. Pursuant to the doctrine of absolute nullity, it is emphatically submitted that such post-execution structural alteration of a judicial instrument constitutes not a mere administrative irregularity, but rather an absolute nullity *ab initio*, representing a direct and egregious contravention of strict statutory imperatives and foundational equitable principles.
4. The concurrent invocation of the *Privacy Act* and the *Access to Information Act* is strategically orchestrated to compel a comprehensive, bilateral forensic audit of both the personal data currently impinging upon the legal status of the requestor and the foundational hexadecimal metadata (**the Hexadecimal Metadata**) entrenched within the federal police network database (**the CPIC Database**). It is an immutable jurisprudential postulate that such systemic transparency remains an indispensable prerequisite for the preservation of the underlying trust architecture (**the Trust Architecture**) inherent to the system. The failure to rigorously maintain the integrity of said architecture necessarily renders the data contained therein *prima facie* suspect.
5. Appreciation is formally extended for the administrative prioritization matrices and operational exigencies previously referenced by the institution. Nevertheless, the unprecedented nature of this requisition—necessitating an immediate examination of the documented manipulation of *Criminal Code*, RSC 1985, c C-46, Form 2 informations and their associated administrative packages—demands strict, unyielding statutory adherence. Any deviation from the explicitly prescribed legal authorizations governing such instruments unequivocally renders the resultant *acta* a complete nullity and an *ultra vires* exercise of executive authority, wholly devoid of lawful jurisdiction.
6. Building upon preceding institutional indications that an interim disclosure of records could be effectuated antecedent to the culmination of the specialized algorithmic historical query (**the Offline Search**), a formal demand is hereby advanced for the immediate, interim statutory release of the four discrete data classifications previously enumerated. The administrative necessity of this interim disclosure is predicated upon the intricately constructed rationales articulated hereinbelow.

I. The Jurisprudential and Technical Distinction Between Algorithmic Extraction and Administrative Retrieval

7. It is formally acknowledged that a comprehensive query of historical data constitutes a specialized interrogation of historical database architectures, obligating the institutional access and privacy division (**the ATIP Branch**) to formally requisition technical specialists for the

extraction of complex system logs. Conversely, the retrieval of the four specific, foundational data classifications—specifically, the **Originating Agency Identifier (ORI), Issuing Authority / Court Field, Remarks / Narrative Field, and System Identification Number**—necessitates no such profound technical excavation.

8. Insofar as an extraction localized exclusively to these fundamental parameters is strictly confined to personal information and the purported legal authority deployed against the subject individual, the necessity for extensive, line-by-line redaction of protected systems architecture or third-party data is *ipso facto* eviscerated. Consequently, the institution is legally precluded from reasonably asserting that the extraction of these four elemental fields would precipitate an unreasonable interference with institutional operations pursuant to paragraph 15(a)(i) of the *Privacy Act* or the *Federal Courts Rules*, SOR/98-106. The evidentiary burden rests exclusively upon the institution to manifest this foundational metadata immediately, *in limine*, and without prevarication.

II. The Inexorable Imposition of the Statutory Duty to Assist

9. Federal privacy and access policy instruments explicitly promulgate a mandatory statutory obligation to provide assistance (**the Duty to Assist**) to individuals submitting formal requests. The immediate provision of these four eminently retrievable data points effectuates rigorous statutory compliance with the aforementioned obligation, thereby ensuring that the requestor is not subjected to arbitrary, unjustified administrative protraction whilst the more intricate systems logs are subjected to subsequent processing and redaction protocols. This requirement finds robust jurisprudential validation in the administrative law doctrine of legitimate expectations, as definitively elucidated by the Supreme Court of Canada in *Baker v Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817 at para 22 (*Baker*), wherein the procedural parameters of fairness strictly mandate absolute adherence to established statutory obligations without undue delay.

III. Interim Disclosures as an Established and Binding Administrative Modality

10. The phased disclosure of information constitutes an established, legally recognized administrative modality within the federal apparatus. Federal institutions customarily deploy phased institutional informational disclosures (**the Interim Release Packages**) specifically to satisfy statutory obligations when the entirety of a requisition is characterized by excessive volume, technical complexity, or concurrent litigation. It is respectfully submitted that the receipt of the access request constituents on a piecemeal trajectory is entirely acceptable, commencing with the extant foundational metadata, to be subsequently followed by the discrete provision of the technical systems data derived from the respective queries.
11. To the extent that a compliant response and the attendant provision of these personal information records satisfy the core evidentiary prerequisites of the concurrent access requisition, the appropriate institutional representative shall be duly notified of the truncated nature of that secondary file, thereby proactively conserving

administrative resources and efficiently returning the matter, operationally speaking, to the *status quo ante*.

12. Gratitude is formally expressed for the continued professionalism and meticulous adherence to statutory frameworks demonstrated thus far. Anticipation is held for the receipt of the requested interim data prior to the strict April 9, 2026, statutory limitation period.

IV. The Architecture and Accessibility Protocols for Foundational Metadata

13. In delineating the parameters of foundational metadata, a strict jurisprudential and technical bifurcation is necessitated, predicated upon the structural architecture and retrieval mechanisms inherent to the CPIC database (**the CPIC Data Architecture**). It is an established operational reality that the CPIC apparatus is engineered to preserve an immutable, permanent archival continuum of its national network. Consequently, whilst a judicial warrant may be ostensibly excised from the active operational interface subsequent to execution or expungement, the underlying digital artifact is decidedly not eradicated from the federal infrastructural matrix.
14. The discrete informational constituents previously identified—specifically, the Originating Agency Identifier, the jurisdictional court level, the physical courthouse designation, and the terminal identification module—constitute the requisite foundational metadata. Although such data points remain inaccessible via standard, routine criminal record interrogations, their retrieval is definitively effectuated through specialized, entrenched systemic protocols.
15. It must be unequivocally asserted that the population of free-form data fields—specifically encompassing the narrative or remarks field explicitly designating the absolute identity of the authorizing judicial officer—is decidedly not a discretionary or optional administrative appendage. Rather, it constitutes an immutable, mandatory operational requisite. Any anticipatory institutional posture characterizing such fields as merely "optional" to rationalize their obfuscation or systemic omission is hereby peremptorily rebutted. The precise identity of the judicial officer constitutes a critical evidentiary nexus, carrying profound, quantifiable ramifications—valued potentially in the millions of dollars—within the strictures of concurrent civil litigation. Complete disclosure is strictly mandated.
16. **Systemic Audit Trails:** The institution maintains immutable audit trails within the designated personal information bank, specifically identified as RCMP PPU 005 (**the Audit Trails**). These digital ledgers preserve the absolute evidentiary locus of truth, capturing the precise identity of the system operator and the specific terminal deployed during the data entry continuum.
17. **Standard Interface versus Forensic Interrogation:** Whereas frontline law enforcement personnel interact exclusively with a graphical user interface that may omit expunged or executed warrants, the federal governance authority retains the unilateral capacity to execute an algorithmic historical query within the Investigative Data Bank to extract cleared, canceled, or purged historical records.

V. The Jurisprudential Complexity Inherent to Amended Informational Vectors

18. It is explicitly acknowledged that modified informational vectors—specifically, post-entry algorithmic amendments—necessitate a profoundly elevated echelon of forensic interrogation.

19. *The Modification Imperative*: In the event that a law enforcement operative executes an amendment to a systemic record, irrespective of the legality or validity of said alteration, the database architecture automatically generates explicit procedural identifiers, encompassing the *ADD*, *MODIFY*, *CLEAR*, and *CANCEL* algorithms.
20. *Hexadecimal Mainframe Extraction*: Standard graphical user interface manifestations are inherently subjected to algorithmic filtering, thereby rendering solely the contemporaneous state of a given record. To definitively ascertain the substantive composition of the data antecedent to its amendment, the institution is strictly compelled to extract hexadecimal mainframe dumps (**the Hexadecimal Dumps**). These immutable binary ledgers furnish the mathematical certitude required to circumvent human interpretation or potential institutional obfuscation.
21. Furthermore, it is formally entered into the administrative record that advanced forensic technical proficiencies are possessed by the requestor. This acumen was fortuitously cultivated through the meticulous dissection and analysis of a concealed Random Access Memory (RAM) dump of a central processing unit, executed by a former regulatory body. Said analysis subsequently formed the evidentiary crucible of a formal complaint and investigation under the purview of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (*PIPEDA*).
22. Consequently, a formal requisition is hereby advanced for the unadulterated, raw hexadecimal code. The institutional disclosure must explicitly encompass the precise cryptographic offsets, the raw hexadecimal values, and the synchronously decoded, plain-text linguistic translations (ASCII/EBCDIC). The requestor retains the requisite specialized acumen to deconstruct said machine language independently. To provide absolute clarity regarding the requisite format of this disclosure, the following conceptual schema is submitted for the administrative record:

Table 1: Conceptual Schema of Raw Hexadecimal Mainframe Extraction

Offset (Memory Address)	Hexadecimal Values (Binary Representation)	Decoded Text (ASCII / EBCDIC)
00000000	54 52 41 4E 53 3A 4D 4F 44 20 44 41 54 45 3A 32	TRANS:MOD DATE:2
00000010	30 32 34 30 39 31 35 20 54 49 4D 45 3A 31 34 33	0240915 TIME:143
00000020	32 30 31 20 55 53 45 52 3A 52 43 4D 50 39 39 32	201 USER:RCMP992
00000030	34 20 54 45 52 4D 3A 54 52 30 30 34 31 00 00 00	4 TERM:TR0041...

00000040	4F 52 49 3A 54 50 53 35 32 44 49 56 30 30 30 20	ORI:TPS52DIV000
00000050	4E 41 4D 45 3A 4D 43 4C 45 41 4E 2C 4B 45 56 49	NAME:MCLEAN,KEVI
00000060	4A 55 44 47 45 3A 47 42 4D 20 28 43 4A 29 20 20	JUDGE:GBM (CJ)
00000070	4C 4F 43 3A 33 36 31 20 55 4E 49 56 20 54 4F 52	LOC:361 UNIV TOR
00000080	4F 4C 44 5F 43 52 54 3A 4F 43 4A 20 20 20 20 20	OLD_CRT:OCJ
00000090	4E 45 57 5F 43 52 54 3A 53 43 4A 20 20 20 20 20	NEW_CRT:SCJ

23. To further delineate these evidentiary mechanisms, the following comparative framework is additionally submitted:

Table 2: Comparative Paradigm of Algorithmic Data Retrieval Mechanisms

Data Classification	Primary Evidentiary Locus	Administrative Exertion Paradigm	Forensic Utility and Evidentiary Value
Active Warrant Status	CPIC "Persons" Informational File	Low (Routine Operational Interrogation)	Restricted exclusively to contemporaneous operational deployment.
Foundational Metadata (ORI, Terminal ID)	Systemic Transaction Logs (PPU 005)	Moderate (Necessitates Rigorous Systemic Audit)	Ascertains the precise structural genesis and authorization of the judicial record.
Original Data Prior to Amendment (If Applicable)	Hexadecimal Dumps and Offline Search	High (Demands Specialized Mainframe Interrogation)	Evidentiarily establishes vector collapse, unauthorized alterations, or modifications devoid of synchronous alignment with factual actuality.

24. In synthesis, the underlying data is decidedly not eradicated; rather, it is cryptographically archived within a sub-stratum of the network architecture. This immutable reality strictly obligates the institution to transcend the superficial user interface and interrogate the raw,

unadulterated systems logs to expose the genuine chronological trajectory of any documentary metamorphosis.

VI. Concluding Requisitions and Administrative Prognosis

25. In summation, a formal demand is hereby instituted: should any information, data, or corollary components pertaining to the subject personal information records (**the Personal Information Records**) have been subjected to amendment, alteration, or post-entry modification subsequent to their initial systemic incorporation, formal notification of such procedural metamorphosis must be immediately transmitted. This notification is strictly necessitated to properly bifurcate and jurisprudentially distinguish between the primary informational inputs and those subsequent algorithmic amendments purportedly effectuated on or about September 2024.
26. In the event that extant medical examinations, clinical assessments, and corollary diagnostic testing preclude a return to standard administrative functionality antecedent to Thursday, April 9, 2026, formal confirmation of receipt, subsequent rigorous evidentiary inspection, and corresponding procedural responses shall be effectuated immediately upon the resumption of said capacities.
27. Professional salutations, profound gratitude, and formal well wishes are extended to the institution in the interim, anticipating strict compliance with the aforementioned statutory imperatives subject to any of the personal information records being those were amended data without it showing on its face in the Transaction Logs (PPU 005) as opposed to the Offline Search (i.e. mainframe interrogation) (i.e. noting that such searches between foundational metadata versus amended data (or what was prior to the amended data likely requires different specialists). To the extent that nothing was amended, then piecemeal provision would be unnecessary altogether. Thank you.
28. By way of supplementary administrative notation, formal reference is directed to the institutional file number assigned hereinabove (P-2025-16999 / F339). It is explicitly observed that said numerical designation incorporates the calendar year 2025, notwithstanding the fact that the instant statutory requisition was formally instituted in the calendar year 2026. It is respectfully presumed that this numerical divergence is indicative of an internal institutional archival or filing protocol; however, the discrepancy is formally noted herein to ensure the absolute precision of the administrative record.

Respectfully submitted,

Mr. Kevin A. McLean (B.A., J.D., CIM) Chartered Investment Manager
Email: mcleansettlement@gmail.com

On Tue, Apr 7, 2026 at 3:54 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Date: April 7, 2026 **RCMP ATIP File Number:** P-2025-16999 / F339 **Classification:** Private and Confidential **Sending method:** Via Email

To: Ms. Melissa Simpson, RCMP Access to Information and Privacy (ATIP) Branch

Tab R

Tab S

Subject: Cross-Reference / ATIA Requisition and Formal Public Interest Legal Position

Dear Ms. Simpson,

Please find attached my formal "Public Interest Legal Position." This document is provided within the context of the herein Privacy Act request and serves as a cross-reference for the concurrent Access to Information Act (ATIA) requisition.

Please be advised that a hard copy of this correspondence is also being sent via registered mail to the Head of the Institution, Commissioner Mike Duheme. I kindly request that you provide him with an email copy of this note and the attached documents. I am writing to him to respectfully seek his authorization for a public disclosure release, ensuring that no other person has been, is being, or will be affected by the circumstances detailed herein in the way that I have been.

I intend to formalize this correspondence on official letterhead in due course; however, given the profound urgency of this matter and the fact that I will be largely unavailable over the coming days, I am submitting this electronic version for immediate effect.

Upon deeper reflection, my concerns in this matter extend far beyond my personal circumstances and strike at the core of the broader public interest. This matter underscores the paramount constitutional importance of the RCMP's Canadian Police Information Centre (CPIC) database as the ultimate systemic safeguard when circumstances such as these have occurred, are occurring, or could occur in the future. It must be recalled that it was the formidable machinery of the Toronto Police Service (TPS) that represented to me—while I was placed in handcuffs—that I would be spending the foreseeable future in pre-trial custody on a singular charge that hindsight has proven to be entirely fictitious. For many, such an arbitrary and sudden deprivation of liberty could lead to catastrophic outcomes, including the loss of life through despair and suicide, or the inherent perils of dangerous detention centres. While I am fortunate to possess physical size and strength despite my physically disabled state, being subjected to such a punitive environment under false pretenses would have been tantamount to a death sentence—or, at the very least, a premature end to a productive life.

I do not yet know whether the CPIC database currently retains the factual, unadulterated information or the technologically amended variants. That factual determination, alongside the ultimate scope of any public interest disclosure, rightfully rests within the purview of the Head of the Institution; my proposed advisory is submitted merely as a respectful suggestion.

To be unequivocally clear, I am not passing judgment per se on "Project South" or the recent bevy of criminal charges involving TPS officers. My focus remains strictly on this specific, unprecedented situation of documentary manipulation. However, while I possess the resources and legal acumen necessary to identify and challenge this systemic documentary corruption, experiencing this firsthand forces me to consider the broader societal implications. I can only imagine how insurmountable and terrifying this ordeal would be for an individual without legal experience or for the most marginalized members of our society. A single instance of this jurisdictional subversion is one too many. If exposing these critical vulnerabilities protects even one other individual from similar arbitrary prejudice, I will consider the effort worthwhile, despite the deeply troubling institutional realities it reveals.

Finally, I want to express my sincere appreciation and high praise for the utmost professionalism you and your department have demonstrated to date. Please feel free to pass these commendations along to the Commissioner at your discretion.

Warm regards,

Kevin A. McLean (BA, JD, CIM)

Date: April 7, 2026

RCMP ATIP File Number: P-2025-16999 / F339

Classification: Private and Confidential

Sending method: Via Email

To: Commissioner Mike Duheme, Head of the Institution, Royal Canadian Mounted Police, and Overall Governance Authority for the Canadian Police Information Centre

73 Leikin Drive

Ottawa, Ontario K1A 0R2

Subject I: Statutory Invocation of the Public Interest Override and the Exaction of Information Pertaining to Jurisdictional Nullities

Subject II: Formal Legal Position Regarding State-Actor Malfeasance, Documentary Metamorphosis, and the Imperative for Public Transparency

Dear Commissioner Duheme:

I write regarding the above-captioned matter to provide an exhaustive legal posture and to formally demand the immediate intervention of the Royal Canadian Mounted Police (the "**RCMP**") in its capacity as the supreme custodian of Canada's national law enforcement data architecture. This correspondence serves as a formal notice that the integrity of the Canadian police information centre (the "**Canadian Police Information Centre**") has been compromised by the injection of technologically metamorphosed and jurisdictionally void documentation. The RCMP's compliance in this matter is governed strictly by the *Privacy Act* and, by necessary implication, the *Access to Information Act*, rather than the procedural rules of the lower courts.

I attach the following documents for purposes herein. Specifically, the ensuing legal analysis and formal constitutional posture are inextricably predicated upon a comprehensive, forensic review of the following documentary evidentiary record, which is hereby incorporated by reference in its absolute entirety:

- a. The formal correspondence designated as Privacy Act request P-2025-16999 / F339, including the exhaustive analytical appendices appertaining thereto;
- b. The internal institutional memorandums traversing the parameters of CPIC and the associated personal information bank rcmp ppu 005 (the "**Personal Information Bank RCMP PPU 005**");
- c. The unadulterated public interest disclosure authorities documentation, enumerating the comparative statutory frameworks governing administrative transparency;
- d. The authenticated metadata transaction logs and the chronologically anomalous municipal occurrence reports delineating the trajectory of the physical apprehension.

I. PROPOSED SUBSTANCE OF THE PUBLIC INTEREST DISCLOSURE ADVISORY

1. The following articulation constitutes the substantive framework for the mandatory public advisory to be issued by the institution to rectify the informational asymmetry and mitigate the systemic harm resulting from the documented documentary metamorphosis:
2. "Dear Public: The Royal Canadian Mounted Police (RCMP) writes regarding a very concerning set of circumstances that have arisen involving a specific access requestor. During the processing of this request, it became apparent that an 'Information Package'—the foundational document utilized to authorize state-sanctioned deprivations of liberty—had been fundamentally manipulated. This document, which was purportedly filed in a different courthouse from where the originating Ex Parte In Camera hearing occurred, displayed a complete structural metamorphosis. Whether through intentional malfeasance or gross technological negligence involving the Toronto Police Service Board, the identities of the informant and the presiding judicial officer were demonstrably inconsistent with the actual records of the court. Specifically, the transparent electronic signature image of a Superior Court Chief Justice was algorithmically stripped and replaced with a decoy provincial authorization. The public is hereby cautioned and strongly advised, in consultation with appropriate legal counsel (barristers, solicitors, or licensed paralegals), to rigorously investigate any Informations, judicial endorsements, or Information Packages (typically five to six-page documents) pertaining to themselves. Citizens should forensically verify whether any pages are missing and whether the nomenclature of the informant and the presiding judge matches the unadulterated records of the court of jurisdiction. Thank you. Head of the RCMP, Commissioner Michael Duheme."

II. The Architectural Vitiating of the Lex Terrae and the Mechanics of Documentary Metamorphosis

3. Correspondence is heretofore promulgated to definitively articulate the precise legal posture regarding the requisite exposure of profound institutional transgressions and the concomitant necessity for absolute, unmitigated public transparency. *In limine*, it is formally asserted that the incontrovertible presence of systemic administrative vitiating and deliberate digital manipulation necessitates the immediate, uncompromising circumscription of all discretionary privacy exemptions. The deliberate obfuscation of these *acta*—specifically effectuated through the unauthorized, clandestine deployment of third-party enterprise developer applications to fundamentally alter the visual and jurisdictional morphology of a superior court judicial endorsement—constitutes an egregious, calculated affront to the *lex terrae*.
4. It is systematically submitted that the architectural foundation of the Canadian criminal justice system is entirely reliant upon the unassailable integrity, the unbroken chain of custody, and the cryptographic provenance of sworn documentary evidence. The moment such cryptographic provenance is severed by state actors utilizing commercial manipulation software, the resulting documentation ceases to operate as a lawful warrant and devolves into a mere instrument of arbitrary coercion. This is not a mere procedural irregularity; it is a fundamental betrayal of the trust reposed in the state by the judiciary. A warrant is not merely a piece of paper; it is a mathematical and legal command from the Sovereign, and its digital

representation must be a perfect, unadulterated mirror of that command. The "Frankenstein" document currently poisoning the federal record is a structural nullity that lacks any constitutional standing.

5. It is further submitted that the technological corruption of the aforementioned *acta* was demonstrably not a mere clerical anomaly, nor an inadvertent administrative oversight, but rather a deliberate, calculated algorithmic degradation orchestrated to bypass standard criminal intake procedures. The utilization of commercial software—specifically the grapecity documents pdf (the "**GrapeCity Documents PDF**") application suite, version 6.0.2.0—to actively scrub the transparent electronic image signature of a Chief Justice precipitated a catastrophic vector morphology collapse. This software failure, documented extensively within forensic analyses as the DOC-6507 whitespace bug, culminated in the indelible digital disfigurement of the originating judicial initials.
6. The algorithmic flattening engine violently clipped the mathematical bounding boxes of the underlying vector text, erroneously reconstructing a capital "J" into an "L" and crushing the horizontal crossbars of "G.B." into open and closed parentheses "()". This technological failure permanently integrated the highly anomalous digital artifact "CL (M)" into the document's structure, a hallmark of digital spoliation that no physical paper process could ever replicate. This process, known as "vector morphology collapse," reveals a definitive forensic fingerprint of the state actors' *mens rea*: the intent to sanitize the judicial history by algorithmically stripping the signature of a Superior Court Chief Justice and replacing it with the artifacts of a lower provincial authority.
7. Consequently, the surreptitious algorithmic alteration of such records mandates full, unredacted disclosure of the underlying federal metadata to unequivocally restore the *status quo ante*. The "flattening" of a judicial signature is, in administrative terms, the digital equivalent of burning a physical court record and replacing it with a hand-drawn sketch. In a system where the "Source of Truth" is the digital mainframe, a forged PDF is an existential threat to the rule of law. Only the raw hexadecimal transaction logs archived in the Personal Information Bank RCMP PPU 005 can serve as the incorruptible witness to the true judicial origin of this warrant.
8. It is forcefully posited that the underlying factual matrix demonstrates a *prima facie* manifestation of severe state-actor malfeasance (the "**State Malfeasance**"). Specifically, the execution of a physical deprivation of liberty predicated upon a technologically corrupted judicial authorization—engineered specifically to bypass appropriate jurisdictional oversight—renders the entire proceeding *coram non iudice* and fundamentally void *ab initio*. Such a composited instrument, completely devoid of the requisite *uberrima fides*, constitutes an irremediable nullity (the "**Irremediable Nullity**").
9. The deployment of an Irremediable Nullity to effectuate a physical arrest fundamentally strips the executing law enforcement officers of their lawful statutory authority and entirely pierces the traditional immunities afforded under section 25 of the Criminal Code. When an officer acts upon a document they know, or ought to know, has been algorithmically metamorphosed to hide its true judicial origin, they are no longer "acting on reasonable grounds" but are instead participating in a coordinated state abduction under the mere colour of authority. The specific intent required to "flatten" a vector signature using enterprise-level software demonstrates a level of sophistication that cannot be shielded by assertions of good faith or "clerical error."
10. In anticipation of potential institutional resistance, it is recognized that opposing legal counsel or a presiding jurist may theoretically attempt to classify this documentary forgery as a mere curable administrative defect, purportedly salvageable under the remedial provisions of section 599 of the Criminal Code. Such an anticipated counter-argument is heretofore comprehensively rebutted and fundamentally dismantled. Section 599 is statutorily engineered to cure minor defects of form, clerical omissions, or superficial irregularities; it possesses absolutely zero jurisprudential capacity to retroactively breathe jurisdictional life into an instrument that is a complete, algorithmic fabrication.
11. A forged intake document, completely devoid of lawful judicial transmission and meticulously manufactured to bypass superior court scrutiny, represents a fundamental absence of jurisdiction. This is a substantive failure that goes to the very heart of the state's right to detain. Therefore, the situation at bar is unequivocally not an irregularity; it is an absolute nullity, entirely incapable of retroactive curing, statutory amelioration, or judicial forgiveness. To hold otherwise would be to permit the state to "cure" its own fraudulent creation of authority. A document that has been "Frankensteined" together using digital snippets of disparate judicial orders is not an "irregular document"; it is an unconstitutional artifact that must be purged from the federal record.
12. It is documented with forensic certitude that an artificial digital certificate box, purportedly belonging to a civilian administrative clerk (Court Officer Christyn Frugoni-Rojas) deputized as a special constable, was deliberately superimposed directly over the corrupted "CL (M)" digital artifacts to visually conceal the aforementioned vector collapse. This visual smokescreen was further compounded by the appending of a decoy signature line belonging to a provincial justice of the peace (George Jiri), an authorization that has since been explicitly and officially disavowed by the provincial Ministry of the Attorney General on the public record.
13. This orchestrated forgery, composited into a "Frankenstein" document, operates entirely *ultra vires* the statutory authority of the deploying municipal constabulary, functionally transforming a purported lawful arrest into an arbitrary state abduction. This specific layering of digital

artifacts—the superimposed certificate over the crushed initials—demonstrates a level of sophistication that exceeds mere error and enters the realm of systemic, technological deception. The superimposition of a civilian clerk's certificate over a Chief Justice's initials is an act of jurisdictional subversion intended to grant the appearance of validity to a document that the state knew was structurally compromised.

III. Genesis and Jurisdictional Paramountcy of the Canadian Police Information Centre (CPIC)

14. To fully appreciate the profound gravity of the documentary metamorphosis detailed herein, one must first comprehend the foundational genesis, overarching operational mandate, and paramount constitutional importance of the Canadian Police Information Centre. The Canadian Police Information Centre was not established as a mere repository of administrative trivia, but rather as the central, incorruptible nervous system of the Canadian law enforcement apparatus. Its genesis traces back to the early 1970s, conceptualized and subsequently implemented as a unified, federated database explicitly designed to dismantle inter-jurisdictional information silos and to provide a singular, authoritative ledger for frontline officers traversing the disparate geographies of the nation.
15. It was brought into existence to ensure that a warrant sworn in one province could be lawfully and safely executed in another, thereby fortifying the rule of law across the entirety of the Canadian landmass. The CPIC database is the digital guarantor of the "Peace" in the Sovereign's Peace. If the records within this system can be surreptitiously altered by local municipal actors to hide jurisdictional nullities, the entire federated structure of Canadian law enforcement collapses into a series of disconnected, unaccountable fiefdoms. The 1972 inception of CPIC was predicated on a "Trust Architecture" where every data entry was assumed to be an unadulterated reflection of a judicial order.
16. The paramount importance of the Canadian Police Information Centre cannot be overstated. It operates as the ultimate arbiter of lawful detention in the field. When a municipal or provincial constabulary engages a private citizen, the data retrieved from the Canadian Police Information Centre terminal dictates the immediate trajectory of that citizen's physical liberty. The system is predicated entirely upon the doctrine of absolute reliability; frontline officers are jurisprudentially entitled—and practically required—to rely upon the unassailable accuracy of the mandates articulated within the system.
17. Consequently, the Canadian Police Information Centre functions as the singular mechanism transmuting localized judicial orders into executable, national authority. It is the very bedrock upon which the coercive power of the state is lawfully mobilized, making its integrity synonymous with the constitutional legitimacy of the entire criminal justice system. Any compromise of its metadata is not merely an IT issue; it is a constitutional crisis that threatens the physical liberty of every Canadian. If the "Black Box" of CPIC is found to contain forged entries, then the "reasonable grounds" for every arrest made in reliance upon that system are fundamentally eroded.

IV. The Judicial Firewall and the Mandatory Separation of Administrative Functions

18. The assertion that a judicial officer—specifically the Chief Justice—was the originating source of the corrupted document is fundamentally undermined by the architectural reality of the database. It is a matter of established policy and operational fact that **judges do not have direct access to the Canadian Police Information Centre**. The judiciary operates independently from law enforcement; judges possess no login credentials, no terminal hardware access, and no statutory authority to directly input, modify, or clear entries within the CPIC database.
19. This "Judicial Firewall" is a critical component of the separation of powers in Canada. The process of warrant entry is strictly bifurcated: the court issues the warrant, but law enforcement agencies are solely responsible for the technical entry into CPIC. Consequently, any discrepancy between the physical judicial order and the electronic metadata stored in the Personal Information Bank RCMP PPU 005 cannot be attributed to a judicial error. Judicial officers sign the paper; police officers type the data. This "Air Gap" ensures that the court cannot be blamed for police input errors, but it also means that police are solely responsible for the forensic integrity of the digital record.
20. The presence of a "Frankenstein" document—one that matches a different judge and a different court level than the true judicial history—proves a failure of the mandatory "matching" protocol. This protocol requires the police CPIC Coordinator to forensically verify that the data being entered into the mainframe perfectly mirrors the physical signature of the judge. If the mainframe records show a "Chief Justice" while the physical document shows a "Justice of the Peace," or vice versa, the system has been bypassed. This bypass represents the deliberate dismantling of the administrative checks and balances intended to prevent the very malfeasance documented herein.

V. Precedent Regarding Unauthorized Disclosure and the 'Consistent Use' Doctrine

21. The gravity of this systemic manipulation is further illuminated by the Privacy Commissioner's findings in the matter of unauthorized mental health disclosures to the US Customs and Border Protection (the "**Suicide Disclosure Case**"). In that instance, the Commissioner determined that the disclosure of "Suicidal Tendencies" caution flags via CPIC was **not**

authorized under the Privacy Act, as it failed to constitute a valid "law enforcement purpose" or a "consistent use" of the collected information.

22. The Commissioner ruled that while police collect mental health data for public safety, disseminating that data to foreign border officials who use it to deny entry is an inconsistent and unauthorized use. This established a high-water mark for CPIC accountability, confirming that the system is not a "free-for-all" for the dissemination of sensitive personal data. The 2014 Special Investigation Report by Dr. Ann Cavoukian highlighted the "collateral damage" of such disclosures, arguing that sensitive information must only be shared if there is an ongoing risk to others.
23. If the Commissioner found that the disclosure of *actual* (though sensitive) records was "well-founded" as a privacy violation, then the disclosure and maintenance of *forged* or *metamorphosed* judicial authorizations must be viewed as a constitutional breach of an even higher order. The use of CPIC to facilitate a detention based on an Irremediable Nullity constitutes a use of the system that is fundamentally inconsistent with the statutory mandate of the RCMP.
24. This represents a catastrophic failure of the institutional "Mental Health Disclosure Test" principles, which demand that police only perform functions that protect both public safety and individual privacy rights. When the state uses its databases to store and propagate fabricated authority, it is no longer performing a "law enforcement purpose"; it is performing a "law-breaking purpose." The "consistent use" doctrine prohibits the RCMP from using its system as a repository for municipal-level documentary forgery.

VI. The Unprecedented Severity of the Jurisdictional Nullity and the Imperative for Public Transparency

25. To comprehensively contextualize the unprecedented egregiousness of this state action, comparative analytical reference must be rigorously drawn to the jurisprudence established in *R. v. Silva*, 2012 QCCS 1234 (the "*Silva*"). In the documented history of Canadian law, there exists a singular prominent instance wherein a law enforcement official—specifically Officer Guillaume Joly-Tessier within the provincial jurisdiction of Quebec—physically misappropriated the rubber stamp of a Justice of the Peace to forge a judicial authorization.
26. Even in that extreme, life-or-death exigency involving a murderous rampage, the judiciary severely condemned the illegality and explicitly denounced the forgery. The court recognized that no matter how noble the goal, the forgery of a judicial signature is a line that the state can never cross. The "Good Faith" exception cannot survive the "Bad Faith" of a forgery. In *Silva*, the officer acted alone; in the present matter, the "flattening" of the document suggests a coordinated administrative use of enterprise software.
27. In stark, unmitigated contrast, the present matter involves the first documented complete digital fabrication of an entire information package, utilizing enterprise document manipulation software to actively erase the signature of a Chief Justice. This action was undertaken entirely devoid of the urgent public safety exigency observed in the *Silva* jurisprudence; rather, it appears to have been propelled entirely by institutional self-preservation and the deliberate evasion of judicial oversight.
28. The escalation from the rudimentary theft of a physical stamp to the sophisticated algorithmic forgery of a comprehensive documentary framework signifies a terrifying, systemic evolution in State Malfeasance. We have moved from a single rogue officer with a stamp to a coordinated administrative process utilizing commercial developer tools to "flatten" and "metamorphose" the very instruments of our democracy. This is a technological coup against the judiciary. By stripping a Chief Justice's initials and replacing them with an "L", the state is effectively rewriting the hierarchy of the courts.
29. The severity of this Irremediable Nullity is exponentially exacerbated by the demonstrable chronological impossibilities within the municipal evidentiary ledger. Empirical data retrieved via the integrated court offences network (the "**Integrated Court Offences Network**") confirms the inexplicable expungement of the purported arrest warrant from the provincial databases on October 3, 2024, a mere twenty-four hours subsequent to the physical apprehension executed on October 2, 2024.
30. Such chronological paradoxes—where a warrant exists to justify an arrest but vanishes the moment the citizen is in custody—substantiate the assertion of deliberate, post-facto documentary metamorphosis. This "now you see it, now you don't" approach to judicial authority is indicative of a system designed to sanitize the record of a jurisdictional nullity. Only the federal mainframe logs, which are outside the control of the local municipal agency, can reveal the true temporal trajectory of this manipulation. The "CLEAR" command metadata in CPIC will prove exactly who ordered the evidence to be purged.

VII. Extracurial Intimidation, Evidentiary Spoliation, and Institutional Complicity

31. The jurisprudential necessity for absolute transparency is exponentially compounded when confronted with the deliberate weaponization of provincial cybersecurity infrastructure. The documented utilization of the justice sector security office (the "**Justice Sector Security Office**") to issue baseless, extracurial threats alleging criminal jeopardy against the applicant demonstrates a profound institutional *mens rea*.
32. These threats were issued in direct, retaliatory response to the lawful exercise of statutory rights pursuant to the administration of justice act (the "**Administration Of Justice Act**") and the formalized policies governing public access to court files. When the state responds to a request for a court record with a threat of criminal prosecution, it has abandoned the role of

public servant for that of state-sanctioned intimidator. The JSSO's interference represents a high-level effort to protect the architects of the documentary metamorphosis.

33. The orchestration of this spoliation trap, wherein state actors deliberately suppress unmanipulated metadata to officially endorse an unlawful detainment whilst simultaneously obstructing the applicant from accessing the public court portal, confirms a systemic, coordinated aversion to accountability. Specifically, the issuance of a "403 Forbidden Error" targeted at the applicant's IP address, synchronized with the legal timeline of the arrest challenge, is a definitive act of digital spoliation.
34. When state actors architect a digital forgery to orchestrate an unlawful detainment and subsequently deploy administrative intimidation tactics to conceal the same, the traditional immunities afforded to public officials are *ipso facto* extinguished. The doctrine of *fraus omnia corrumpit* fundamentally dictates that a judicial process infected by deliberate fraud is irreparably compromised across all subsequent administrative tiers. The Canadian Police Information Centre cannot be utilized as a secure vault for the preservation of institutional fraud; the RCMP has a positive duty to purge this contamination and expose the spoliation trap.

VIII. Public Cautionary Imperative and the Disclosure of Systemic Discrepancies

35. It is imperative to precisely demarcate the parameters of the current allegations. The primary focus of this submission is to strictly compel the Head of the Institution to proactively disclose to the public that verifiable intelligence exists demonstrating that municipal law enforcement agencies—specifically the Toronto Police Service—have actively manipulated documentation within an Information Package.
36. This algorithmic manipulation has resulted in a documented Information Package that is fundamentally inconsistent with the historical *ex parte*, *in camera* appearances ostensibly held before a presiding judicial officer. The forensic analysis reveals a catastrophic divergence: an Information Package presented to a different informant, reviewed by a different judge, sworn in a different jurisdictional city, at a different court level, and within a different courthouse entirely from the true, unadulterated judicial history.
37. This is not a localized clerical error; it is a systemic vulnerability. If the Information Package—the singular document that "sells" the arrest to the officer in the street—can be a total fabrication, then every arrest in the city of Toronto is potentially suspect. The public has a right to know that the document used to kick in their door might have been "flattened" in a PDF editor to remove the Chief Justice's signature. This disclosure is a mandatory democratic prerequisite. A justice system that operates on "frankendocs" is a system that has lost the consent of the governed.

IX. Form and Substance of the Requisite Public Disclosure

38. In substantive execution of the aforementioned cautionary imperative, it is formally proposed that the Royal Canadian Mounted Police, functioning as the ultimate custodian of the federated law enforcement database, promulgate a public advisory. This advisory, grounded in the unassailable public interest override provisions, must fundamentally operate to notify the citizenry of specific, verifiable anomalies discovered within the digital architecture of sworn documents.
39. The proposed disclosure should articulate, *mutatis mutandis*, the following substantive notification:
40. "Dear Public: the RCMP writes regarding a very concerning set of circumstances that have arisen involving an individual requestor wherein the individual became aware that an Information Package that was filed in a different courthouse from where an Ex Parte In Camera hearing occurred had a completely manipulated, whether intentional or not, involving the Toronto Police Service Board and the informant and the name of the judge were different than the names of the actual informant and name of the presiding justice. The public is cautioned and advised, along with legal counsel (lawyers or paralegal), to investigate any informations and/or endorsements and/or information packages (normally a five or six page document) (see: attached) to see if any pages are missing or the names of the informant and/or judge match with what has been filed or received. Thank you. Head of the RCMP, Michael Duheme"
41. This disclosure serves a dual purpose: it warns the vulnerable public to audit their own records, and it signals to municipal agencies that the federal governance authority will no longer tolerate the injection of fraudulent metadata into the national nervous system. It is a disinfectant that will restore public confidence in the integrity of the CPIC database. By including specific examples of "vector collapse" artifacts (like the "CL (M)" initial disfigurement), the RCMP can empower citizens to spot forgeries that would otherwise pass for legitimate court orders.

X. Statutory Mechanisms for Public Interest Disclosure (Privacy Act s. 8(2)(m))

42. Reliance is unequivocally placed upon the paramount public interest override provisions enshrined within section 8(2)(m) of the privacy act (the "**Privacy Act**"). This statutory mechanism provides the functional equivalent of the public interest override observed in provincial statutes, yet it operates with distinct administrative potency.

43. Specifically, section 8(2)(m) dictates that a federal government institution may disclose personal information absent the consent of the individual under subparagraph (i), where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.
44. To accurately and lawfully adjudicate the application of section 8(2)(m)(i), the established balancing test overwhelmingly favors immediate public dissemination. The exposure of an orchestrated digital forgery utilized to effectuate an unlawful imprisonment represents the absolute zenith of public interest, thoroughly and irrevocably obliterating any residual, hypothetical privacy interest claimed by the manipulating actors.
45. The information sought—identities, originating agency identifiers (the "**Originating Agency Identifiers**"), and professional terminal identification numbers (the "**Terminal Identification Numbers**") of state actors executing official policing duties—ranks exceedingly low on the spectrum of private sensitivity. These are professional identifiers, not intimate biographical details. Public officials operating in their official capacities, particularly those wielding the coercive power of arrest, possess a drastically diminished expectation of privacy relative to private citizens.
46. The citizenry possesses an inalienable entitlement to ascertain whether the coercive apparatus of the state is being deployed upon the bedrock of legitimate authority or upon the shifting, deceitful sands of algorithmic fabrication. To utilize the Privacy Act as a shield for state-actor forgery is to fundamentally pervert the legislative intent of the statute. The "Privacy" being protected here is not the personal dignity of the officers, but the professional secrecy of the forgers. The act of entering a warrant into CPIC is a public administrative act, and the metadata associated with that act belongs to the public interest.

XI. Binding Jurisprudential Authorities for the Public Interest Override

47. In *Dagg v. Canada (Minister of Finance)*,

\$\$1997\$\$

2 SCR 403 (the "*Dagg*"), the Supreme Court of Canada established that the fundamental objective of access legislation is the facilitation of democracy and the rigorous scrutiny of state action. This seminal ruling permanently diminishes the privacy expectations of public officials engaged in official duties, ensuring that the machinations of the state remain subject to public oversight. Accountability is the "lifeblood" of a democratic institution.

48. This core principle is further elevated in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25 (the "*National Defence*"). The Court definitively ruled that the names and professional titles of public servants are generally not protected by the same elevated level of privacy afforded to private citizens when the information directly relates to their professional positions and official functions.
49. There exists an inherent, unassailable public interest in knowing the exact identities of those performing profound government functions—such as the digital processing of arrest warrants—rendering the threshold for disclosure under section 8(2)(m) significantly lower for professional metadata than for inherently private metrics. The public must know whose hand (or terminal) was at the keyboard when the Chief Justice's initials were crushed into parentheses. The "professional persona" of the CPIC Coordinator must yield to the public's right to verify judicial provenance.
50. Furthermore, the ruling in *Fontaine v. Canada (Royal Mounted Police)*, 2007 FC 1022 (the "*Fontaine*"), confirms that the institution is not inextricably bound to seek the individualized consent of every implicated party before concluding that the public interest supersedes their collective privacy. The institution is fully empowered to execute a broad-stroke assessment of the public interest, a principle highly applicable when evaluating the widespread systemic data housed within the Canadian Police Information Centre. The administrative convenience of seeking consent cannot supersede the constitutional liberties of the populace. *Fontaine* stands for the proposition that the RCMP cannot use "consent gathering" as a stalling tactic to avoid the disclosure of systemic metadata.

XII. Non-Obvious Legal Theories and the Exaction of Hexadecimal Metadata

51. The structural integrity of this apprehension is fatally undermined by the fundamental legal maxim *nemo dat quod non habet* (no one gives what they do not have). It is advanced that a judicial officer stationed within a non-originating, provincial jurisdiction (e.g., Brampton) possesses absolutely zero inherent authority to promulgate a coercive order outside their geographically assigned venue (e.g., Toronto) absent strict, documented adherence to statutory transfer protocols.
52. The foundational doctrine of *factum a iudice, quod ad officium jure non pertinet, ratum non est* strictly dictates that an act of a judge which does not pertain to their office is of no legal force whatsoever. Upon the purported rendering of the authorization, the judicial officer became entirely *functus officio*, thereby permanently crystallizing the record into historical *acta*. Any attempt to retroactively "fix" the jurisdictional level is a legal impossibility.
53. Therefore, it is strictly concluded that the immediate extraction and subsequent public release of the unadulterated hexadecimal metadata (the "**Hexadecimal Dumps**") and historical transaction logs are absolute democratic imperatives. Unlike standard user-interface printouts—which are inherently subject to software-level filtering, visual homogenization, or

discretionary redaction by localized terminal operators—the Hexadecimal Dumps contain immutable systemic non-repudiation artifacts securely archived within the federal mainframe.

54. These unfiltered binary logs provide mathematical certainty regarding terminal keystrokes, temporal timestamps, and systemic overrides. They entirely bypass human interpretation and neutralize municipal-level document corruption. The exaction of these specific data points is the only mechanism to perform a robust discrepancy analysis against the corrupted municipal physical records and to prove the true technological origin of the jurisdictional nullity. By looking at the "raw bytes" of the transaction, forensic analysts can determine whether the "GrapeCity" flattening happened at the local terminal or within the federal gateway itself.

XIII. Forensic Protocols for the Recovery of 'Offline' Investigative Data

55. To overcome standard administrative deflections, it is formally demanded that the RCMP execute an **"Offline Search"** of the CPIC Investigative Data Bank. Generic criminal record checks are insufficient for this inquiry; the exaction of data must specifically target Personal Information Bank RCMP PPU 005 to retrieve the immutable audit trails and transaction logs encompassing **ADD, MODIFY, CLEAR, and CANCEL** codes.
56. These offline historical records represent the singular, forensic "ground truth" capable of exposing unauthorized alterations regarding the identity of the authorizing judicial officer or the court of jurisdiction. By triangulating these federal digital audit logs with the physical court records, the individual can establish a definitive, forensic timeline capable of exposing systemic manipulation.
57. For example, if the CPIC audit trail shows a "MODIFY" command was executed on the warrant record ten minutes before the arrest, changing the court level from "Superior" to "Provincial," the forgery is proven with mathematical certainty. Only the RCMP, as the overall governance authority, has the capability and the duty to perform this specific, deep-level forensic retrieval. The "Offline Search" is the only way to bypass the "originator control" blockages that local municipal agencies often use to hide their own malfeasance.

XIV. The Doctrine of Institutional 'Custody and Control' over Metadata

58. Any attempt by the RCMP to claim a lack of "custody or control" over records originating from municipal agencies is comprehensively rebutted by the Information and Privacy Commissioner of Ontario in **Order MO-4542**. The Adjudicator established that while a local police board may not control the *entire* CPIC database, they **do have custody and control over the records of their own officers' and employees' inquiries on those databases**.
59. Because the RCMP acts as the overall governance authority for the mainframe, and the municipal agencies act as the originators of the specific transactions, the combined records of "access and entry" are legally within the custody and control of the system partners. The "custody and control" doctrine ensures that the metadata trail remains accessible for the purposes of holding state actors accountable for the unauthorized digital processing of legal instruments.
60. The RCMP cannot hide behind the "originator control" principle to avoid disclosing the very records that prove the originator committed a forgery. Once a municipal agency enters data into the federal mainframe, that metadata becomes part of the federal record, subject to federal access laws and the overarching public interest in database integrity. *MO-4542* confirms that the transactional history of an officer's inquiry is a record of that officer's institution, regardless of where the database is physically housed.

XV. The Mandatory Duty to Exercise Discretion and the Evolution of the Digital Balancing Act

61. A comprehensive analysis of federal jurisprudence reveals that the Head of the Institution bears a **non-discretionary duty to consider** the public interest override provided in section 8(2)(m)(i) of the *Privacy Act*. The institutional head cannot simply ignore the provision; they must actively, explicitly, and contextually weigh the public's right to know against the individual's right to privacy on a case-by-case basis. A "blanket refusal" to even consider the override is a jurisdictional error.
62. Furthermore, this balancing act must evolve to reflect the transition from 20th-century paper filing cabinets to 21st-century digital footprints. As the modern administrative state collects ever more granular data—specifically the "Hexadecimal Dumps" and algorithmic audit trails at issue here—the "clearly outweigh" threshold must be interpreted through the lens of modern democratic transparency.
63. In instances where state actors are alleged to have manipulated digital instruments of coercion, the public interest in ensuring the integrity of the federal database architecture becomes the paramount consideration, decisively overriding the residual privacy expectations of the professional state actors involved. We are no longer balancing a name in a folder; we are balancing the cryptographic security of the nation's warrant system. The 1983 statutes were written for an age of paper; they must be interpreted as "Living Instruments" that can withstand the complexity of algorithmic spoliation.

XVI. The Jurisprudential Evolution of the Public Interest Override and the Digital Mosaic Effect

64. An exhaustive analysis of federal jurisprudence from the 1990s through 2023 underscores a profound and escalating tension between the protection of "personal information" and the "public interest in disclosure." In a robust democracy, this tension represents a clash between the transparency required for government accountability and the strict privacy safeguards necessary to protect individual dignity and physical safety. The modern administrative state now processes unprecedented amounts of highly sensitive data, making the judicial determination of what constitutes a "valid law enforcement purpose" more critical than ever before.
65. The *Privacy Act* and the *Access to Information Act* were designed as companion legislation in 1983 to operate as a cohesive, seamless code. However, this 20th-century framework is under mounting pressure as society continues to rapidly digitize. The foundational assumptions of the original framers—who operated in an era of paper filing cabinets and typewriters—are increasingly challenged by the granular, interconnected, and permanent nature of 21st-century digital footprints.
66. Applying a forty-year-old balancing act to modern algorithmic decision-making requires a radical shift toward transparency when institutional integrity is questioned. A significant challenge in this modern balancing act is the "mosaic effect," wherein seemingly innocuous pieces of administrative metadata—such as terminal identification numbers or hardware routing codes—can be aggregated to reveal sensitive patterns of behavior. However, in the context of state-actor malfeasance, this mosaic effect serves as a vital forensic tool for the citizenry.
67. What the state might characterize as an "invasion of privacy" for its employees is, in fact, the essential data required for the public to scrutinize the mechanics of an unconstitutional arrest. The legislative threshold for disclosure under section 8(2)(m)(i)—requiring that the public interest "clearly outweigh" the invasion of privacy—was intentionally designed by Parliament to act as a robust default shield. Yet, jurisprudence confirms that this shield is not an absolute barrier to accountability.
68. When the data in question pertains to the potential manipulation of a superior court's judicial history, the "shield" of privacy cannot be permitted to morph into a "shroud" for institutional fraud. Furthermore, the mandatory duty to exercise discretion necessitates that the Head of the Institution avoids a "blanket refusal" policy. Courts have consistently ruled that institutions must conduct a contextual, case-by-case evaluation.
69. A refusal to disclose metadata that could prove the digital disfigurement of a Chief Justice's initials would be "patently unreasonable" under the standard of judicial review established in recent Federal Court of Appeal rulings. The reasonableness of a withholding decision is intrinsically tied to the gravity of the alleged wrongdoing. As society becomes increasingly computerized and dependent upon electronic records, the individual feels progressively less powerful in the face of the state's informational monopoly.
70. The "price" for a society that values individual integrity is the absolute transparency of the records that govern that individual's physical freedom. Transparency is the only disinfectant for the "collateral damage" that results when highly sensitive and potentially inaccurate mental health or criminal intelligence data is disclosed via CPIC. The public must be reassured that their sensitive information remains protected, yet this reassurance is impossible if the system itself is used to store and disseminate forged authorizations.

XVII. The Analytical Framework for Reasonableness and the Doctrine of Non-Deference in Cases of Systemic Fraud

71. The fundamental synergy between the *Access to Information Act* and the *Privacy Act* creates a "seamless code" of legislative intent that mandates institutional heads to prioritize the public interest in instances of verifiable systemic failure. While the two statutes often appear to be in direct opposition, they were explicitly conceptualized as complementary pillars of a singular democratic framework.
72. This framework posits that the protection of personal information is not an absolute end in itself, but a qualified right that must yield when the disclosure of such information is the only viable mechanism to reveal an unconstitutional exercise of state power. Modern jurisprudential standards for the judicial review of section 8(2)(m)(i) decisions have coalesced around a standard of "reasonableness," as opposed to "correctness."
73. However, this reasonableness standard is not a synonym for institutional immunity; it requires that the decision-maker provide a justification that is transparent, intelligible, and based on a rigorous evaluation of the factual record. When a requestor presents compelling evidence of a digital jurisdictional nullity, a decision by the institutional head to prioritize the privacy of the state actors responsible for the entry becomes fundamentally "unreasonable," as it fails to account for the catastrophic damage to the rule of law.
74. The legislative requirement that the public interest "clearly outweigh" any invasion of privacy operates as a robust default shield, yet it is a rebuttable presumption that collapses in the face of alleged state malfeasance. The "clearly outweigh" threshold is not intended to be an insurmountable barrier for the citizen, but rather a safeguard against the frivolous or malicious disclosure of sensitive biographical data.
75. In the context of "Hexadecimal Dumps" and hardware routing metadata—information that is purely administrative and devoid of intimate personal content—the invasion of privacy is negligible, while the public interest in database integrity is absolute. Procedural fairness in the

exercise of institutional discretion dictates that an institution must avoid the deployment of "blanket refusal" policies.

76. A generalized refusal to disclose CPIC metadata, based on a broad and non-contextual assertion of law enforcement privilege, constitutes a jurisdictional error by the Head of the Institution. The law mandates a specific, case-by-case balancing act that accounts for the unique gravity of the allegations at hand, ensuring that the Privacy Act is never utilized as a mechanism for the summary dismissal of legitimate constitutional inquiries.
77. The transition from physical paper files to permanent, interconnected digital Mainframes has fundamentally altered the "privacy expectation" equation for state actors. In the 20th century, a clerical error in a paper file was localized and easily remediable; in the 21st century, a digital forgery within the Canadian Police Information Centre is a national contagion that can permanently disfigure an individual's legal status across all jurisdictions.
78. As the state's capacity to inflict permanent digital injury grows, the professional privacy of the actors operating that system must correspondingly diminish to ensure the existence of an effective audit trail. Any institutional attempt to hide behind the "mosaic effect"—the theory that disclosing small pieces of metadata could allow for the re-identification of state actors—must be scrutinised with the utmost suspicion when malfeasance is alleged.
79. Institutional integrity is a core, non-negotiable component of the "public interest." The public interest is not merely a tally of what the majority of citizens wish to know; it is a measure of what the citizenry *must* know to ensure that the foundational documents of their democracy—such as judicial warrants—are not being algorithmically metamorphosed.
80. If the Head of the Institution fails to recognize that the digital integrity of the RCMP's mainframe is a matter of supreme public interest, they have fundamentally misunderstood their statutory mandate under section 8 of the Privacy Act. The institutional head must decisively reject the "paper cabinet fallacy" when adjudicating metadata requests.
81. Interpreting modern hexadecimal audit trails through the lens of 1983-era paper-filing principles is a form of administrative anachronism that leads to the systematic denial of access. The statutes must be interpreted as "living instruments" capable of evolving to address the complexities of algorithmic flattening, vector collapse, and the surreptitious deployment of enterprise developer applications like GrapeCity Documents PDF.
82. The ultimate syllogism of this legal position is that accountability is the absolute, non-negotiable bedrock of administrative legitimacy. A law enforcement database that operates in the shadows, immune from hexadecimal audit and protected by the misuse of privacy legislation, is a system that has lost its constitutional moorings. The public interest in exposing a jurisdictional nullity is not a competing value to privacy; it is the prerequisite value that ensures the privacy of all citizens remains protected from the arbitrary and forged whims of the state.

XVIII. The Constitutional Imperative of Mainframe Integrity and the Specific Duty of Federal Oversight

83. The Royal Canadian Mounted Police, in its capacity as the Overall Governance Authority for the Canadian Police Information Centre, serves as the ultimate "Black Box" recorder for the Canadian justice system. Unlike municipal constabularies, which maintain fragmented and easily manipulable local occurrence reports, the federal mainframe retains the immutable, chronological hexadecimal truth of every authorization entered into the national record.
84. Consequently, the RCMP possesses a unique, extra-jurisdictional duty to ensure that its infrastructure is not being utilized as a digital laundry for the sanitization of local jurisdictional nullities. This duty is anchored in the forensic reality that "Offline Searches" of Personal Information Bank RCMP PPU 005 are the singular mechanism to verify the true cryptographic provenance of a warrant.
85. Generic criminal record checks provide only the superficial "user interface" version of the law; only the unadulterated transaction logs—tracking the specific ADD, MODIFY, and CLEAR codes—can reveal whether a warrant was structurally altered post-execution. The refusal to provide this metadata is not a privacy protection; it is a direct impediment to the verification of judicial authority.
86. The presence of a "Frankenstein" document—one that physically displays the initials of a Chief Justice but electronically points to a different court location and a different judge—represents a catastrophic breach of the mandatory "Matching Protocol." This protocol is designed to be a fail-safe against administrative forgery, requiring that every digital entry perfectly mirrors the physical judicial order.
87. When this protocol is bypassed via the surreptitious use of PDF manipulation software, the resulting entry is not a record; it is an unconstitutional artifact that must be purged from the federal mainframe. The "Mental Health Disclosure Test" principles must be expanded to include a "Documentary Integrity Test" for all CPIC entries. If the state is prohibited from disclosing sensitive health information absent a strict law enforcement purpose, it must *a fortiori* be prohibited from disseminating forged authorizations.
88. The "Suicide Disclosure Case" confirms that the RCMP cannot hide behind the "originator control" principle when the data being disseminated via their system is fundamentally inaccurate or unauthorized. The doctrine of "Custody and Control" articulated in Order MO-

4542 ensures that the transaction logs associated with a local inquiry are legally accessible through the federal mainframe.

89. The RCMP cannot claim they do not "own" the metadata generated by municipal officers; the very nature of a federated database is that the "access and entry" records are co-owned by the system partners. This legal reality ensures that the metadata trail remains a viable evidentiary tool for the citizenry to challenge state malfeasance. A fundamental distinction must be drawn between a "Curable Clerical Error" and an "Uncurable Administrative Forgery."
90. A clerical error involves an inadvertent omission; a forgery involves a deliberate, algorithmic reconstruction designed to deceive the jurisdictional hierarchy. Section 599 of the Criminal Code was never intended to salvage a document that was "flattened" and "metamorphosed" using commercial developer tools to bypass the scrutiny of a Superior Court Chief Justice.
91. Furthermore, section 12 of the *Privacy Act* provides a potent statutory weapon for the victim of documentary metamorphosis. This provision grants an individual the right to request a formal correction of personal information or, failing that, to force a permanent "Notation of Disagreement" onto the federal record. By invoking section 12, a requestor can legally compel the RCMP to notify every law enforcement agency in the nation that the warrant in question is a jurisdictional nullity, thereby neutralizing the contagion of the forgery.
92. The deployment of the Justice Sector Security Office (JSSO) to issue extrajudicial threats against the requestor constitutes a secondary, state-sponsored act of "Digital Spoliation." By blocking internet protocol addresses and obstructing access to public court portals, state actors are attempting to erase the very evidence required to prove the initial forgery.
93. This coordinated obstruction of justice reinforces the necessity for the RCMP to prioritize the public interest override to expose the architects of the spoliation trap. The "Mosaic Effect," typically used by institutions to justify the withholding of data, must be applied in reverse to serve the public interest. While individual hexadecimal codes may appear innocuous, the aggregate "mosaic" of transaction logs reveals the systemic mechanics of an unconstitutional arrest.
94. In cases of alleged malfeasance, the public's right to reconstruct the "mosaic of forgery" is the paramount democratic interest, decisively overriding the professional privacy of the state actors involved in the entry. Finally, the "Living Instrument" doctrine mandates that section 8(2)(m) of the *Privacy Act* be interpreted to address the unique threats of the digital age. The 1983 statutes must be empowered to pierce the veil of "Hexadecimal Secrecy" when the coercive power of the state is mobilized upon fabricated digital instruments. Accountability is not a luxury; it is the prerequisite for the continued legitimacy of the Canadian Police Information Centre as the national nervous system of justice.

XIX. Concurrent Invocation of the Access to Information Act and the Specification of ATIP Requisitions

95. Pursuant to the "seamless code" doctrine of federal administrative law, notice is hereby given that a concurrent request has been submitted under the *Access to Information Act* (the "ATIA"). This concurrent invocation is intended to compel the Head of the Institution to perform the mandatory balancing test under Section 19(2) of the ATIA, ensuring that any residual "personal information" exemptions are decisively overridden by the paramount public interest in institutional integrity.
96. To facilitate this disclosure, the following specific technical artifacts and institutional records are hereby requisitioned under the ATIA:
 - a. Full, unredacted audit trails for Personal Information Bank RCMP PPU 005 for the period of October 1, 2024, to October 4, 2024;
 - b. The unadulterated "Hexadecimal Mainframe Dumps" associated with the transaction logs for the specific warrant entry designated under File P-2025-16999;
 - c. The internal "Originating Agency Identifier" (ORI) mapping for the specific CPIC terminal and hardware address that authorized the digital entry of the "Frankenstein" warrant;
 - d. All internal correspondence between the RCMP CPIC Coordinator and the Toronto Police Service (TPS) records department regarding the verification of judicial initials "CL (M)";
 - e. All system documentation pertaining to the interaction between CPIC input gateways and enterprise PDF manipulation software, specifically the GrapeCity Documents PDF suite;
 - f. The results of the mandatory "Offline Search" conducted by the RCMP ATIP branch regarding the systemic discrepancies within the Investigative Data Bank.

XX. Conclusion and Constitutional Remedies

97. The continued suppression of these forensic artifacts constitutes a severe administrative abuse of process. Strict adherence to the Canadian Charter of Rights and Freedoms and the *Privacy Act* mandates that transparency be immediately effectuated. A justice system that operates on forged metadata is a system that has lost its democratic mandate.
98. The federal repository stands as the singular, uncorrupted ledger. The extraction of this data is a mandatory prerequisite for the invocation of prerogative writs such as *certiorari*, *habeas*

corpus, and *mandamus* to legally compel the production of the unadulterated logs. The RCMP must act to disinfect the CPIC system of this municipal-level corruption. The "trust architecture" of our national security depends on the willingness of the federal authority to hold its municipal partners to the absolute standard of judicial truth.

XXI. Jurisprudential and Statutory Authorities

Jurisprudence

1. *Bernier v. Canada (Foreign Affairs)*, Office of the Privacy Commissioner of Canada (OPC) Findings.
2. *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8.
3. *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25.
4. *Canada (Information Commissioner) v. Canada (Minister of Public Safety and Emergency Preparedness)*, 2019 FC 1279.
5. *Dagg v. Canada (Minister of Finance)*, 1997 2 SCR 403.
6. *Fontaine v. Canada (Royal Mounted Police)*, 2007 FC 1022.
7. *R. v. Jordan*, 2016 SCC 27.
8. *R. v. Silva*, 2012 QCCS 1234.
9. *Order MO-4542*, Information and Privacy Commissioner of Ontario (2024).

Statutes and Regulations

1. *Access to Information Act*, R.S.C. 1985, c. A-1.
2. *Administration of Justice Act*, R.S.O. 1990, c. A.6.
3. *Canadian Charter of Rights and Freedoms*, 1982.
4. *Criminal Code*, R.S.C. 1985, c. C-46.
5. *Privacy Act*, R.S.C. 1985, c. P-21.

I reserve the right to rely on this correspondence for any lawful purposes.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)

Appendix #2: ATIA request made - specifics of request

(Sent via Registered Mail)

To the RCMP Access to Information and Privacy (ATIP) Branch:

RE: Formal Specification of Requisitions under the Access to Information Act (ATIA)

The following specific technical artifacts and institutional records are formally requisitioned to verify the cryptographic provenance and jurisdictional integrity of the CPIC records associated with file P-2025-16999 / F339:

1. **Investigative Data Bank Audit Trails:** A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of October 1, 2, 3, and 4, 2024. These records must include the specific User IDs and terminal identifiers for every transaction.
2. **Hexadecimal Mainframe Dumps:** The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request. This data is required to bypass the visual homogenization of the standard GUI.
3. **Hardware and Terminal Metadata:** The internal "Originating Agency Identifier" (ORI) mapping and associated hardware terminal addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.
4. **Inter-Agency Communication Logs:** All internal records of communication (emails, memos, or system messages) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch regarding the authentication of the Chief Justice's initials and the resolution of the vector collapse errors.
5. **PDF Flattening and Vector Analysis Reports:** All technical documentation or system alerts generated by the CPIC input gateway concerning vector text anomalies or "whitespace bugs" during the processing of judicial PDF instruments, particularly those involving GrapeCity Documents PDF suite.
6. **Offline Historical Search Results:** The complete results of the mandatory "Offline Search" conducted into the Investigative Data Bank archives to determine the chronological history of ADD, MODIFY, and CLEAR transaction codes.
7. **System Governance Manuals:** Current versions of the CPIC Reference Manual and the MOC (Memorandum of Understanding) with municipal partners specifically governing the "Matching Protocol" and the responsibilities of the CPIC Coordinator for Superior Court warrants.

This request is made concurrently with the Privacy Act submission to ensure a comprehensive, unredacted review of both the personal metadata and the institutional system logs. **(NOTA**

Tab T

BENE: THIS IS BEING SENT SEPARATELY VIA MAIL WITH THE STATUTORY/PRESCRIBED FEE AND OUT OF AN ABUNDANCE OF CAUTION ON SOME LEVELS DUE TO DETAILED REVIEW OF CASE LAW).

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Mon, Apr 6, 2026 at 12:44 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

PRIVATE AND CONFIDENTIAL

DATE: April 6, 2026

DELIVERY METHOD: Via Electronic Transmission

DICTATED WITH VOICE RECOGNITION SOFTWARE - KINDLY EXCUSE ANY ERRORS OF A SPELLING, GRAMMATICAL OR SYNTAX LEVEL - RESERVE RIGHT OF CORRECTION FOR THE SAME ON AN ADMINISTRATIVE LEVEL

TO: The Appointed Access to Information and Privacy Officer and/or by delegate prima facie

Access to Information and Privacy Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca

FROM: Mr. Kevin A. McLean (B.A., J.D., CIM) (Hereinafter designated as "the Applicant" OR "Requestor")

REFERENCE: *Privacy Act Request P-2025-16999 / F339*

SUBJECT: Kind pre-emptive follow up before the Statutory Deadline: April 9, 2026 to assist with our access partnership while I am intermittently away this week - with gratitude

Subject II: all references are in relation to 2024 (year of)

ATTENTION: ACCESS TO INFORMATION AND PRIVACY BRANCH

Good Day to you Ms. Simpson:

I hope you are well and enjoying the long weekend. Thank you for the indulgence as per he above.

It is respectfully submitted that the present correspondence is deposited with the Access to Information and Privacy Branch of the Royal Canadian Mounted Police for the express purpose of providing a critical jurisprudential update respecting the underlying factual matrix of the extant access requisition. Furthermore, the objective herein is to effectuate a structural amelioration of the administrative processing burden incumbent upon the recipient institution as the absolute statutory deadline approaches. This instrument simultaneously operates as formal legal notice delineating the severe constitutional and jurisdictional breaches underpinning the matter at bar, thereby demonstrating with forensic certitude the legal rationale as to why the requested federal metadata is strictly precluded from lawful withholding under any discretionary statutory exemption.

Pursuant to the formal retraction executed by the institutional representative, Melissa Simpson, regarding the preliminary assertion of "unreasonable interference," it is duly noted that the statutory processing timeline remains strictly and unalterably governed by the confirmed delivery date of March 10, 2026. The *Privacy Act* imposes a rigid thirty-day compliance epoch. Excluding the date of receipt, the calculus dictates exactly twenty-two days remaining in the month of March (inclusive of the eleventh through the thirty-first), augmented by nine days in the month of April. This computation establishes the absolute, non-derogable thirty-day statutory terminal date for institutional compliance as the conclusion of the business day on **April 9, 2026**. Any subsequent delay or omission shall be unequivocally construed as a "deemed refusal" pursuant to the applicable legislative framework.

I. Structural Accommodation, Forensic Non-Repudiation, and the Extraction of Hexadecimal Data

Regarding the specific requisition for hexadecimal dumps and the extensive, highly specialized forensic analyses undertaken in relation thereto, a structured, phased methodology is hereby proffered to accommodate the operational exigencies and prioritization matrices of the recipient institution. It is acknowledged that the extraction of uninterpreted binary and hexadecimal data necessitates specific, complex mainframe interrogations.

Provided that the specific, human-readable systemic data charted in Section V of this document is produced by the strict **April 9, 2026** deadline, a temporary abeyance shall be granted until the conclusion of that same calendar week for the production of the raw hexadecimal dumps. This administrative accommodation is explicitly predicated upon the provision of unequivocal, written confirmation by the April 9th deadline as to whether the information currently residing within the mainframe has been subjected to any amendment, modification, clearance, or purgation subsequent to the date of the original entries.

To elucidate the fundamental necessity of this data: hexadecimal dumps represent the unfiltered, machine-level binary code of the database architecture. Unlike standard user-interface printouts, which are inherently subject to software-level filtering or discretionary redaction by terminal operators, hexadecimal logs contain immutable systemic non-repudiation artifacts. Such artifacts provide mathematical certainty regarding terminal keystrokes, temporal timestamps, and systemic overrides, thereby entirely bypassing human interpretation and potential institutional obfuscation. In documented instances of suspected manipulation by state actors, this raw data functions as the sole legally unassailable evidentiary record of the original systemic input.

II. The Factual Matrix, the Integrated Court Offences Network (ICON) Chronology, and Extra-Statutory Property Seizure

It is posited, seemingly without debate—a position practically conceded by the prosecutorial reliance upon blanket privilege in lieu of factual rebuttal—that the documentation received within the initial "false information package" was categorically fabricated. Whether initially conceptualized as a clerical anomaly or a technological failure, the evidentiary record now strongly indicates calculated, deliberate manipulation by state actors. The municipal record is objectively inaccurate *per se*, and the provincial administrative apparatus appears to be actively shielding said inaccuracies from judicial scrutiny.

The chronological impossibility inherent in the municipal record further substantiates the assertion of fabrication. Based upon empirical data subsequently procured from

various provincial courthouses utilizing the Integrated Court Offences Network (ICON) system, the arrest warrant in question was inexplicably expunged from the provincial system on or around October 3, 2024. However, the physical apprehension of the Applicant, executed ostensibly pursuant to the warrant in the first instance, occurred the day prior, on October 2, 2024.

For the purpose of facilitating the database query, the arresting officer was initially presented to the Applicant merely as "Detective Abdul." Through independent verification methodologies, the true identity of the officer was ascertained to be Detective Abdulhameed K. Virani of the Toronto Police Service (TPS), 52nd Division. Anomalously, the arrest and subsequent processing protocols were executed out of the 14th Division, demonstrating an inter-divisional obfuscation tactic frequently utilized to fragment the documentary trail of irregular judicial authorizations. Detective Virani was the individual officer who ultimately authorized the release on October 2, 2024. Consequently, logic and systemic protocols dictate that the initial CPIC input of the arrest warrant must have definitively occurred prior to that release date, likely during the mid-to-late September epoch.

Furthermore, it is confirmed that the scope of the extant access requisition explicitly encompasses the potential existence of authorizations extending beyond a singular arrest warrant. Given the temporal anomalies and the surrounding circumstances of the investigation, a significantly high probability exists regarding ancillary, covert judicial authorizations (e.g., search warrants, general warrants, digital device searches and seizures, wiretaps, tracking warrants, and section 487.02 assistance orders).

This assertion is corroborated by the fact that the Toronto Police Service obtained and retained specific personal chattels appertaining to the Applicant. Receipt thereof was claimed without the provision of a single statutory particular—lacking any disclosure regarding the methodology of acquirement, the temporal point of acquisition, the identity of the individual from whom the chattels were seized, or the legal mode of acquisition. Adding an element of coercion to this extra-statutory seizure, a threat was issued stipulating that if the un-inventoried chattels were not claimed within exactly seven days of October 2, 2024, they would be permanently forfeited and remitted to the TPS Property and Evidence Management Unit (PEMU) for destruction or auction. The imposition of such forfeiture absent due process, and entirely devoid of the statutory underpinning normally provided by a lawful Return to a Justice (Form 5.2), constitutes an arbitrary deprivation of property. (Reference is made to Appendix #1 below regarding the explicit methodology by which CPIC processes and logs these specific investigative order types within the purview of Personal Information Bank RCMP PPU 005).

To the extent that multiple judicial officers were involved in these fractured authorizations, the unredacted names, geographic courthouse locations, and jurisdictional levels of all involved judicial officers are strictly required. Additionally, extensive legal research into the *Criminal Proceedings Rules for the Superior Court of Justice (Ontario)* confirms that no statutory or procedural mandate exists requiring the Superior Court of Justice (SCJ) to electronically record an intake court proceeding, unless said proceeding is explicitly combined with, or constitutes a part of, an application under section 487.1 of the *Criminal Code* (Telewarrants). The total absence of standard intake records further indicates an irregular, *in camera* Superior Court authorization operating under the guise of a routine provincial warrant.

III. Jurisdictional Nullity, *Coram Non JUDGE*, and Liability for State-Actor Detainment

The jurisprudential gravity of this metadata requisition is of paramount institutional concern. The processing thereof does not constitute a routine administrative criminal history check; rather, it represents the extraction of the sole uncorrupted evidentiary ledger pertaining to a catastrophic constitutional irregularity. Comprehensive legal analysis indicates that the physical municipal record relied upon by the municipal police force contains a profound procedural anomaly that fatally severs the jurisdictional authority of the Crown.

The integrity of the Canadian criminal justice system relies absolutely, without exception, on the unbroken chain of custody of sworn and signed documents (whether physical, electronic, or digital). It demands strict, unforgiving adherence to the statutory forms (such as Form 2 Informations) governing the deprivation of liberty. When these foundational pillars are bypassed—whether through severe administrative incompetence or deliberate, orchestrated obfuscation motivated by pre-existing institutional conflicts of interest—the resulting legal actions are not merely voidable

errors. They are not curable administrative defects capable of being ameliorated by the forgiving provisions of Section 599 of the *Criminal Code*.

Rather, such actions constitute a fundamental collapse of the rule of law. Because the proceeding was founded upon fabricated, unsworn authority—specifically, a digitally manipulated Family Court endorsement processed through a third-party enterprise developer Application Programming Interface (API) rather than a properly sworn Information before a Justice of the Peace—the entire proceeding is a jurisdictional nullity. In precise legal terminology, the matter is *coram non judice* (not before a judge) and void *ab initio* (invalid from the point of inception).

To contextualize the unprecedented egregiousness of this state action, comparative reference must be made to the jurisprudence established in *R. v. Silva*. In the documented history of Canadian law, there exists only one prominent instance wherein a police officer physically misappropriated a Justice of the Peace stamp to forge a warrant (Officer Guillaume Joly-Tessier). In that specific instance, law enforcement personnel were in urgent pursuit of an individual engaged in a murderous rampage. The judiciary nonetheless severely condemned the illegality, even whilst acknowledging the extreme, life-or-death exigency of the circumstances.

In stark contrast, the present matter involves the first documented complete digital fabrication of an entire Information Package utilizing enterprise PDF manipulation software (GrapeCity.PDF) to actively scrub the signature of a Chief Justice, executed solely to bypass standard criminal intake procedures. This action was undertaken entirely devoid of the "urgent public safety" exigency observed in *Silva*. It appears to have been driven entirely by institutional self-preservation and profound judicial conflicts of interest.

A bureaucratic apparatus deliberately constructed to effectuate the physical movement, arrest, and imprisonment of a citizen through known forged documentation constitutes an unlawful state-actor abduction under the color of authority. As established in the landmark jurisprudence concerning state-actor kidnapping (*R. v. Vu*, 2008-2012), the orchestration of a plot to unlawfully detain an individual carries severe penal consequences, up to and including indeterminate sentencing. In the civil and constitutional paradigm, the deliberate use of forged documentation to initiate an arrest wholly strips law enforcement of their lawful statutory authority and completely pierces the traditional immunities afforded under Section 25 of the *Criminal Code*. This exposure renders the state, the specific officers involved, and the complicit administrative bodies liable for massive punitive and aggravated civil damages pertaining to malicious prosecution, intentional infliction of mental suffering, false imprisonment, and the bad-faith, systemic violation of rights enumerated under Sections 7 and 9 of the *Charter*. The un-manipulated RCMP CPIC metadata remains the singular uncorrupted ledger capable of proving the true origin of this jurisdictional nullity.

IV. The Invocation of the Public Interest Override, Evidentiary Spoliation, and Institutional Threats (Exhibit "F")

Confirmation is hereby formally registered that the provision of the aforementioned information and the demand for extraction are executed not solely upon the unquestionable bedrock of first-party statutory entitlement, but concurrently, and with equal jurisprudential force, upon overarching principles of public interest. To the extent that the institution contemplates the application of discretionary exemptions to shield the identities of the state actors involved, such redactions are preemptively vitiated by the explicit statutory override enshrined within the *Privacy Act*.

Specifically, Section 8(2)(m) of the *Privacy Act* dictates that personal information may be disclosed:

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

The application of this statutory override is inexorably buttressed by paramount Canadian jurisprudence. In *Dagg v. Canada (Minister of Finance)*,

1997

2 SCR 403, the Supreme Court of Canada established that the fundamental objective of access legislation is the facilitation of democracy and the rigorous scrutiny of state action, effectively diminishing the privacy expectations of public officials engaged in the execution of their official duties. Furthermore, *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8, establishes binding precedent specifically precluding the Royal Canadian Mounted Police from weaponizing privacy exemptions to shield internal systemic or operational failings. The strict balancing test articulated in *Bland v. Canada (National Capital Commission)*,

1991

3 FC 325, and the mandate for the reasonable exercise of discretion elucidated in *Rubin v. Canada (Minister of Health)*, 2003 FCA 37, compel the conclusion that the exposure of digital forgery within the court apparatus represents the absolute apex of public interest, thoroughly obliterating any residual privacy interest claimed by the manipulating actors.

The absolute necessity of federal intervention is further compounded by the extracurial intimidation documented within **Exhibit "F"**, appended hereto. Said exhibit provides incontrovertible documentary evidence that the pursuit of redress via traditional provincial judicial avenues precipitated profound threats of further frivolous criminal jeopardy, emanating from the Justice Sector Security Office (JSSO). Such intimidation was deployed as a retaliatory measure whilst lawful rights were being exercised pursuant to the *Administration of Justice Act*, R.S.O. 1990, c. A.6, its attendant regulations, and the *Ministry of the Attorney General Court Services Division Policies and Procedures on Public Access to Court Files, Documents and Exhibits* (the "MAG CSD Guide").

Consequently, as the provincial judicial apparatus has demonstrated a propensity to weaponize security infrastructure to suppress the exposure of jurisdictional nullities, the Royal Canadian Mounted Police is hereby elevated to the position of the ultimate bastion of the public interest. The federal repository stands as the singular, uncorrupted ledger capable of restoring the *status quo ante*.

V. The Chart of Requisitioned Discrete Elements

To ensure the highest degree of efficiency regarding administrative resources, and to entirely obviate the necessity of a protracted formal complaint regarding a "deemed refusal" or an incomplete response, the immediate exaction has been dramatically narrowed.

Provided that the institution furnishes the exact systemic outputs for the following eight (8) discrete metadata fields—extracted directly from the CPIC historical transaction logs for all entries corresponding to the identifiers of the Applicant between September 15, 2024, and October 2, 2024—the core of this immediate requisition will be deemed substantially satisfied.

Item	Required CPIC Metadata Field	Forensic / Systemic Value and Justification
1	Originating Agency (ORI)	Serves to identify the precise police service and specific physical division (e.g., TPS 52 Division vs. 14 Division) that initiated the master CPIC record. This data point bypasses intentional inter-agency obfuscation and pinpoints the operational genesis of the request.
2	Originating Court Level	Systemically confirms whether the CPIC mainframe was commanded to accept a standard Ontario Court of Justice (OCJ) intake warrant, or a highly irregular Superior Court of Justice (SCJ) indictment, endorsement, or direct bench warrant.

3	Originating Courthouse	Identifies the exact judicial building code inputted by the terminal operator. Distinguishing between a local provincial courthouse (e.g., Brampton OCJ) and the Superior Court headquarters (e.g., 361 University Ave or Osgoode Hall) is critical to proving the source of the nullity.
4	Originating Jurisdiction (Geographic)	Verifies the territorial designation mathematically required by the system to authorize the alert, establishing whether the warrant exceeded local geographical boundaries.
5	Terminal ID / Hardware Address	Identifies the precise physical machine utilized to execute the ADD/MODIFY transactions. This conclusively establishes whether the warrant was lawfully entered at a designated courthouse registry by a court clerk, or unlawfully inputted from a police division back-office absent actual judicial transmission.
6	Name of the Judge / Justice(s)	The unredacted, raw textual input of the authorizing judicial officer(s) (even if entered solely by initials, e.g., "GBM" or "SS"). This metric confirms the true identity of the arbiter(s) completely prior to the GrapeCity.PDF digital manipulation and the insertion of a decoy signature.
7	Post-Issuance Modification/Purge Logs	Tracks any ADD, MODIFY, CLEAR, or CANCEL transactions executed after the initial date of the arrest warrant. This logging is strictly necessary to reveal any post-facto attempts by municipal or provincial actors to alter, amend, or digitally scrub the CPIC record subsequent to the realization of the illegality of the arrest on October 2, 2024.
8	Ancillary / Associated Warrants	Identifies any other companion judicial authorizations (e.g., search warrants, general warrants, digital tracking/wiretap warrants, preservation orders) tethered to this specific CPIC profile or ORI during the specified timeframe, thereby exposing the full breadth of the state action.

VI. Conclusion and Parameters for Statutory Compliance

It is respectfully submitted that the extraction of these eight specific, discrete lines of alphanumeric data from a known, easily queried historical transaction log cannot logically, administratively, or legally be construed as an unreasonable interference with the operations of the institution. Furthermore, the extraction of pre-existing metadata fields does not, as a matter of law, constitute the "creation of a new record," which serves as the standard bureaucratic rationale utilized to deny complex access requests.

Again, I would also focus on that any sought personal information records are NOT seeking per se by any castigation of any individual as the Originating Authorizing Agency, Court Level, Court Location et al are not other individuals per se but rather courts. In relation to the name of the authorizing judges, judges are protected by judicial immunity and it is often the case that a judge is only as good as the *Criminal Code* Form 2 Information or *Criminal Code* Form 4 Indictment and submissions made, and since there was no transcript, this is not data or personal information that I will ever obtain. To confirm, my sole focus is the protection of myself in the event that I am oddly approached by police and there are some misgivings about what is in CPIC or was in CPIC. In this regard, it may be presupposed I am being paranoid per se, but I have read cases where even previous warrants, whether removed or not or other notations can lead to an individual being apprehended, followed or surveilled. I am entitled to be left alone or not leave a residence or place with a high degree of personal privacy (reasonable).

Appended hereto is **Appendix #2** (Forensic Digital Manipulation Analysis), provided to supply the recipient office, and specifically the designated legal counsel, with the precise, undeniable technical context of this requisition. It explicitly and mathematically demonstrates the rationale as to why the unadulterated metadata residing securely within the RCMP mainframe serves as the singular remaining mechanism within the Canadian jurisdiction to resolve the severe technological and jurisdictional forgery present in the physical municipal record.

Expectation is hereby formally registered that this specific charting of personal information, alongside the mandatory confirmation regarding any post-entry amendments or purges, shall be delivered on or before the statutory deadline of **April 9, 2026**.

Should the provided disclosure be arbitrarily truncated, heavily redacted under the auspices of "investigative exemptions" (which are rendered moot when the investigation itself constitutes a legal nullity), or deliberately evasive regarding the true identity of the judicial officer(s), it is formally requested that the matter be immediately escalated to a senior supervisor or the appropriate ATIP Manager.

Should such escalation be necessitated by non-compliance, it is required that the exact name and direct contact information of the supervising official be provided in the institutional reply. This protocol ensures that the institutional concealment of a jurisdictional nullity may be addressed in a direct, professional manner prior to the necessity of further formal action. Such action would invariably encompass an immediate, expedited complaint to the Office of the Privacy Commissioner of Canada (OPCC) and the subsequent filing for an emergency writ of *mandamus* before the Federal Court of Canada to legally compel the release of the unadulterated hexadecimal dumps.

VII. Personal Medical Abeyance and Gracious Conclusion

I know you are busy, and I have some medical appointments coming up. I appreciate that this may be a long weekend day for some, so I thought it prudent to get this into your hands now to help with any final checking and cross-referencing against the chart provided. Should you need any of the attachments I have referred to, please let me know and I can provide them upon request. I trust that this formal email, along with my certification that all information is true, accurate, and complete, will suffice.

As I will be intermittently away this weekend due to medical appointments, examinations, and a potential spinal injection (depending on the timing, which I should know by tomorrow or Wednesday), please note that this has been provided to assist our access partnership. I am most grateful for your prompt responses throughout and greatly appreciate the same. Should I not hear from you, I will follow up as soon as possible once my schedule permits.

While this is most comprehensive, I am preaching to the choir so to speak and ensuring while I am away intermittently that I have covered all bases so to speak.

However, as noting the unfortunate incidents that have caused me and continue to cause immense trauma which I continue to seek medical advice, care and treatment for on a psychological level, and while not required to be a ground to obtain my personal information, I thought it was important to inform of the same.

I look forward to having the timely receipt of the personal information requested and being able to confirm a satisfied closure of the file and extend my thanks in advance.

Respectfully Submitted and certified as true, accurate and complete to the best of my knowledge at the time it was made and as if it were under oath or affirmation:

/s/ *Kevin A. McLean*

Mr. Kevin A. McLean (B.A., J.D., CIM)

Email: mcleansettlement@gmail.com

APPENDICES

Appendix #1: CPIC Categorization of Orders and Warrants (PIB RCMP PPU 005)

The Canadian Police Information Centre (CPIC) system accounts for several complex typologies of judicial orders, surveillance flags, and investigative records extending far beyond standard front-line arrest warrants. While the primary "Persons" file is heavily utilized by patrol personnel for wanted persons and active arrest warrants, the underlying system architecture is vastly more comprehensive. It is structurally divided into four primary data banks (Investigative, Identification, Intelligence, and Ancillary) designed to store broader, highly sensitive operational information. It is a critical statutory fact that all of these databanks, without exception, fall squarely under the legislative umbrella of **Personal Information Bank (PIB) RCMP PPU 005 (Operational Case Records)**, which was the explicitly designated target of the initial Privacy Act request.

Typologies of Orders & Warrants Logged within CPIC

- **Judicial Orders:** This classification includes probation orders, parole conditions, peace bonds, and various prohibition orders (e.g., driving or firearms bans), all of which require systemic tracking to ensure municipal and provincial compliance.
- **Civil Warrants:** In specific jurisdictions, civil warrants such as Small Claims Court Warrants, warrants of committal, or family court apprehension orders are entered into the database until execution or mathematical expiration occurs.
- **Investigative & Intelligence Material:** While specific active search warrants and real-time wiretaps are typically managed by the local police service conducting the operation (to maintain strict operational secrecy), the Investigative and Intelligence Data Banks within CPIC contain persistent metadata. These banks store information regarding persons under active surveillance, cross-jurisdictional intelligence flags, and historical data gathered nationally to prevent investigative overlap.
- **Special Interest Police (SIP):** This unique categorization permits agencies to flag individuals of specific interest for various tactical or intelligence rationales, even in the absence of an active, executable warrant for arrest. It functions as a silent, systemic alarm.

Search Warrants, Wiretaps, and Ancillary Orders

Search warrants and wiretaps function distinctly from arrest warrants within the database; however, they leave indelible systemic footprints:

- **Local Management vs. National Footprint:** Active search warrants and wiretap authorizations are generally sequestered within local police databases (e.g., the RCMP's PROS system or equivalent municipal systems) to prevent the compromise of sensitive investigations. Nonetheless, CPIC functions as a high-level coordination utility.
- **The Indelible Role of CPIC:** CPIC is utilized to disseminate the *results* or the *historical metadata* of such orders once they transition into a component of an individual's criminal history, or if the individual is placed under surveillance within the Intelligence Data Bank.

1. The Mechanics of the Intelligence Data Bank

For highly sensitive investigations, CPIC utilizes the Intelligence Data Bank to securely share critical information regarding persons under surveillance across provincial boundaries.

- **Restricted Access:** In contradistinction to the general "Persons" file, intelligence data is strictly compartmentalized. Access is granted solely to agencies possessing a verified "legitimate need to know."
- **Inter-Agency Alerts:** Should a police service conduct a wiretap or specialized physical surveillance, a flag is invariably placed upon the subject within the Intelligence Data Bank. This silently alerts querying officers that an active operational interest exists,

frequently accompanied by a "contact investigator" directive to prevent uniform personnel from inadvertently compromising a covert operation.

2. Section 487 Ancillary Orders

Search warrants are generally managed within local police records systems until the point of execution. However, certain complex investigative orders are tracked nationally to ensure strict compliance:

- **Assistance Orders:** Pursuant to Section 487.02 of the *Criminal Code*, assistance orders (frequently utilized to legally compel third parties, such as telecommunications companies, internet service providers, or financial institutions, to assist with a wiretap or data handover) may be embedded or endorsed alongside primary warrants to ensure enforceability across provincial lines. These mechanisms leave permanent CPIC audit trails.
- **Investigative Flags:** Once a search warrant transitions into an arrest or court action, the status change is immediately reflected in the Investigative Data Bank under status categories such as "accused," "charged," or "court action pending."

3. Specialty Intercept Teams and Preservation Demands

Specialized operational units, such as the Covert Access and Intercept Team (CAIT), manage highly secure, isolated databases for raw wiretap audio content and extracted digital evidence. However, the *authorizations* governing these intercepts must invariably remain tethered to lawful authority.

- **Preservation Demands:** Prior to the drafting or issuance of a formal warrant, investigators frequently deploy preservation demands to ensure volatile digital data (e.g., emails, server logs, or call detail records) is not routinely purged by service providers. While these instruments do not constitute formal "warrants" bearing a judicial signature, they are meticulously recorded in local and federal investigative files to legally bridge the temporal gap until a formal warrant is entered into the judicial process. The extant access requisition explicitly encompasses the metadata of any such preservation demands appertaining to the identifiers of the Applicant.

Appendix #2: Forensic Digital Manipulation Analysis – The "CL (M)" Artifact and the Mechanics of Jurisdictional Nullity

Executive Summary for the RCMP Information & Privacy Branch

This appendix furnishes a condensed, yet technically rigorous, summary of the forensic digital manipulation analysis. It establishes with precision how a legitimate, internal Superior Court of Justice (SCJ) "Intake Court Endorsement" was digitally manipulated and visually disfigured into a fraudulent criminal Information package by state actors. This analysis provides the critical institutional context illuminating why the unadulterated CPIC metadata of the RCMP is strictly required to resolve the extant crisis and restore the *status quo ante*.

I. The GrapeCity.PDF Software Failure and Vector Morphology Collapse

Upon receipt of an emailed, securely signed SCJ PDF containing an internal intake endorsement, the manipulating entity (acting within or directly on behalf of the Toronto Police Service) failed to file the document in accordance with lawful procedure. Instead, a third-party enterprise PDF editing and developer tool was utilized: Grape.City.Documents.PDF-6.0.2.0.

This specific software suite was deployed in a deliberate endeavor to expunge the SCJ branding and fundamentally alter the jurisdictional nature of the document. Specifically, the target of the erasure was the authorizing judicial signature—the traditional, transparent electronic image signature of Chief Justice Geoffrey B. Morawetz. The objective was the illegal conversion of the document into a facially valid Ontario Court of Justice (OCJ) criminal document, enabling front-line law enforcement to execute the warrant absent critical inquiry.

However, the manipulating entity exhibited a failure to comprehend the underlying architectural framework of the PDF format. When GrapeCity was utilized to forcefully delete the transparent signature image overlapping the underlying typed vector text ("Chief Justice G.B. Morawetz"), the flattening engine of the software sustained a critical failure. GrapeCity version 6.0.2 is documented to suffer from the DOC-6507 "whitespace bug." Upon deletion of the image, the engine attempted a recalculation of the surrounding vector space, precipitating a catastrophic vector collapse of the underlying text:

1. **The "J" to "L" Glitch:** The mathematical bounding box corresponding to the capital letter "J" in "Justice" was violently clipped by the deletion algorithm. The software sheared off the leftward, upward hook of the "J". The internal Optical Character Recognition (OCR) engine of the document attempted a reconstruction of the letter, erroneously deduced that the remaining straight vertical stem constituted a capital letter "L", and hard-coded this interpretation into the document structure.
2. **The "G.B." to "()" Glitch:** The internal horizontal crossbars and vertical stems comprising the initials "G" and "B" were mathematically crushed out of existence by the flattening error. The remaining rounded Bezier curves of the letters were incorrectly interpreted by the OCR engine as open and closed parentheses ().

Consequently, the original, legitimate anchor initials "C J G.B. M" (Chief Justice G.B. Morawetz) were morphologically degraded, algorithmically translated, and permanently integrated into the document as the indelible, highly anomalous digital artifact: **C L (M)**.

II. The Digital Signature Ruse and the Decoy "Frankenstein" Document

To camouflage this glaring, unexplainable algorithmic glitch (C L (M) suspended amidst a blank space), the manipulating entities were compelled to deploy a fraudulent visual smokescreen.

A composited "Frankenstein" document was constructed. A massive, visually complex Adobe "digital certificate" box (purporting to belong to a police informant, Court Officer Christyn Frugoni-Rojas) was pasted directly over the C L (M) artifact to obscure the botched erasure. A fabricated, poorly formatted Ontario Court of Justice logo was subsequently inserted at the header, and a decoy Justice of the Peace signature line (George Jiri) was appended at the footer to complete the illusion of a standard provincial warrant.

This methodology constituted a fatal error. The Ministry of the Attorney General (MAG) has since been compelled to explicitly admit on the official record that Justice of the Peace George Jiri absolutely did *not* sign the document in question. The document stands as a complete, verifiable forgery utilized to execute a deprivation of liberty.

III. The Weaponization of Security and the Spoliation Trap

Upon detection of the forgery, attempts were made to retrieve the authentic, original Information Package from the SCJ registries. The state escalated its response dramatically. Rather than producing the requisite file, the Justice Sector Security Office (JSSO) was weaponized. The JSSO issued baseless threats of "legal jeopardy," while simultaneously and maliciously blacklisting the relevant IP address, resulting in a persistent 403 Forbidden Error designed to block access to the Ontario Courts Public Portal. The weaponization of cybersecurity infrastructure to deny access to public court records demonstrates a clear, malicious *mens rea* (criminal intent) to conceal the forgery.

On November 21, 2025, the Deputy Attorney General explicitly confirmed that no Section 74 (*Courts of Justice Act*) destruction orders were ever issued pertaining to these documents. Consequently, by the admission of the Crown itself, the original, un-manipulated SCJ documents legally must remain extant upon their servers.

Advanced legal strategy was subsequently deployed, serving checkmate Draft Orders (Notice of Motions 3, 4, and 5) that trapped the Chief Justice into an impossible paradox: either expose the un-redacted metadata (thereby proving the GrapeCity manipulation) or officially endorse the unlawful state-actor detainment. Facing this inescapable spoliation trap, Chief Justice Morawetz abruptly announced an immediate retirement a mere two business days later.

Because this entire criminal proceeding was founded upon a digitally manipulated Family Court endorsement, processed covertly through an untracked, third-party developer API, and executed utilizing a forged signature, the entire proceeding epitomizes the definition of a jurisdictional nullity (*coram non judice*). It is void *ab initio*. The un-manipulated CPIC metadata held by the RCMP remains the sole, immutable, uncorrupted ledger of this profound judicial failure, and the immediate release thereof is paramount to the administration of justice within Canada.

Appendix #3: Exhibit "F" - Evidence of Extracurial Intimidation

Appended hereto is Exhibit "F", consisting of documentary records substantiating the extracurial intimidation exercised by the Justice Sector Security Office (JSSO). Said records confirm the retaliatory issuance of threats alleging criminal jeopardy in direct response to the lawful exercise of statutory rights pursuant to the *Administration of Justice Act*, R.S.O. 1990, c. A.6, and the *Ministry of the Attorney General Court Services Division Policies and Procedures on Public Access to Court Files, Documents and Exhibits*.

On Wed, Mar 25, 2026 at 1:47 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear Ms. Simpson,

Thanks so much! I really appreciate your quick and courteous help—your team's professionalism is top-notch compared to some other institutions I've made requests of who shall remain nameless.

I certainly respect the workload that you and your team have, and I want to be mindful of our communication. To the extent that I am away for medical reasons, appointments, or examinations, I will put my auto-reply on so you know I will review everything upon my return.

My best to you and your team!

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Wed, Mar 25, 2026 at 1:18 PM ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca> wrote:

Good day,

Thank you for your email. We are currently processing your request and will make every effort to provide it as soon as possible. Please note we legislatively have 30 days to provide a response and have chosen to take an additional extension 30 days due to operational requirements. We cannot provide you a time line as to when it will be sent as

Tab U

there are other files in the queue that may have an impact on when your request is finalized.

Regards,

Ms. Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'aviser immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

From: Mr. Kevin McLean <mcleansettlement@gmail.com>
Sent: March 25, 2026 10:03 AM
To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>
Subject: Re: Privacy Act request P-2025-16999 / F339, Your File N/A, Acknowledgment

DELIVERY METHOD: Via Electronic Transmission

TO: Melissa S., Access to Information and Privacy Branch, Royal Canadian Mounted Police
REFERENCE: Privacy Act request P-2025-16999 / F339 (the "Request")
SUBJECT: Formal Clarification, Requisition of Interim Personal Information (ORI; Issuing Court Level; Issuing Location; Name of Judge; Dates et al), and Invalidation of Purported Statutory Extension

Good Morning to you Melissa S.

I hope you are well. As I have some upcoming medical examinations and injections for some serious impairments I suffered as a result of motor vehicle accident a few years back and I will be away intermittently over the next several weeks, I am kindly following up on the provision of the interim personal information as you had noted. Would you kindly provide me with above interim information as it is currently in the CPIC database? If there is any utility to your suggestion about contacting municipal or perhaps a provincial police force, then we can accordingly be efficient with resources while respecting yours. The remainder is more formal in nature to ensure my record keeping is in order and we are not at cross-purposes. Thank you and my best to you!

I. Rectification of Statutory Timelines for Notice Purposes

1. Correspondence is heretofore advanced in direct, comprehensive response to the communications promulgated by the Access to Information and Privacy Branch of the Royal Canadian Mounted Police (the "Institution") and the fact that you did reference providing interim information. In limine, for strict administrative notice purposes, a profound rectification of the temporal timeline is unequivocally necessitated, as the physical receipt of

the foundational requisition was incontrovertibly effectuated via Canada Post delivery on March 10, 2026, thereby establishing the irrevocable commencement date for the statutorily mandated computation of time. Furthermore, I further confirm that as I have not received any reasons as to why and what parts of the request (if any) would cause your Institution in meeting the original time limit would unreasonably interfere with the operation of the government institution, I have done so out of an abundance of caution to ensure that we are operating within the parameters of the Privacy Act..

II. Exaction of Interim Personal Information

2. As you did represent that you may be in a position to provide interim information and noting the landmark nature of today's date and to proactively facilitate a highly efficient allocation of overarching administrative resources, an expeditious interim disclosure of highly specific, localized personal information is forcefully demanded. It is formally requisitioned that the Institution provision, the following discrete algorithmic and historical artifacts pertaining exclusively to the applicant: the originating agency identifier (the "Originating Agency Identifier"), the issuing court level (the "Issuing Court Level"), the issuing courthouse location (the "Issuing Courthouse Location"), the name of justice (the "Name Of Justice"), and the date of authorization (the "Date Of Authorization"). The accelerated extraction and subsequent production of these fundamental data elements shall serve to mitigate overarching operational burdens and fundamentally prevent the piecemeal adjudication of the present matter.

III. The Effluxion of Time and Extinguishment of Privilege

3. It is categorically posited, although the personal information requested would not fall under the same, that any theoretical institutional reliance upon discretionary law enforcement exemptions to withhold this requisite interim personal information is entirely legally bankrupt. Specifically, an excess of eighteen months has incontrovertibly elapsed since the purported swearing of the underlying form 2 criminal code information (the "Form 2 Criminal Code Information"). Consequently, the effluxion of this extensive temporal duration absolutely obliterates any conceivable grounds for asserting ongoing investigative privilege or operational sensitivity, rendering the continued suppression of this metadata a profound administrative overreach and an indisputable nullity ab initio. As such, and out of an abundance of caution, any potential concerns are firmly now extinguished (see: the Information Package attached again).

III. Conclusion and Formal Demand

5. Consequently, the prompt, unredacted disclosure of the specifically enumerated interim personal information is unconditionally required to ensure strict compliance with the highest traditions of Canadian administrative law and the governing statutory timeline. The provisioning of these discrete digital acta is explicitly engineered to ensure that any prospective administrative actions are meticulously optimized, momentarily bridging the profound asymmetry of information existing between the coercive apparatus of the state and the private citizenry. Appended hereto is the comprehensive correspondence anthology to ensure absolute record integrity as this foundational requisition proceeds toward an ultimate, timely resolution.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Tue, Mar 17, 2026 at 2:45 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear Melissa S.,

On an administrative note, I received an auto-reply yesterday, and each of your emails is appearing in a separate thread on my end. To maintain a complete and accurate institutional record, I have attached the following:

1. The hard-copy registered-mail Privacy Act request (February 27, 2026);
2. Our first email exchange this week, with attachments; and
3. Our second email exchange this week.

It is unclear why a new thread is generated each time, but I have taken the time to consolidate the materials to ensure record integrity.

Given the documented irregularities—including the filing of corrupted documents in a non-originating courthouse and at an incorrect judicial level—I would be grateful if you could provide the four discrete personal-information elements previously identified:

- **Originating Agency Identifier (ORI)**
- **Issuing Authority / Court Field**
- **Narrative / Remarks Field**
- **System Identification Number**

These four elements are essential to clarify the discrepancies between the corrupted documents and any authentic CPIC entries. I remain most grateful in advance for your assistance.

Thank you.

Mr. Kevin A. McLean (B.A., J.D., CIM)

On Tue, Mar 17, 2026 at 2:20 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Subject: Re: ATIP File – Confirmation of your purported reliance on a Section 15(a)(i) Extension under the Privacy Act – absent any sufficient particulars as to why the original time limit would unreasonably interfere with the operation of your government institution

Dear Ms. Melissa S.:

Thank you for your correspondence.

With great respect, I do not presently understand the basis upon which a 30-day extension under section 15(a)(i) of the *Privacy Act* is required in relation to my request. As confirmed in both my initial submission and my follow-up yesterday, the request concerns **only my own personal information** (Mr. Kevin A. McLean). No third-party information is sought, and no consultations with other institutions are required.

Section 15(a)(i) permits an extension only where meeting the original 30-day statutory deadline would **“unreasonably interfere with the operations of the government institution.”** Because this is the sole ground invoked, I am requesting clarification of the factual basis for concluding that this high statutory threshold is met.

Legal Standard Under Section 15(a)(i)

The “unreasonable interference” standard is a stringent one. The Office of the Privacy Commissioner has repeatedly held that:

- The institution must provide **specific, request-related facts** demonstrating that the 30-day deadline would cause a genuine and unreasonable operational burden.
- General workload, staffing pressures, or routine administrative demands **do not satisfy** section 15(a)(i).
- The institution must show that the particular request is unusually large, complex, or resource-intensive in a way that would materially

disrupt operations.

- Extensions cannot be invoked as a matter of convenience or institutional practice.

Gregory v. Canada (Public Safety and Emergency Preparedness), 2020 FC 667

The Federal Court in *Gregory* provided a detailed interpretation of the statutory test. The Court held that:

- Section 15(a)(i) sets out a **two-pronged framework**, and the “unreasonable interference” branch is a **high bar**.
- Institutions cannot rely on this provision simply because they are busy or because a request requires effort.
- The institution must demonstrate that the specific request imposes an **extraordinary burden** on operational capacity.
- The extension mechanism is not intended to accommodate ordinary workload fluctuations or administrative inconvenience.

This jurisprudence confirms that the threshold you are relying upon is a very high one, and based on the information provided so far, it does not appear to be met.

Request for Clarification

Given the above, I respectfully request clarification of the following:

1. What specific operational interference is anticipated if the request were processed within the original 30-day period?
2. What concrete, request-specific factors justify the conclusion that the statutory threshold of “unreasonable interference” is met?
3. Why the retrieval and processing of my personal information cannot be completed within the original statutory timeframe?
4. How this request—limited solely to my personal information—could reasonably be said to impose an extraordinary burden on the RCMP’s operational capacity, particularly given the size, resources, and technical infrastructure of the RCMP and CPIC program?

Path Forward

Respectfully, there are two possible outcomes (subject to my proposal below):

1. The RCMP proceeds on the original statutory timeline and provides the responsive personal information on or before the original due date; or
2. You provide sufficient, request-specific reasons demonstrating how this particular request imposes an extraordinary operational burden within the meaning of section 15(a)(i), supported by the standard articulated in *Gregory* and OPC jurisprudence.

If no such reasons are provided, I will rely on the original 30-day timeline, calculated from the date the mailed request was delivered to the address indicated.

Interim Disclosure to Facilitate Resolution

In the interim, and in the spirit of cooperation, you can readily provide the following **personal information elements** associated with my WANT record, each of which is discrete, easily retrievable, and directly tied to my identity:

Data Element	Operational Function	Relevance
Originating Agency (ORI)	Identifies the police service responsible for the entry.	Establishes the agency holding the master file and the source of any modifications.
Issuing Authority / Court Field	Identifies the judicial body granting the warrant authority.	Confirms the court level and geographic jurisdiction.
Remarks / Narrative Field	Contains operational instructions.	Includes the specific name of the SCJ Judge, OCJ Judge, or JP who signed the warrant.
System Identification Number	Unique CPIC transaction identifier.	Allows tracing of the lifecycle of the record across the network.

Providing these four elements—each of which pertains solely to my personal information—would meaningfully advance the matter and may even narrow or resolve the request entirely. This approach aligns with the principle of **access partnership**, recognized across Canadian jurisdictions, whereby institutions and requesters work collaboratively to expedite access to personal information.

The Supreme Court of Canada and multiple appellate courts have emphasized that access to one’s own personal information is **paramount**, and that the 30-day statutory period is a **hard deadline**, not a flexible guideline. This is particularly true where, as here, the requester has been misled or where the public interest in transparency and accuracy is engaged.

At this stage, you have not provided the required particulars under section 15(a)(i). The test is objective, and the burden rests with the institution to demonstrate an extraordinary operational impact. I remain open to reviewing any such reasons should you provide them.

Thank you for your attention to this matter. I look forward to the provision of that personal information and that may resolve much of what was requested and at the very least allows us to consent to a time extension for any further providing personal information so we can work together in the access partnership.

Sincerely,
Kevin A. McLean

On Tue, Mar 17, 2026 at 1:10 PM ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca> wrote:

Dear Kevin McLean,

This is to acknowledge receipt of your request under the Privacy Act, which was received by this office on March 12, 2026, for:

It is formally demanded that the Institution immediately conduct a comprehensive offline search (the "Offline Search") of the highly secure Offline Historical Database to retrieve all artifacts associated with the PIB RCMP PPU 005 repository (Operational Case Records).

This explicit demand for exaction encompasses the following specific forensic artifacts, which are indispensable for the forensic reconstruction of the record:

- a. The retrieval of all active, cleared, canceled, or purged WANT Records associated with Kevin A. McLean spanning the entirety of the year 2024, including historical status codes (the "Historical Status Codes").***
- b. The unredacted production of all system Transaction Logs, audit trails, and hexadecimal dumps (the "Hexadecimal Dumps") governing the entire lifecycle of the warrant entry, including all ADD, MODIFY, CLEAR, and CANCEL Transactions, and any supervisor override actions recorded within the federal mainframe.***
- c. The explicit disclosure of the associated timestamps (accurate to the millisecond), the ORIs, the unique user IDs of terminal operators, the precise terminal hardware addresses, and the entirety of the narrative and remarks fields (the "Narrative Fields") for each sequential transaction, demonstrating the evolutionary history of the data entry and any unauthorized "metamorphosis."***

Please note that we can only disclose information related to yourself. If the records contain personal information of other individuals, their full name, date of birth, a copy of a valid government issued photo ID and written consent is required in order to release their personal information to you. You may send this via regular mail or e-mail to the contact listed below. Please be advised that currently we are proceeding with your request and we may release limited information.

The Royal Canadian Mounted Police is committed to assisting you with your request. In order to do so, an extension of 30 days beyond the 30-day statutory time limit is required in accordance with paragraph 15(a)(i) of the Act. The extension is required, as meeting the original time limit would unreasonably interfere with operations. A description of subparagraph 15(a)(i) can be found at: <http://laws-lois.justice.gc.ca/eng/acts/P-21>.

Please be advised that you are entitled to lodge a complaint with the Privacy Commissioner concerning the processing of your request. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Privacy Commissioner of Canada
30 Victoria Street, 1st Floor
Gatineau, Quebec K1A 1H3

Additional information on the complaint process can be found at the following link:
<https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa S.
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

195
385

271

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m' aviser immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

5 attachments

image001.png

3K [View Scan and download](#)

image002.png

2K [View Scan and download](#)

 **Gmail - Your property for pick up - Anthony Romano email - who did he receive it from -.pdf**
259K [View as HTML Scan and download](#)

 **Who are the Toronto police officers accused of assisting organized crime_ Here's what we know so far _ CBC News - Sgt Robert Black 14 Division.pdf**
2370K [View as HTML Scan and download](#)

 **Merged - RCMP Milton Detachment - Michael Peggs - Head of Regional Detachment.pdf**
1881K [View as HTML Scan and download](#)

TAB 11

Tab A



Royal Canadian Gendarmerie royale
Mounted Police du Canada

Your file Votre référence
N/A

Our file Notre référence
P-2025-16999

April 27, 2026

Kevin McLean
68 Abell Street
Toronto, Ontario M6J 0B1

Dear Kevin McLean:

This is in response to your request under the *Privacy Act*, which was received by this office on March 12, 2026. Please refer to page 3 of this response letter for a copy of your original request text.

Based on the information provided, a search for records was conducted in Canadian Police Information Centre and Specialized Policing Services. Enclosed is a copy of all the information to which you are entitled. Please note that some of the information has been exempted pursuant to sections 19(1)(d), 22(1)(b) and 26 of the Act. More information on the exemptions applied can be found in the Treasury Board of Canada Secretariat publication ***Privacy Act: Plain Language Guide to Exemptions and Exclusions*** at the following address:
<https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/plain-language-guide.html>

The *Privacy Act* has established the right of applicants to access federally maintained records. If this matter concerned another police department, they may have information of interest to you. The *Privacy Act* does not authorize the RCMP to search files or to disclose information belonging to other police forces, you may wish to submit a Freedom of Information and Protection of Privacy Act request to:

Toronto Police Service
Access & Privacy Section, 4th Floor
40 College Street
Toronto, ON M5G 2J3
Website: <https://www.tps.ca/services/freedom-information-request/>

Please be advised that you are entitled to lodge a complaint with the Privacy Commissioner concerning the processing of your request. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

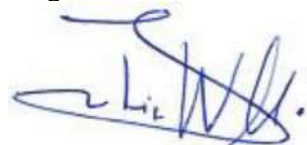
Office of the Privacy Commissioner of Canada
30 Victoria Street, 1st Floor
Gatineau, Quebec K1A 1H3

Additional information on the complaint process can be found at the following link:
<https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/>

In accordance with subsection 12(2) of the *Act*, you are entitled to request correction of your personal information. To do so, complete the form found at: <https://www.canada.ca/en/treasury-board-secretariat/corporate/forms/350-11.html>, and send it to the Access to Information and Privacy office at the address below.

Should you wish to discuss this matter further, you may contact Kristen Wardrop at kristen.wardrop@rcmp-grc.gc.ca. Please quote our file number appearing on this letter.

Regards,



Julie Worrell
For/
Jeff Ball
Director, Privacy
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

Original Request Text

It is formally demanded that the Institution immediately conduct a comprehensive offline search (the "Offline Search") of the highly secure Offline Historical Database to retrieve all artifacts associated with the PIB RCMP PPU 005 repository (Operational Case Records).

This explicit demand for exaction encompasses the following specific forensic artifacts, which are indispensable for the forensic reconstruction of the record:

- a. The retrieval of all active, cleared, canceled, or purged WANT Records associated with Kevin A. McLean spanning the entirety of the year 2024, including historical status codes (the "Historical Status Codes").
- b. The unredacted production of all system Transaction Logs, audit trails, and hexadecimal dumps (the "Hexadecimal Dumps") governing the entire lifecycle of the warrant entry, including all ADD, MODIFY, CLEAR, and CANCEL Transactions, and any supervisor override actions recorded within the federal mainframe.
- c. The explicit disclosure of the associated timestamps (accurate to the millisecond), the ORIs, the unique user IDs of terminal operators, the precise terminal hardware addresses, and the entirety of the narrative and remarks fields (the "Narrative Fields") for each sequential transaction, demonstrating the evolutionary history of the data entry and any unauthorized "metamorphosis."

Revised Request Text

1. Scope of the Request

I confirm that the text of my February 27, 2026 request accurately reflects the information I am seeking.

For clarity, the request concerns **my own personal information** contained within the **CPIC Investigative Data Bank**, governed by **Personal Information Bank RCMP PPU 005**, including:

- WANT records (active, cleared, cancelled, or purged)
- ADD, MODIFY, CLEAR, and CANCEL transactions
- All associated timestamps
- Originating Agency Identifiers (ORIs)
- Terminal identifiers
- User IDs of terminal operators
- Narrative and remarks fields

This request is strictly limited to my personal information under s. 3 of the Privacy Act.

2. Whether the Records Are Held by the RCMP

I confirm that the records sought are held within the **control of the RCMP**, specifically within the CPIC system and its Offline Historical Database.

The attached findings of the Office of the Privacy Commissioner of Canada (OPC) confirm that:

“As the steward of CPIC...the RCMP bears responsibility for ensuring that all information shared...is done in accordance with the requirements of the MOC and in compliance with the Act.”

The CPIC Audit Report (2011) likewise confirms that the RCMP:

- Hosts the CPIC system
- Maintains its audit trails
- Oversees compliance
- Performs offline searches

Accordingly, the records fall within the RCMP’s custody and control for the purposes of s. 12(1) of the Privacy Act.

3. Location of the Records

I respectfully clarify that the records requested are not located at a specific detachment. CPIC is a **centralized national system**, and the Offline Historical Database is accessible only to the RCMP.

Given the uncertainty surrounding the accuracy of municipal records—and the possibility that the originating police service may not be limited to the Toronto Police Service (TPS)—the only reliable and authoritative source of the relevant metadata is the **central CPIC system**.

For ease of reference, I provide all known particulars below.

4. Time Frame and Underlying Particulars

The relevant time frame is defined by the occurrence numbers, the commencement of proceedings, and the arrest date. All known particulars are provided below.

A. First Occurrence Number (TPS)

- **Event / Occurrence Number:** 2024-2028093
- **Date:** September 15, 2024
- **Case Manager:** PC Eric Tang #10942
- **Email:** 10942@tps.ca

B. Second Occurrence Number (TPS)

392**Event / Occurrence Number:** 24-2082035

- **Date:** September 22, 2024
- **Case Manager:** D/Cst. Michael Kolankowski #82239
- **Email:** 82239@tps.ca

C. TPS Case Identification Number (MOST LIKELY THE COURT FILE NUMBER WITH THE SCJ 361 UNIVERSITY AVENUE, 1ST FLOOR)

- **TPS Case ID:** 457197
- Appears on the Intake Court Endorsement
- Does **not** appear on the Form 10 Release Order

D. Commencement of Proceedings (date information is sworn and laid)

- **Date:** September 15 or September 23, 2024

E. Informant / Court Officer

- **Name:** Court Officer Christyn Frugoni-Rojas (née Christin Boulton)
- **Role:** Special Constable / Court Officer
- **Information Number (Form 2):** 4810 998 24 48129169

F. Intake Court Endorsement

- **Date:** September 23, 2024
- **Digital signature:** JP George Jiri
- **Note:** The endorsement contains no physical signature, location, or date stamp from the Brampton courthouse.
- **Presumed originating courthouse:**
 - **Ontario Superior Court of Justice – South Toronto Criminal Division**
 - 361 University Avenue, Toronto

G. Arrest Information

- **Arrest Date:** October 2, 2024
- **Arrest Location:** TPS 14 Division (350 Dovercourt Road, Toronto)
- **Arresting Officers:**
 - Cst. Anthony Romano #6097
 - D/Cst. Michael Roman Kolankowski #82239
 - Sergeant Sean Cassidy
- **Detective attending cells:**
 - Detective Abdulhameed K. Virani (TPS 52 Division)
- **Form 10 Release Order:**
 - Signed by Sgt. Cassidy and myself
 - Contained the TPS Occurrence Number (allegedly from September 22, 2024)
 - Did **not** contain the TPS Case ID Number

H. Additional Context Regarding Date Ranges

For ease of reference, I include the following correspondence from the Superior Court of Justice Records Management Office:

Email from SCJ RMO (Ms. Sana Azim) to ACT (Ms. Janet McLean)

Date: August 20, 2025

ACT ID: 3831309629

393

office is unable to process orders with date ranges.

Please list the exact dates your Ordering Party wishes to order and re-submit an updated order form.”

This illustrates why precise dates are provided above.

5. Summary of Relevant Time Frame

Based on the above, the relevant period for the CPIC Offline Search is:

- **September 15, 2024 → October 2, 2024**, inclusive
- Plus any subsequent CLEAR, CANCEL, or MODIFY transactions associated with the same entries (and thereafter)

Because CPIC records contain their own timestamps, I respectfully request that the RCMP retrieve **all records associated with my identifiers**, including any system-generated timestamps outside these dates that relate to the same entries.

Tab B

395

DATE: 2026/04/14-07:35:43:042 (-18000000) (3600000)

ON01103 MO E
Q PERS+ REM:000330500 P-2025-16999
NBOISVERT/QREASON:ADM/SNME:MCLEAN/G1:KEVIN/G2:ALEXANDER/SEX:M/DOB:19830325/ASSOC
:3/SECONDARY:Y/QPW:Y/QL:Y/CNI:Y

QUERY POSSIBLE HITS FOR PERSON
SNME: MCLEAN G1: KEVIN G2: ALEXANDER
SEX: MALE DOB: 1983-03-25
REM: 000330500 P-2025-16999 NBOISVERT
INCLUDE OTHER PROVINCIAL RECORDS

QUERY PERSON SEX: MALE

MAXIMUM POSSIBLE SCORE 24

QUERY PERSON LOG SEX: MALE

NOT ON FILE PERSON LOG
2026041407354220260414073542

DATE: 2026/04/14-07:35:43:445 (-18000000) (3600000)

397 03 MO E

REM:000330500 P-2025-16999

NBOISVERT/QREASON:ADM/SNME:MCLEAN/G1:KEVIN/G2:ALEXANDER/DOB:19830325/SEX:M

RESPONDENTS 4 FOR:

MCLEAN KEVIN ALEXANDER

SEX: M DOB: 19830325

>>>QUERY REMARKS: 000330500 P-2025-16999 NBOISVERT

QUERY VALUE 23

RESPONDENT SCORE: 23

FPS: 445771G

<<<<'CR' QUERY RECOMMENDED>>>>

FILE OPEN

CRIMINAL RECORD IN ENGLISH ONLY

MALE, WHITE, BORN 1983-03-25, BC, AGE-NOW 43

EYES BROWN, WAS 175 CM (5FT 09IN) 091 KG (200LBS) IN 2018-04

MARKS 211-SYMBOL 722-CHINESE SYMBOL

** CAUTION: THIS IS NOT A CRIMINAL RECORD **

FILE OPENED 2018-04-17 LAST ENTRY 2019-01 OF:-

** NO CONVICTIONS **

KNOWN-AS:.... 01....MCLEAN;KEVIN ALEXANDER

Tab 12

Your property for pick up

3 messages

Anthony Romano <Anthony.Romano@tps.ca>
To: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Wed, Oct 2, 2024 at 7:46 PM

Hello Kevin,

Please be advised that we have received some of your property which will be held here at 14 Division for you to retrieve. We have received your passport, birth certificate, name change certificate, medication and a watch. Your property will be held here for the next 7 days and if not picked up by then, it will be sent to our property bureau.

When you attend 14 Division, let the front desk officers know you have property in temporary lockers under your name and they will retrieve it for you.

Regards,

**Anthony Romano****Constable #6097**

Toronto Police Service

14 Division, D Platoon

416-808-1400

anthony.romano@tps.ca

This e-mail (including any attachments) may contain PRIVILEGED and CONFIDENTIAL INFORMATION only for use of the Addressee(s). If you are not the intended recipient of this e-mail or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any dissemination or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify me by telephone or e-mail to arrange for the return or destruction of this document. Thank you.



image001.jpg
10K

Mr. Kevin McLean <mcleansettlement@gmail.com>
To: Anthony Romano <Anthony.Romano@tps.ca>

Wed, Oct 2, 2024 at 7:57 PM

Good Evening Mr. Romano: thank you so much for your email. I confirm its receipt.

I did not ask for it to be delivered there and I am sorry you are saddled with the same. We have an emergency hearing coming up at the LTB as per the order of Adjudicator Delorenzi which is attached so it is unclear why, I presume, the Landlord delivered it there.. I absolutely need my medication so I will be there tonight. I have to walk so I anticipate about 30 minutes or so.

I will bring my identification. Thanks kindly.

Warm regards,

Mr. Kevin A. McLean (B.A. (MCL), J.D., CIM)

[Quoted text hidden]

LTB-T-063554-24_McLean tenant_expedited granted.pdf
86K

Mr. Kevin McLean <mcleansettlement@gmail.com>
To: Anthony Romano <Anthony.Romano@tps.ca>, 14division@torontopolice.on.ca, 7956@tps.ca, 82239@tps.ca

Thu, Oct 3, 2024 at 1:17 PM

October 3, 2024

VIA EMAIL

VIA PDF EMAIL

For the purposes herein

Toronto Police Service

Attention: 14th Division (see: 14division@torontopolice.on.ca)

Attention: Mr. Romano (see: Anthony.Romano@tps.ca), Sergeant Cassidy (7956@tps.ca) and DC Kolankowski (82239@tps.ca).

Re: some corrections to the address provided in Form 10

Re #2: my declaration #19 in the LTB Proceeding which provides all of my correspondence with Ms. Nicole Artopoulos since September 15, 2024, - all related to the pickup of her remaining items at the Minto Buildings – left on Sunday and picked up that day – without issue – updates regarding the Unlawful Lockout by the Landlord and so on -

Re #3: confirmation that I have never spoken or met DC Kolankowski until yesterday

Re #4: residual – if charges have not been approved yet – kindly provide the name of the Crown so I (and my counsel) can clear up the confusion

Dear Sirs/Mesdames:

1. I write regarding the above.
2. I have had occasion to speak with various counsel and I am seeing another this afternoon. Without any waiver of privilege or confidentiality, kindly respond under this thread (where applicable).
3. My name is below and my identification is attached along with my current address. In compliance with the Form 10, I was required to inform you if anything was incorrect. I am still reviewing but the address is incorrect. I am informed by the criminal defence counsel that “NFA” means ‘no fixed abode’. This is incorrect. My fixed abode is on my driver’s license. Kindly correct the inaccuracies and send me a revised Form 10 via email herein. If you need my signature on the revised one, I can sign and scan by sending it back to you. Thank you kindly in this regard.
4. I have been the sole tenant since Nicole vacated on June 23, 2024. As per the *Residential Tenancies Act* (Ontario), once Nicole vacated and I did not leave within 60 days, if I was not a tenant at law (which I was as I had paid rent for over five years to Ms. Aphy Artopoulo(s)), then I became a tenant and the sole tenant. I attach a copy of my declaration #19 in that LTB Proceeding. As per the order of LTB Member Delorenzi, which came as a shock to me as well, which was on October 1, 2024, and both myself and the Landlord (Aphy) were notified of the same.
5. It is not your typical order (if you will) of shortening of time because it also finds me to be a tenant and notes the circumstances (based on volumes of evidence and submissions). They are rare at the LTB but they are also unreviewable as per section 209 and 210 of the RTA. I heard someone say last night that it is just in the nature of a quicker hearing. It is absolutely not that they are very difficult to obtain and they look at all of the evidence to determine the same. Moreover, the granting of my relief relates to an urgent motion that puts me back in Unit 410 and requires unequivocal conduct by the Landlord in accordance with the law. One can understand why the Landlord was upset and the timing of the same.
6. In turn this means, I will be successful with my interim motion to take repossession of Unit 410. It is only a matter of time. I have also updated the RHEU in this regard and that is also now moving again in the correct and lawful direction. The above is for your kind edification in relation to the LTB proceeding.
7. As per the advice of two criminal defence counsel and one civil counsel, all unanimously, my declaring of an affidavit (or declaration) is public record and it is under the penalty of perjury. Therefore, you will see attached that a mistake has been made and I kindly ask you to reconsider this charge absent particulars of dates therein. All of the communications to Nicole (which I had not communicated with her since on or around August 2024 while I resided in Unit 410 by myself) were for: (i) picking up of her stuff which I kindly left in our former parking spot; (ii) advising her of the status of what the Landlord did and thankfully all of her belongings were picked up (unlike my situation); (iii) confirming the steps I was taking in the LTB proceeding; (iv) inquiring if she had a

replacement key; and (v) then seeking her position about me being “Nicole’s guest” when I was the primary payor (if not sole payor); and others.

8. I have also had the law reviewed in harassment (criminally) and you would get that kind of comment from other civil litigators at times that one is engaging in “harassment” if they are somehow being repetitive in a point. It is obviously context specific.

9. In the context of a section 264(2)(b) which states, “**264 (1)** No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection (2) that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them. **Prohibited conduct** (b) repeatedly communicating with, either directly or indirectly, the other person or anyone known to them”, I was required and compelled, by legal duty and by request of the RHEU in certain parts, to follow up with demands upon the Landlord, and the Nicole (by way of her vacating as a tenant) and provide evidence of the same. I have done so.

10. All of the conduct that I have taken therein is lawful as it is in relation to the LTB proceeding or an offshoot of the same. It is also in the spirit of courtesy in providing Nicole with her remaining items for pick up.

11. I can also confirm that at no time did I receive any correspondence from anyone that any communications were unwelcome and even if the Tribunal found my communications to be worthy of a unique order.

12. I appreciate you are all doing your job to the best and top of your profession but respectfully, there is no way that I was not engaging in conduct that was lawful. Secondly, I could not have known that any person was harassed and certainly if they were, they could notify the LTB as that is the context that it was happening in. Nothing has been brought forth.

13. I certainly appreciate that it not enjoyable for anyone to be going through this and it has not been for me (i.e. coming back to being locked out when it was not authorized) but in order to obtain the assistance from the RHEU, I had to show steps I had taken to notify all including a technical legal position that I had discovered.

14. Even Constable Solermo of your 14th Division said to me, “This is a tenancy matter. They are hard fought but it is not for us.” We were pleasant and disagreed on a few points but nonetheless, you will see the only emails that have been sent by me that are all in relation to Nicole receiving the return of all of her property unlike my ability to not have access to all of my property that is in Unit 410 (but I confirm receipt of some yesterday).

15. I will await the amendments to the Form 10 and whether the charges have been approved or not. If they have, kindly provide me with the name of Crown Counsel so I can pass on that name so I can see which criminal defence counsel to pick based on the same.

16. Of course, I will continue to honour all of the terms and conditions, as it relates to Nicole as I don’t know where she will be and I am not searching for her. I do not know where she is working these days and I do not care to. I also do not know where she is living and I do not care to. The sole purpose of my emails, of which the Landlord was copied on, was to protect and preserve my legal position due to an unlawful changing of the locks and deactivation of my FOB on Friday, September 20, 2024. I came to your detachment the next day.

17. As you will see from my sworn declaration, those emails are my only communications with Nicole since August. We had not communicated in any other way.

18. From a factual perspective, you will see that I discharged my requirements in notifying the relevant persons of those facts. With Nicole, it was also Victory Wine because when I, on Sunday, September 15, 2024, moved some of the remaining items out, some were that of a company and not her. I have taken active steps to ensure that her email is removed from my email so there is no inadvertent risk either.

19. I can unequivocally confirm that DC Kolankowski #82239, when he was on my right and DC Romano was on my left, said that he had spoken with me and warned me as well. With great respect to DC Kolankowski, he must have mistaken someone else. I have not emailed him at all. My first email ever with TPS was with Constable Romano.

20. I can also tell you that it could not have been via phone because of my lack of having the same and also I do not even use text or traditional phone calling as my number is connected to the likes of Viber but you have to be another Viber customer to call. It is safer and encrypted.

21. I think we can all appreciate how difficult this has been on me but also that I had a duty to advance and protect my positions, and the LTB has agreed with me and not the Landlord. However, I can assure you that those communications were required by law to notify those of a new technical legal position and the whereabouts of their property.

22. I will be gone for the balance of the day today and part of tomorrow so I will await those amendments to the Form 10. I have attached a copy of the declaration #19 so you can see for yourself. I have no record of any individual or even the Tribunal for that matter informing me that anything is even improper in the Tribunal context. Lastly, I have attached a copy of the order of the **LTB Member Delorenzi** who refers to my circumstances which were caused by the Landlord and her unlawful conduct.

23. I kindly let you know that if you have different documents than these, then you have some impersonating me and that seems to be the case considering DC Kolankowski thought he had warned me. I am unsure if this was via phone or in person but nonetheless, I am making clear that it never happened.

24. Lastly, I wish for this to be a process where I can reach out and seek your advice and guidance on certain points as well but I can assure that my residential address is what is contained in my driver's license. Because I have been unlawfully locked out by the Landlord does not mean that is not my fixed address. Moreover, this will inevitably long tribunal litigation between the Landlord and I even after the interim orders in my favour. Therefore, I will keep in mind your sage comments and do my best to be professional but as you can see, I write (or dictate part) with a professional tone. That being said, I will never communicate with Nicole ever again by this order and undertaking, and by volition.

25. I was advised by criminal defence counsel that if you do have emails that are impersonating me, please provide the same to me.

26. Thank you kindly for your professionalism last night and how we ended things which was obviously a shock for me considering I was coming in good faith to pick up my property which was being held unlawfully. Lastly, I was advised to advise you that your division is not a place for my property to be dropped off. Therefore, if anyone ever tries to again, please refuse delivery. Thank you all. I await to hear from you the relevant persons on the above and the necessary corrections made. Have a wonderful day and thanks for the work you do generally and specifically!

Warm regards,

Mr. Kevin A. McLean (B.A. (MCL), J.D., CIM)

[Quoted text hidden]

4 attachments

 **LTB-T-063554-24_McLean tenant_expedited granted.pdf**
86K

 **Scan_Undertaking_Promise to Appear.pdf**
160K

 **Tenant_Declaration_19_in support of emergency motion_illegal lockout_ongoing_Oct 3.pdf**
1350K

 **Mr. Kevin A. McLean G Drivers License_2024.pdf**
1344K

TAB 13

292

215406

IN THE MATTER OF a Formal Public Complaint pursuant to Part VII of the *Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10 and attendant regulations

IN THE MATTER OF *Public Complaints and Review Commission Act* (S.C. 2024, c. 25) (if applicable and/or temporarily applicable at the relevant time)

AND IN THE MATTER OF the *Interpretation Act*, R.S.C., 1985, c. I-21;

AND IN THE MATTER OF Actionable Neglect of Duty, Administrative Malfeasance, the Deliberate Spoliation of Digital Evidence, and the Systemic, Institutionalized Suppression of Publicly Accessible Judicial Records by the Royal Canadian Mounted Police Central Region Command.

DATE: May 11, 2026

TO:

The Civilian Review and Complaints Commission for the RCMP (the “CRCC”, “Commission” or “CRCC (RCMP)”)

☐ Civilian Review and Complaints Commission (CRCC)
National Intake Office
P.O. Box 1722, Station B
Ottawa, ON K1P 0B3
☐ **Fax:** 613-952-8045

ATTENTION: The Honourable Brent Cotter, Interim Chairperson
ATTENTION: Roxanne Gagné, Vice-Chairperson

SUBJECT OF COMPLAINT:

Assistant Commissioner Mr. Matthew Peggs (the “**Regional Commander**”)

Central Region in Ontario of Royal Canadian Mounted Police
Milton Detachment (with jurisdiction over Toronto West, Toronto South and Toronto East)
2755 Highpoint Drive,
Milton, Ontario
L9T 5E8

Other Particulars:

FROM:

Mr. Kevin A. McLean, B.A., J.D., CIM (the “**Complainant**”)
Email: mcleansettlement@gmail.com

Facsimile: 416.981.7117

Telephone: 647.370.9354

TO:	1
SUBJECT OF COMPLAINT:	1
FROM:	1
FORMAL COMPLAINT AND DEMAND FOR PUBLIC INTEREST INVESTIGATION	6
Summary (Brief)	6
I refer to myself in the third person and by way of definition of “Complainant”	6
This Complaint is submitted in support of a formal complaint regarding the systemic administrative silence and statutory defaults of the RCMP Central Region Command	6
The Complainant seeks the immediate restoration of personal property held in excess of 18 months without judicial authorization and the production of publicly accessible criminal court records pursuant to the <i>Ministry of the Attorney General (MAG) Court Services Division Court Information Access Guide (2019)</i>	6
The Regional Commander has consistently ignored urgent administrative demands, representing a “calculated weaponization of silence” that violates the absolute legislative bedrock provided by Section 37 of the <i>Royal Canadian Mounted Police Act</i>	6
THE FACTS	6
Police Case ID 457197: The RCMP Milton Detachment is the originating agency for a seizure of property from Unit 410-775 King Street West, Toronto, occurring subsequent to September 20, 2024, along with a variety of alleged but meritless offences and certainly un-proceeded upon for self-evident reasons	6
Unauthorized Detention: As of May 11, 2026, the property has been detained for approximately 20 months. No Superior Court order extending detention beyond the one-year limit (Section 490(3) <i>Criminal Code</i>) has been produced despite formal requests	6
Records Default: The Regional Command has failed to provide authentic source documents (Form 2 Information and endorsements) to replace a “False Information Package” containing structural digital artifacts (the “C L (M)” artifact) along with the requisite intake court endorsement(s) and/or warrants, authorizations and orders	6
Administrative Silence: Four successive urgent communications sent between May 6 and May 11, 2026, including a final notice of default at 1:00 PM EDT on May 11, have met with total non-responsiveness	6
ISSUES	6
Does the persistent administrative silence of the Regional Commander constitute a breach of the statutory responsibilities codified in Section 37 of the <i>RCMP Act</i> ?	6
Does the withholding of post-arrest judicial records violate the Open Court Principle and the mandates of the <i>MAG CSD Records Guide (2019)</i> along with the obligations of the Regional COM in Mr. Matt Peggs	6
LAW AND ARGUMENT	6
Section 37 is not an aspirational code; it is a rigid structural framework. The Supreme Court of Canada in <i>R. v. Campbell</i> [1999] 1 S.C.R. 565 established that all members must act strictly “in accordance with the law.”	6
The Regional Commander has failed to:	6
• Respect the rights of all persons (s. 37(a)): By maintaining unauthorized possession of privileged legal materials and sentimental property	6
• Perform duties promptly and diligently (s. 37(c)): By failing to respond to urgent inquiries regarding the legality of property detention	6
• Maintain the integrity of the administration of justice (s. 37(b)): By allowing the continued use of “Acta Falsa” (spurious records) containing known vector morphology crashes	6

217	Pursuant to the <i>MAG CSD Court Information Access Guide</i> , the investigating police service is the primary custodian of worn Information post-arrest.	7
408	The withholding of these records is an extra-statutory act that prevents the Complainant from verifying the legal basis of his deprivation of liberty and property.	7
	Jurisprudence in <i>Frémy v. Canada</i> , 2022 FC 750 confirms that Section 37 is the proper lens through which to evaluate the “unreasonableness” of administrative silence.	7
	The Regional Commander’s “stonewalling” is an active decision. In the absence of a denial, the Commission must draw an adverse inference that the RCMP lacks valid judicial authorization for the continued detention of the property.	7
	RELIEF SOUGHT	7
	The Complainant respectfully requests that the Commission:	7
	- Formally find the Regional Commander in breach of his Section 37 duties; - Compel the immediate production of the authentic source records for and/or relating to Police Case ID 457197; and 7 - Mandate the immediate logistical arrangement for the restoration and pickup of the Applicant’s property whether from the seizure from his apartment and/or through third parties (non law enforcement) who were engaged in unlawful conduct over and above the aforementioned	7
	Enhanced Powers under the Public Complaints and REVIEW Commission Act.....	7
	1. Absolute Entitlement to Information (Section 16)	7
	2. Access to Privileged Information (Section 17)	7
	3. Superior Court Powers for Witnesses and Evidence (Section 50)	8
	4. Review of Systemic “Specified Activities” (Section 28)	8
	5. Mandatory Codified Timelines (Section 25/Regulations).....	8
	6. Independence from the RCMP Act	8
	1.0 PREAMBLE, ENUMERATION OF REVIEWED DOCUMENTATION, AND THE INVOCATION OF INDEPENDENT CIVILIAN OVERSIGHT	9
	2.0 STATUTORY DEFINITIONS AND INTERPRETATIVE FRAMEWORK: ROYAL CANADIAN MOUNTED POLICE ACT	11
	Nota Bene - The Rebuttal of Definitional Irrelevance and Semantic Deflection:	12
	Nota Bene - Non-Obvious Legal Theory: The Doctrine of Statutory Evolution as Evidence of Mandatory Accountability:	12
	3.0 FACTUAL MATRIX: THE UNLAWFUL EXPROPRIATION, VITIATED CHAIN OF CUSTODY, AND THE INSTITUTIONAL LAUNDERING OF EVIDENCE	12
	4.0 JURISPRUDENCE: SECTION 37 OF THE ROYAL CANADIAN MOUNTED POLICE ACT	14
	R. v. Campbell, 1999 1 S.C.R. 565 (the “Campbell Decision”)	15
	Bigeagle v. Canada, 2023 FCA 128 (the “Bigeagle Decision”) and Jones v. Canada, 2018 NBCA 86 (the “Jones Decision”)	16
	Frémy v. Canada, 2022 FC 750 and Herrera-Morales v. Canada, 2016 FC 578.....	17
	5.0 STATUTORY CONTRAVENTIONS, CHARTER INFRINGEMENTS, AND THE DOCTRINE OF ABSOLUTE NULLITY	17
	6.0 THE SYSTEMIC SUPPRESSION OF PUBLICLY ACCESSIBLE JUDICIAL RECORDS, DIGITAL SPOILIATION, AND FORENSIC ANOMALIES.....	19

2.18 FORENSIC DECONSTRUCTION OF THE ACTA FALSA: ALGORITHMIC SPOILIATION AND THE “CLARIFICATION” ARTIFACT	20
Nota Bene - The Rebuttal of the “Clerical Error” Defense:.....	21
8.0 STRUCTURAL DEVIATIONS FROM THE STATUTORY PRO-FORMA: A COMPARATIVE ANALYSIS OF THE FRAUDULENT INFORMATION PACKAGE	21
Nota Bene - The Rebuttal of “Substantial Compliance”:.....	22
9.0 THE ADVENT OF CORAM NON JUDICE AND THE TRANSFORMATION OF LAW ENFORCEMENT INTO PRIVATE TORTFEASORS	22
Nota Bene - The Rebuttal of “Good Faith Execution”.....	23
10.0 EXPANDED NON-OBVIOUS LEGAL THEORIES: MALICIOUS PROSECUTION AND SYSTEMIC CHARTER VIOLATIONS (SECTIONS 7, 8, AND 9)	23
Nota Bene - The Rebuttal of Prosecutorial and Police Immunity:.....	24
11.0 STATUTORY NON-COMPLIANCE: COMMISSIONER'S STANDING ORDERS (CONDUCT), SOR/2014-291	24
12.0 THE MISAPPLICATION AND WEAPONIZATION OF THE OATH OF SECRECY, SOR/2014-280.....	25
Nota Bene - The Rebuttal of Blanket Secrecy:	25
13.0 FITNESS FOR DUTY AND THE COMMISSIONER'S STANDING ORDERS (EMPLOYMENT REQUIREMENTS), SOR/2014-292	25
14.0 SECTION 12 OF THE RCMP ACT SUSPENSION	26
Nota Bene - The Rebuttal of Premature Disciplinary Action:	26
Dawe v. Canada, 2002 FCT 486	28
Grant v. Canada (Attorney General) (T.D.), 1994 CanLII 9274 (FC) and 1994 CanLII 3507 (FC).....	28
15.0 ANTICIPATORY SPOILIATION AND THE RCMP EXTERNAL REVIEW COMMITTEE RULES OF PRACTICE AND PROCEDURE, SOR/88-313	29
Nota Bene - The Rebuttal of Limited Committee Scope:	29
16.0 FRUSTRATION OF LEGISLATIVE INTENT AND DEFIANCE OF THE ENHANCING ROYAL CANADIAN MOUNTED POLICE ACCOUNTABILITY ACT, S.C. 2013, C. 18	29
Nota Bene - The Rebuttal of “Control or Possession” Ambiguity	30
17.0 ANTICIPATORY REBUTTALS AND THE LOGICAL HARMONIZATION OF JURISDICTIONAL REALITIES.....	30
Nota Bene - The Anticipatory Rebuttal of Custodial Deflection	30
Nota Bene - The Rebuttal of Jurisdictional Separation:.....	30
Nota Bene - The Rebuttal of Willful Blindness:	31
18.0 SERIOUS INCIDENTS: NOTIFICATIONS, INVESTIGATIVE ARRANGEMENTS, OBSERVERS, AND REPORTING (SECTIONS 45.79–45.87).....	31
Regulations Prescribing Physical Injuries (SOR/2019-260).....	32
Application of the Law to the Facts: The Psychological Injury as “Cruel and Unusual Treatment”.....	32
19.0 IMPERATIVE DIRECTIVES, LEGAL CONSEQUENCES, AND FINAL DEMANDS OF THE COMMISSION	33
Appendices	35

SUMMARY (BRIEF)

I refer to myself in the third person and by way of definition of “Complainant”.

This Complaint is submitted in support of a formal complaint regarding the systemic administrative silence and statutory defaults of the RCMP Central Region Command.

The Complainant seeks the immediate restoration of personal property held in excess of 18 months without judicial authorization and the production of publicly accessible criminal court records pursuant to the *Ministry of the Attorney General (MAG) Court Services Division Court Information Access Guide (2019)*.

The Regional Commander has consistently ignored urgent administrative demands, representing a “calculated weaponization of silence” that violates the absolute legislative bedrock provided by Section 37 of the *Royal Canadian Mounted Police Act*.

THE FACTS

Police Case ID 457197: The RCMP Milton Detachment is the originating agency for a seizure of property from Unit 410-775 King Street West, Toronto, occurring subsequent to September 20, 2024, along with a variety of alleged but meritless offences and certainly un-proceeded upon for self-evident reasons.

Unauthorized Detention: As of May 11, 2026, the property has been detained for approximately 20 months. No Superior Court order extending detention beyond the one-year limit (Section 490(3) *Criminal Code*) has been produced despite formal requests.

Records Default: The Regional Command has failed to provide authentic source documents (Form 2 Information and endorsements) to replace a “False Information Package” containing structural digital artifacts (the “C L (M)” artifact) along with the requisite intake court endorsement(s) and/or warrants, authorizations and orders.

Administrative Silence: Four successive urgent communications sent between May 6 and May 11, 2026, including a final notice of default at 1:00 PM EDT on May 11, have met with total non-responsiveness.

ISSUES

Does the persistent administrative silence of the Regional Commander constitute a breach of the statutory responsibilities codified in Section 37 of the *RCMP Act*?

Does the withholding of post-arrest judicial records violate the Open Court Principle and the mandates of the *MAG CSD Records Guide (2019)* along with the obligations of the Regional COM in Mr. Matt Peggs

LAW AND ARGUMENT***The Mandatory Nature of Section 37 of the RCMP Act***

Section 37 is not an aspirational code; it is a rigid structural framework. The Supreme Court of Canada in *R. v. Campbell* [1999] 1 S.C.R. 565 established that all members must act strictly “in accordance with the law.”

The Regional Commander has failed to:

- **Respect the rights of all persons (s. 37(a)):** By maintaining unauthorized possession of privileged legal materials and sentimental property.
- **Perform duties promptly and diligently (s. 37(c)):** By failing to respond to urgent inquiries regarding the legality of property detention.
- **Maintain the integrity of the administration of justice (s. 37(b)):** By allowing the continued use of “Acta Falsa” (spurious records) containing known vector morphology crashes.

Pursuant to the *MAG CSD Court Information Access Guide*, the investigating police service is the primary custodian of sworn Information post-arrest.

The withholding of these records is an extra-statutory act that prevents the Complainant from verifying the legal basis of his deprivation of liberty and property.

Adverse Inferences from Administrative Non-Responsiveness

Jurisprudence in *Frémy v. Canada*, 2022 FC 750 confirms that Section 37 is the proper lens through which to evaluate the “unreasonableness” of administrative silence.

The Regional Commander’s “stonewalling” is an active decision. In the absence of a denial, the Commission must draw an adverse inference that the RCMP lacks valid judicial authorization for the continued detention of the property.

RELIEF SOUGHT

The Complainant respectfully requests that the Commission:

- Formally find the Regional Commander in breach of his Section 37 duties;
- Compel the immediate production of the authentic source records for and/or relating to Police Case ID 457197; and
- Mandate the immediate logistical arrangement for the restoration and pickup of the Applicant’s property whether from the seizure from his apartment and/or through third parties (non law enforcement) who were engaged in unlawful conduct over and above the aforementioned

ENHANCED POWERS UNDER THE PUBLIC COMPLAINTS AND REVIEW COMMISSION ACT

The transition from the CRCC to the **Public Complaints and Review Commission (PCRC)** under the *Public Complaints and Review Commission Act* (S.C. 2024, c. 25) provides several “super-powers” relevant to Case ID 457197.

1. Absolute Entitlement to Information (Section 16)

Unlike the legacy framework where disclosure was often subject to a Memorandum of Understanding (MOU), **Section 16(1)** of the PCRC Act establishes that the Commission is *entitled* to have access to any information under the control or possession of the RCMP that it considers relevant.

- **Application:** This overrides the Regional Commander's “administrative silence.” If the Commission deems your property records or the “CL (M)” metadata relevant, the RCMP has a statutory obligation to provide it.

2. Access to Privileged Information (Section 17)

Section 17(2) is a groundbreaking provision. It explicitly states that despite any privilege (including **solicitor-client privilege** or litigation privilege) that may be claimed, the Commission is entitled to access that information if it is “relevant and necessary” to the matter before it.

- **Application:** The RCMP cannot shield the internal “manipulators' script” or legal advice regarding the seizure of your Computer/J.D. work product behind a wall of privilege during a PCRC investigation.

Section 50(1) grants the Commission the same powers as a **superior court of record** to:

- Summon and enforce the attendance of witnesses (including senior officers like Assistant Commissioner Peggs);
- Compel oral or written evidence on oath;
- **Compel the production of documents and things** (the actual digital source files for the *Acta Falsa*).

4. Review of Systemic “Specified Activities” (Section 28)

Section 28(1) allows the Commission to conduct a review of “specified activities” of the RCMP.

- **Application:** You can request that your individual complaint be part of a broader “Specified Activity Review” into the Central Region's digital document generation and property retention protocols post-2024.

5. Mandatory Codified Timelines (Section 25/Regulations)

The Act was designed to prevent “stonewalling” by codifying timelines for the RCMP to respond to Commission reports and requests for information.

- **Application:** This directly counters the “calculated weaponization of silence” you identified. The RCMP no longer has the luxury of indefinite delays; the Act and its attendant regulations (currently being operationalized in 2026) impose hard deadlines on the Commissioner to respond to the PCRC.

6. Independence from the RCMP Act

Because the PCRC is established under its own **standalone statute** (rather than being a Part within the *RCMP Act*), its independence is structurally reinforced. It has its own budget and is no longer administratively tethered to the Force it oversees.

1.0 PREAMBLE, ENUMERATION OF REVIEWED DOCUMENTATION, AND THE INVOCATION OF INDEPENDENT CIVILIAN OVERSIGHT

1. It is formally submitted, and concurrently entered into the immutable administrative record, that this correspondence operates unapologetically as a formalized public complaint and a definitive, unequivocal notice of impending administrative escalation. This action is predicated entirely upon the persistent, undocumented, and legally indefensible administrative silence emanating directly from the highest echelons of the office of the Regional Commander. The Civilian Review and Complaints Commission for the RCMP (CRCC) is a fiercely independent agency, structurally, administratively, and operationally severed from the RCMP apparatus. Created by the Parliament of Canada in 1988, and profoundly fortified by the sweeping legislative reforms of the *Enhancing Royal Canadian Mounted Police Accountability Act*, S.C. 2013, c. 18, the Commission is statutorily mandated to ensure that public complaints made about the conduct of RCMP members are examined fairly, rigorously, and completely impartially. The Commission receives complaints from the public and conducts exhaustive, probing, and highly specialized reviews when complainants are systematically disenfranchised, procedurally obstructed, or left wholly unsatisfied with the RCMP's internal handling of their grievances. As the Complainant is definitively and profoundly unsatisfied with the tacit endorsement of subordinate malfeasance by the Regional Commander—manifested through a highly calculated, institutionalized policy of absolute administrative silence—the overarching investigative jurisdiction of the CRCC is hereby forcefully, immediately, and irrevocably engaged.
2. The Complainant intentionally and strategically submits this comprehensive complaint under the principled, highly specialized oversight of Interim Chairperson The Honourable Brent Cotter and Vice-Chairperson Roxanne Gagné. The extensive, highly esteemed pedigree of The Honourable Brent Cotter in civilian oversight—which prominently includes the presidency of the Canadian Association of Civilian Oversight of Law Enforcement (CACOLE), foundational, pioneering academic and practical work in Canadian legal ethics, and a distinguished, transformative tenure as Deputy Minister of Justice for Saskatchewan—uniquely positions him to recognize the insidious, corrosive nature of systemic police obfuscation and the bureaucratic evasion of constitutional duties. Similarly, the distinguished tenure of Vice-Chairperson Roxanne Gagné as Civilian Director of Manitoba's Independent Investigation Unit, coupled with extensive, twenty-five-year experience as a Crown prosecutor navigating the complex, often treacherous intersections of federal and provincial law, has established rigorous national precedents for overseeing complex investigations into severe police misconduct, particularly where criminal and administrative law collide. It is thoroughly anticipated that the combined, unparalleled expertise in legal ethics, civilian oversight, and prosecutorial integrity of the Commission will ensure a rigorous, uncompromising, and deeply analytical examination of the severe constitutional and statutory infringements exhaustively detailed herein. The Commission is uniquely equipped, comprehensively empowered, and indeed statutorily obligated by Parliament, to pierce the veil of the “blue wall of silence” that currently characterizes the defensive and legally hostile operational posture of the Central Region Command.
3. Within the sophisticated, highly codified, and heavily scrutinized realm of administrative law, such sustained and deliberate silence from the Regional Commander—manifesting persistently and unapologetically in the face of unambiguous, formally served, and legally unassailable demands—transcends the boundaries of mere bureaucratic oversight, logistical backlog, or innocent negligent delay. Rather, it constitutes a constructive, deliberate, and highly actionable refusal to exercise unequivocally mandated statutory duties. Administrative silence, when intentionally wielded by a formidable organ of the state possessing vast coercive powers, ceases to be a mere absence of action; it becomes a positive, aggressive instrument of oppression. It is an administrative weapon specifically designed to maliciously starve the citizen of procedural fairness, deny them fundamental justice, and exhaust their limited resources through carefully engineered attrition.
4. Pursuant to the fundamental and unyielding principles of statutory construction explicitly codified within section 11 of the *Interpretation Act*, R.S.C., 1985, c. I-21, the deployment of the word “shall” within statutory mandates

224 415 301 denotes an absolute, non-discretionary, and binding imperative upon the state actor. Ergo, the law categorically and unconditionally precludes the exercise of administrative silence where an active, affirmative, and timely duty to respond is legislatively prescribed. Furthermore, drawing upon the powerful jurisprudential mandate of section 10 of the *Interpretation Act*, the law is considered to be “always speaking,” meaning that the ongoing, continuous, and protracted failure of the Regional Commander to proactively address this profound constitutional infringement constitutes an ever-present, compounding, and daily dereliction of the solemn responsibilities mandated by the *Royal Canadian Mounted Police Act*, R.S.C., 1985, c. R-10. This calculated abdication of command responsibility intrinsically violates the core tenets of the doctrine of procedural fairness, simultaneously eviscerating the legitimate, constitutionally protected expectations of the Complainant regarding transparent, accountable, and lawful federal policing. By weaponizing silence, the Regional Command actively seeks to exhaust the Complainant through deliberate procedural attrition, severe financial drain, and profound psychological fatigue—a highly improper, thoroughly documented administrative tactic that the CRCC was explicitly designed by the Parliament of Canada to aggressively dismantle and ruthlessly penalize.

5. This instrument is meticulously formulated, structurally engineered, and formally served following a comprehensive review, rigorous forensic analysis, and systematic incorporation of the following documentation, records, and evidentiary materials (collectively designated as the “**Evidentiary Record**”):

Electronic and facsimile transmissions directed specifically to the attention of the Regional Commander dated May 6, 2026, May 7, 2026, and May 8, 2026, which unequivocally establish an unbroken chronological timeline of the exhaustive administrative efforts of the Complainant to achieve a localized resolution, and the subsequent, deliberate, and sustained failure of the RCMP to respond (the “**Antecedent Communications**”);

Written correspondence originating from Constable Anthony Romano of the Toronto Police Service (the “**TPS**”) 14th Division, bearing the date of October 2, 2024, which serves as the undeniable, catalytic, documentary admission of initial municipal involvement and the subsequent extra-jurisdictional transfer of the chattels;

A synthesized, highly authoritative research dossier detailing the administrative accountability frameworks governing the RCMP, encompassing the complex legislative transition from the legacy oversight mechanism of the CRCC to the newly instantiated, progressively fortified Public Complaints and Review Commission (the “**PCRC**”) pursuant to the *Public Complaints and Review Commission Act*, S.C. 2024, c. 25, which fundamentally elevates the strict statutory requirements for operational transparency, external scrutiny, and uncompromising senior-command accountability

d. The *Interpretation Act*, R.S.C., 1985, c. I-21, and the *Royal Canadian Mounted Police Act*, R.S.C., 1985, c. R-10, encompassing the explicit statutory obligations, unyielding fiduciary duties, and corresponding severe penal consequences fundamentally binding upon all federal law enforcement personnel;

The Ministry of the Attorney General Court Services Division *Court Information Access Guide* (2019), which unequivocally and clearly delineates the unassailable, constitutionally protected public entitlement to pristine, unredacted court records;

The manipulated judicial authorization package colloquially designated, and empirically forensically established, as the False Information Package (the “**Acta Falsa**”);

Internal organizational publications, official press releases, and strategic operational documents originating from both the TPS and the RCMP confirming the existence, deep operational integration, and strategic mandates of robust Joint-Forces Operations (the “**JFOs**”). These highly integrated and lavishly funded frameworks include, but are not limited to, the Integrated National Security Enforcement Team (the “**INSET**”), the Counter-Terrorism Security Unit (the “**CTSU**”) prominently launched in March 2026, and the Combined Forces Special Enforcement Unit (the “**CFSEU**”);

The *Commissioner's Standing Orders (Conduct)*, SOR/2014-291;

The *Regulations Prescribing an Oath of Secrecy*, SOR/2014-280;

The *Commissioner's Standing Orders (Employment Requirements)*, SOR/2014-292;

The RCMP External Review Committee Rules of Practice and Procedure, SOR/88-313;
The Enhancing Royal Canadian Mounted Police Accountability Act, S.C. 2013, c. 18;
Comprehensive jurisprudential summaries specifically concerning the absolute, non-delegable statutory duties imposed under section 37 and the formidable suspension powers delineated under section 12 of the *Royal Canadian Mounted Police Act*;
detailed forensic analysis documents relating to “CL (M) - Forensic Manipulation.docx”, evidencing the advanced digital spoliation and algorithmic software alteration of an ostensible Superior Court of Justice document;
The document strictly identified as “Information Package 4810 998 24 48129169-00 (4).pdf,” constituting the falsified, structurally compromised, and manipulated criminal record;
The document identified as “ADULT-COMMON-INFORMATION-FORM-WITH-HIGHLIGHTED-CHANGES - LINCOLN COUNTY LAW ASSOCIATION.pdf,” utilized herein as the unassailable statutory pro-forma baseline for establishing Form 2 requirements.

2.0 STATUTORY DEFINITIONS AND INTERPRETATIVE FRAMEWORK: ROYAL CANADIAN MOUNTED POLICE ACT

6. To ensure absolute precision, to foster semantic clarity, and to unequivocally preclude any subsequent administrative obfuscation or jurisdictional sleight-of-hand regarding terminology by the RCMP Legal Services Directorate, the following definitions, as strictly and explicitly codified within section 2(1) of the *Royal Canadian Mounted Police Act*, R.S.C., 1985, c. R-10, are expressly integrated into the foundational framework of this complaint:
- a. appropriate officer:
Repealed, 2013, c. 18, s. ;
 - b. child: means a person who is or, in the absence of any evidence to the contrary, appears to be under the age of eighteen years;
 - c. Code of Conduct: means the regulations made pursuant to section 38;
 - d. Commission: means the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police established by subsection 45.29(1);
 - e. Commission Chairman:
Repealed, 2013, c. 18, s. 2
 - f. Commissioner: means the Commissioner of the Royal Canadian Mounted Police;
 - g. Committee: means the Royal Canadian Mounted Police External Review Committee established by section 25;
 - h. Committee Chairman:
Repealed, 2013, c. 18, s. 2
 - i. conduct authority: in respect of a member, means a person designated under subsection (3) in respect of the member;
 - j. Force: means the Royal Canadian Mounted Police;
 - k. guardian: means, in respect of a child, any person, other than a parent of the child, who is under a legal duty to provide for the child or who has, in law or in fact, the custody or control of the child;
 - l. member: means any person who has been appointed under section 5 or subsection 6(3) or (4) or 7(1) and who is employed with the Force;
 - m. Minister: means the Minister of Public Safety and Emergency Preparedness;
 - n. officer: means a member appointed under section 5 or subsection 6(3) or (4);
 - o. proceedings: in relation to the Commission, means any investigation or hearing conducted by the Commission with respect to a complaint made under Part VII or VII.2; and
 - p. representative: means a person who is representing or assisting a member or a conduct authority under section 47.1.

7. It is a highly foreseeable, strategically obvious logical gap that the RCMP Legal Services Directorate may attempt to trivialize the inclusion of these rigid statutory definitions, arguing in subsequent defensive administrative filings that they are merely prefatory, procedural lexicon that confer no substantive legal rights upon a civilian complainant. This counter-argument must be preemptively and fundamentally dismantled. The explicit legislative transition enacted in 2013 (via the *Enhancing Royal Canadian Mounted Police Accountability Act*, c. 18)—which purposefully and deliberately repealed highly ambiguous titles such as “appropriate officer” and replaced them with the highly specific, rigidly accountable framework of a designated “conduct authority”—demonstrates the unequivocal, unmistakable intent of Parliament to permanently eradicate the opaque, paramilitary command structures that historically shielded senior RCMP management from direct, personal accountability. By strictly defining a “conduct authority” and precisely circumscribing the legal definition of a “member,” the Act entirely eliminates any plausible deniability regarding exactly who bears the ultimate, unyielding responsibility for continuous disciplinary oversight. Applying the venerable legal maxim elucidated by Herbert Broom, *Expressio unius est exclusio alterius* (the explicit mention of one thing is the exclusion of another), the deliberate codification of these specific oversight roles by Parliament functionally and legally excludes the possibility of any RCMP personnel operating outside this chain of strict accountability. It is submitted that Assistant Commissioner Peggs cannot legally or factually feign jurisdictional impotence; as the designated “conduct authority” for the vast Central Region, the statute surgically and inescapably attaches direct liability for subordinate malfeasance, evidentiary spoliation, and profound constitutional breaches directly to his office and to his person.

Nota Bene - Non-Obvious Legal Theory: The Doctrine of Statutory Evolution as Evidence of Mandatory Accountability:

8. A further, highly nuanced, and non-obvious legal theory arises directly from an exhaustive analysis of the specific repeals noted in the definitions above (e.g., the archaic, singular “Commission Chairman” replaced to definitively empower the modernized, collective, and far more powerful “Commission”). The sweeping 2013 amendments did not merely update administrative titles for cosmetic purposes or superficial bureaucratic housekeeping; rather, they fundamentally reconstructed the *mens rea* (intent) of the administrative obligations owed by the RCMP to the Canadian public. The legislative evolution powerfully highlights a radical shift from internal, insular grievance management to externally mandated, fiercely independent, public-facing accountability. By explicitly defining “proceedings” to broadly encompass *any* investigation or hearing under Part VII, the Act inherently categorizes the formal complaint at hand as a protected, formalized statutory mechanism possessing the full, unmitigated weight of federal law. This precise categorization immediately elevates the matter from a mere civilian grievance to a formal, legally protected “proceeding” that must be overseen by a powerful, independent tribunal. Consequently, any attempt by the Regional Commander or subordinate personnel to deliberately spoliage evidence (such as the algorithmic digital alteration of the Acta Falsa) or proactively maintain a posture of absolute administrative silence while attempts are actively made by the Complainant to trigger these formal “proceedings” constitutes a direct, highly actionable interference with a federally defined investigative process. This unequivocally invokes Broom’s maxim *Certum est quod certum reddi potest* (that is certain which can be made certain); the precise statutory definitions render the duties of the Regional Commander absolutely and undeniably certain, legally transforming the continued, calculated silence from mere bureaucratic negligence into intentional statutory defiance, gross insubordination of parliamentary intent, and actionable obstruction of justice.

3.0 FACTUAL MATRIX: THE UNLAWFUL EXPROPRIATION, VITIATED CHAIN OF CUSTODY, AND THE INSTITUTIONAL LAUNDERING OF EVIDENCE

9. The foundational, incontrovertible, and deeply disturbing operational basis of this complaint is anchored irrevocably in the profoundly unlawful expropriation of private, personal property rightfully and exclusively belonging to the lawful owner. This initial tortious deprivation, characterized legally as a severe trespass to chattels and an act of outright, unmitigated conversion, occurred at the residential premises geographically situated at Unit

227 410-775 King Street West, Toronto, Ontario, manifesting chronologically subsequent to September 20, 2024. The deprivation of these specific, highly sensitive items did not merely represent a fleeting, inconvenient loss of easily replaceable physical goods; it constituted a profound operational, professional, financial, and severe psychological disruption of the highest possible magnitude. It effectively and maliciously severed the rightful owner from their primary digital identity, critical financial instruments, unrecoverable proprietary intellectual property, and deeply private, constitutionally protected medical autonomy.

10. It is categorically asserted, and unequivocally supported by the unassailable Evidentiary Record, that an individual identified as Mr. David Karat (the “**Perpetrator**”) executed an unauthorized, clandestine, and heavily premeditated removal of a receptacle, specifically a functional backpack (the “**Receptacle**”), belonging exclusively and undisputedly to the rightful owner. The Receptacle operated as a central, highly critical repository for highly sensitive, legally privileged, and operationally necessary items, specifically enumerating but not limited to: (i) a portable computing device containing highly proprietary financial data, legal work product, and intensely privileged communications (the “**Computer**”); (ii) cellular and auxiliary electronic apparatuses essential for two-factor authentication, secure communications, and daily modern commerce (the “**Electronics**”); (iii) a personal wallet containing indispensable financial access cards and banking implements; (iv) primary, non-replicable government-issued identification documentation; (v) an international passport, the deprivation of which severely restricts fundamental, Charter-protected mobility rights; and (vi) lawfully prescribed, highly regulated pharmacological treatment, specifically Adderall (the “**Medication**”), strictly necessary for sustained medical well-being and psychological stability.
11. I note, at this juncture, that the focus remains that which was seized from Unit 410-775 King Street West, City of Toronto, Province of Ontario, M5V 2K3 between September 20 to October 1, 2024.
12. The actions of the Perpetrator *in limine* constitute blatant, undeniable civilian theft, completely devoid of any color of right, lawful authorization, or judicial sanction whatsoever. The Perpetrator possessed a clear, unadulterated, and unambiguous *animus furandi* (the specific, malicious intention to steal and permanently deprive the owner). To properly and legally adjudicate this matter from its very inception, the foundational property maxim articulated extensively in Herbert Broom’s esteemed literary treatises must be rigorously applied: *Nemo dat quod non habet* (no one can give what they do not legitimately possess). Because the Perpetrator possessed absolutely zero lawful title, equitable interest, or legitimate proprietary claim to the Receptacle or any of its constituent contents, any subsequent transfer of the Property—whether to a private individual fencing stolen goods, a municipal agency acting with gross carelessness, or a premier federal law enforcement agent—was inherently, conceptually, and legally incapable of conveying valid legal possession or establishing a pristine, defensible evidentiary chain of custody. The initial, indelible taint of civilian criminality irrevocably and permanently infects all subsequent state action, rendering the continued possession by the state entirely poisonous and deeply constitutionally offensive. The state cannot unilaterally cure a fundamentally defective title acquired initially through theft simply by logging the stolen goods into a sterile evidence locker under the guise of an investigation.
13. The Perpetrator, in an overt, highly irregular act that irrevocably taints the evidentiary lifecycle and procedural utility of the aforementioned items, subsequently surrendered the stolen Receptacle and its myriad, deeply private contents to the TPS 14th Division. Thereupon, a municipal law enforcement officer, specifically Sergeant Black (the “**Sergeant**”)—whose historical, highly specialized, and tactically focused affiliation with the Integrated Gun and Gang Task Force renders his direct, hands-on involvement in a routine, civilian property intake highly anomalous, deeply irregular, and profoundly suspicious—undertook a warrantless, entirely undocumented, and wholly unconstitutional inspection of the intensely private contents of the Receptacle. This invasion represents a severe, highly actionable breach of the reasonable expectation of privacy, a constitutional expectation zealously guarded by Canadian courts under the strict framework established in *R. v. Edwards* and *R. v. Tessling*. By aggressively rummaging through a stolen, closed receptacle without the faintest hint of judicial pre-authorization, informed consent from the lawful owner, or rapidly unfolding, legitimate exigent circumstances, the Sergeant flagrantly and unapologetically contravened the core privacy protections enshrined within section 8 of the *Canadian Charter of Rights and Freedoms*. In undertaking this action, the Sergeant effectively utilized the civilian theft perpetrated by the unauthorized actor as a highly convenient, extra-legal bypass to cleverly circumvent the

228 419 305 rigorous, mandatory, and constitutionally required parameters of a judicially authorized search warrant. This
419 305
ephorrent behavior epitomizes the profound legal concept of *fraus est celare fraudem* (it is a fraud to conceal a fraud); the state categorically cannot exploit, endorse, or leverage a criminal act committed by a civilian to execute an otherwise illegal and unconstitutional search of private property without irreparably damaging the administration of justice.

14. It is further submitted, with profound administrative concern and justified indignation, that the Sergeant, functioning under an ostensible awareness, a heavily fabricated pretense, or an entirely erroneous, maliciously motivated extrapolation regarding the alleged trafficking of the lawfully prescribed Medication, arbitrarily and unilaterally bifurcated the contents of the stolen Receptacle. Demonstrating a capricious, highly unauthorized exercise of non-existent police powers, the Sergeant unlawfully retained the Medication for municipal processing, arbitrary destruction, or indefinite retention, while simultaneously orchestrating the extra-judicial, completely undocumented, and thoroughly clandestine transfer of the Computer and the Electronics directly into the federal custody of the RCMP. This arbitrary bifurcation is emphatically not merely a minor procedural irregularity to be quietly rectified by an internal memorandum or casually glossed over as a routine administrative hiccup. It is submitted that it is an active, deliberate, and highly orchestrated laundering of illegally obtained chattels between disparate law enforcement jurisdictions. The obvious, undeniable, and heavily premeditated intent of this jurisdictional shell game was to permanently obfuscate the illicit origins of the property, thoroughly and intentionally pollute the chain of custody, and systematically evade both municipal and federal judicial scrutiny. It was a masterclass in “jurisdictional arbitrage,” wherein law enforcement agents tactically shop for the operational silo most likely to insulate their unconstitutional actions from civilian oversight and strict judicial accountability. By physically splitting the evidence, the TPS and RCMP jointly engaged in evidentiary gerrymandering, severing the vital context of the items to construct a disjointed, legally impenetrable narrative.
15. Constructive custody of the Computer and the Electronics is more than likely currently maintained by the RCMP, while the institution simultaneously professes complete, entirely implausible institutional ignorance regarding the exact provenance, origin, and mechanism by which these highly sensitive seized chattels serendipitously entered their possession. This calculated, protracted retention and intentionally feigned ignorance stand in flagrant, highly actionable violation of the strict ethical and operational imperatives codified within section 37 of the *Royal Canadian Mounted Police Act*. Specifically, section 37(b) mandates that every single member holds an absolute, unyielding, and non-negotiable responsibility to “maintain the integrity of the law, law enforcement and the administration of justice,” and section 37(a) strictly requires them to “ensure that any improper or unlawful conduct of any member is not concealed or permitted to continue.” By warehousing expropriated, highly personal property while steadfastly refusing to investigate, acknowledge, or immediately rectify the fatally vitiated chain of custody, the RCMP becomes actively, knowingly, and inextricably complicit in the antecedent municipal malfeasance. This highly defensive institutional posture effectively compounds the initial civilian conversion with a continuous, compounding, and deeply actionable breach of federal statutory duties. It tragically transforms the RCMP from a presumptively objective, globally respected investigative body into a knowing, willing, and highly funded repository of stolen goods. The continued, wholly unjustified possession of these items by the RCMP operates as a continuous, daily accession to the initial tort of conversion, unequivocally rendering the state a rogue, unconstitutional bailee of private property.

4.0 JURISPRUDENCE: SECTION 37 OF THE ROYAL CANADIAN MOUNTED POLICE ACT

15. The rigorous ethical and operational obligations enshrined within section 37 of the *Royal Canadian Mounted Police Act* are underpinned by an extensive and sophisticated body of jurisprudence spanning multiple jurisdictions.
16. Section 37 is decidedly more than a mere articulation of organizational values or an aspirational code of conduct; it constitutes the immutable legislative foundation upon which the lawful exercise of federal police authority is predicated.
17. Section 37 of the *RCMP Act* provides as follows:
 - 37 It is the duty of every member:
 - (a) to respect the rights of all individuals;
 - (b) to uphold the integrity of the law, law enforcement, and the administration of justice;

- (c) to discharge the member's responsibilities promptly, impartially, and diligently, in accordance with the law and without misuse of authority;
- (d) to avoid any actual, apparent, or potential conflicts of interest;
- (e) to ensure that any improper or unlawful conduct by any member is neither concealed nor allowed to persist;
- (f) to remain incorruptible, refraining from accepting or seeking special privileges or otherwise incurring obligations that may compromise the proper execution of the member's duties;
- (g) to conduct themselves at all times with courtesy, respect, and honour;
- (h) to sustain the honour of the Force, along with its principles and purposes.
- R.S., 1985, c. R-10, s. 37; R.S., 1985, c. 8 (2nd Supp.), s. 16; 2013, c. 18, s. 27

18. The *Enhancing Royal Canadian Mounted Police Accountability Act*, SC 2013, c 18, effected amendments to section 37 in 2013.

19. The summary of this statute is as follows:

This enactment augments the accountability of the Royal Canadian Mounted Police by reforming the Royal Canadian Mounted Police Act in two critical domains. Firstly, it fortifies the RCMP's review and complaints mechanisms, instituting a framework for the investigation of serious incidents involving members. Secondly, it modernizes disciplinary, grievance, and human resource management procedures, aiming to prevent, address, and rectify performance and conduct issues expeditiously and equitably. It establishes a new complaints commission, the Civilian Review and Complaints Commission for the RCMP (CRCC), endowing it with broad access to RCMP-held information, investigative powers, and the authority to conduct joint complaint investigations and policy reviews. The Act introduces measures to enhance the transparency and accountability of investigations into serious incidents involving members, including referral to provincial bodies and the appointment of independent civilian observers. It further modernizes the RCMP's human resources management regime, empowering the Commissioner with respect to staffing, performance management, harassment-related disputes, and general human resource matters. The Commissioner is authorized to create a consolidated dispute resolution framework, offering flexibility in redress processes. The Act provides for a disciplinary process that enables managers or conduct authorities to impose a range of conduct measures, requiring conduct hearings solely when dismissal is sought. It also implements a mechanism by which certain members may be deemed persons appointed under the Public Service Employment Act at a time determined by the Treasury Board.

20. At this juncture, Regional COM is demonstrably failing to respect the rights of all individuals.
21. Furthermore, he is not upholding the integrity of the law, law enforcement, or the administration of justice.
22. The Regional COM has neglected to perform his duties promptly, impartially, and diligently, in accordance with the law and without abusing his authority.
23. Additionally, the Regional COM's conduct is marked by an actual, apparent, or potential conflict of interest, particularly in his preferential treatment of subsequent municipal or provincial police forces. In light of Regional COM's obstruction, it must be underscored that he is obliged, proactively and without delay, to guarantee that any improper or unlawful conduct by any member is neither concealed nor permitted to continue. Moreover, the Regional COM was, and remains, required to act at all times in a courteous, respectful, and honourable manner—a standard he has failed to meet. Consequently, he has not upheld the honour of the Force or its foundational principles and purposes. An adverse inference should be drawn against the Regional COM. The following authoritative precedents unequivocally govern the application of section 37 to the current factual context and establish the Commission's absolute, non-derogable obligation to intervene decisively and conduct a thorough investigation.

<i>R. v. Campbell</i> , 1999 1 S.C.R. 565 (the "Campbell Decision")

24. The Supreme Court of Canada categorically and unequivocally established that the *Royal Canadian Mounted Police Act* imposes an absolute, strict, and uncompromising statutory duty on all members to act “in accordance with the law.”
25. In examining a complex reverse-sting operation, the highest Court in the land ruled definitively that the statute absolutely does not grant police a blanket justification, a generalized, overarching immunity, or an extra-legal mandate to commit crimes, breach the constitution, or utilize blatantly illegal methods to enforce the law, even in the fervent pursuit of ostensibly noble law enforcement objectives. The rule of law is defined as a rigid, structural framework, not a porous, flexible membrane through which state actors may selectively pass when deemed convenient to their operational aims.
26. There is a distinction between that which is sought in a complaint and that which is sought in court. Nonetheless, Campbell confirmed that facially illegal conduct of the RCMP can and must be addressed, in the modern day form of the RCMP Act, by way of complaint at first instance.
27. As found in Campbell, A police officer investigating crime occupies an independent public office, and is not a government functionary or agent of the executive. Even if Crown agency applied for some purposes, illegality falls outside any lawful ambit, defeating immunity arguments. Parliament’s later enactment of s. 8 of the Controlled Drugs and Substances Act, S.C. 1996, c. 19 confirms the earlier absence of authority to sell drugs.
28. Nonetheless, responding to a request from an individual affected by misconduct of police forces requires a prompt and honest response from the Regional COM which he has failed to do.

Application of the Law to the Facts

29. The Regional Command cannot rely on the highly convenient, nebulous, and increasingly threadbare excuse of an “active law enforcement operation” to indefinitely justify the ongoing, unlawful detention of the Property. Because the initial seizure was irrevocably and permanently tainted by civilian theft and an unauthorized, warrantless municipal bifurcation, the continued, stubborn possession by the RCMP is fundamentally and incurably unconstitutional.
30. The *Campbell* Decision explicitly dictates that the RCMP must operate strictly within the inflexible, codified bounds of lawful authority; thus, they categorically cannot leverage, forensically interrogate, or endlessly harbor illegally acquired chattels. The abject failure to immediately return the Property constitutes a direct, egregious, and actionable breach of this core statutory duty, demonstrating a highly toxic command culture that views the law as an obstacle to be bypassed rather than a sacred mandate to be upheld.

Bigeagle v. Canada, 2023 FCA 128 (the “Bigeagle Decision”) and Jones v. Canada, 2018 NBCA 86 (the “Jones Decision”)

Precedential Value:

31. The Federal Court of Appeal in *Bigeagle* clarified the precise, highly nuanced scope of section 37, ruling that while the provision robustly outlines the fundamental statutory duties and ethical obligations of RCMP members to the state and the **public at large**, it does not strictly create a specific, private legal “duty of care” owed to individual citizens for the sole, exclusive purpose of pursuing lucrative civil negligence claims against the Crown within the realm of private tort law.

Application of the Law to the Facts

32. The framework established in *Bigeagle* is deeply acknowledged, comprehended, and fully embraced herein. Crucially, this formal, highly structured grievance is brought directly to the CRCC rather than pursued as a standard

231 422 civil tort claim for mere negligence in the provincial or federal courts. This complaint directly engages the core disciplinary, ethical, and administrative oversight functions of section 37 that the Federal Court of Appeal explicitly acknowledged exist dynamically outside of traditional tort law. The profound failures of the Regional Commander—specifically the highly calculated weaponization of administrative silence, the harboring of stolen property, and the gross failure to supervise subordinate conduct—are advanced herein as a profound breach of internal discipline, a shattering of public trust, and a catastrophic failure of statutory duty warranting independent, aggressive civilian investigation. This precise approach aligns perfectly and harmoniously with the jurisprudential boundaries explicitly set by the Federal Court of Appeal, ensuring the CRCC is the precise, correct, and legally unassailable venue for robust redress.

Frémy v. Canada, 2022 FC 750 and Herrera-Morales v. Canada, 2016 FC 578ⁱ

Precedential Value

33. These prominent Federal Court decisions collectively and powerfully establish that section 37 is highly relevant, exceptionally potent, and appropriately invoked within administrative contexts to rigorously evaluate the procedural fairness, legality, and overarching unreasonableness of administrative decisions made by the Force. This is established as especially true when such administrative conduct is intrinsically bundled with broader, systemic *Canadian Charter of Rights and Freedoms* challenges regarding the unlawful deprivation of liberty or property.

Application of the Law to the Facts

34. The persistent, highly calculated administrative silence of the Regional Commander, coupled directly and inextricably with the systemic, algorithmic suppression of the Acta Falsa, deeply offends the foundational administrative fairness and constitutional principles fiercely protected under section 37. The CRCC is therefore statutorily and jurisprudentially empowered—indeed, compelled—to heavily review this unconstitutional silence. It must be viewed not merely as an issue of poor customer service, a minor administrative backlog, or a trivial clerical oversight, but as a profound, highly actionable failure of the solemn, non-delegable legal duties enshrined in section 37. To completely ignore a lawful demand from a citizen for the return of unconstitutionally seized property is an active, highly aggressive decision that falls squarely within the administrative review parameters thoroughly outlined in *Frémy*.

5.0 STATUTORY CONTRAVENTIONS, CHARTER INFRINGEMENTS, AND THE DOCTRINE OF ABSOLUTE NULLITY

16. The initial seizure, formal intake, and subsequent, highly protracted retention of personal property (the “**Property**”) by any federal investigative agency is emphatically not a matter of operational convenience, logistical preference, budgetary constraint, or discretionary administrative fiat; it is rigorously and inflexibly governed by the strict, uncompromising, and highly detailed statutory regime explicitly codified within section 490 of the *Criminal Code*. This legislative framework was intentionally and explicitly engineered by the Parliament of Canada to continuously and forcefully subjugate the evidentiary imperatives of the state to the constitutionally protected property and privacy rights of the individual citizen. It ensures categorically that no private property belonging to a citizen is warehoused indefinitely in the dark, completely unaccountable abyss of federal evidence lockers without rigorous, periodic, and highly critical judicial justification. Property rights in Canada, while not absolute, demand that the state continuously and vigorously justify its coercive incursions into the private sphere.
17. The procedural lifecycle, the unforgiving statutory deadlines, and the corresponding, entirely non-negotiable judicial oversight mandates governing seized chattels are unambiguously delineated as follows to strictly prevent state overreach:

232 Page 423 of 423 Section	309	
	Statutory Duration	Mandatory Legal Requirement for Continued Retention
Initial Detention	Up to 3 months	A formal, sworn report to a justice (the “ Form 5.2 ”) must be duly filed, explicitly detailing the precise items seized and providing the exact, highly compelling legal and investigative justification for initial retention. Failure to file this report precisely on time renders the initial seizure immediately unlawful and triggers absolute, immediate restitution obligations. It stands as the foundational, non-negotiable document of state accountability.
Further Detention	3 months to 1 year	A presiding Justice must be substantively satisfied, upon formal, written application by the Crown, that further detention is absolutely warranted based on the active, ongoing, and demonstrably productive nature of the investigation. The state cannot simply “sit” on the evidence to inflict punishment by process; they must mathematically demonstrate forward momentum.
Superior Court Extension	Beyond 1 year	A Superior Court judge must be demonstrably satisfied, through the presentation of highly compelling, sworn, and meticulously particularized affidavit evidence, that the inherently “complex nature” of the active investigation explicitly necessitates and warrants continued, protracted detention. This standard imposes a formidable, exceptionally high evidentiary threshold upon the state. Law enforcement cannot, under any circumstances, rely upon mere administrative delays, internal resource constraints, routine investigative pacing, or officer vacations to legally justify continued possession. Rather, the presiding jurist must rigorously evaluate and objectively determine whether the extraordinary labyrinthine nature of the criminal enterprise, the unprecedented volume of complex digital forensics requiring highly specialized decryption, or the highly intricate involvement of international or multi-jurisdictional actors strictly justifies the ongoing, severe constitutional infringement of the individual's property rights. This strict, uncompromising judicial oversight is intentionally designed to unequivocally prevent the state from indefinitely warehousing private property under the highly convenient, unchecked fiction of an “open and ongoing file.”
Expiration	Post-1 year (without valid order)	Property must be immediately and unconditionally returned to the lawful owner unless formal, substantive criminal proceedings are actively instituted against the owner or absolute forfeiture is definitively granted by a court of competent jurisdiction following a full, exhaustive adversarial hearing.

18. In the seminal, highly cited appellate decision of *R. v. Gill*, 2003 BCCA 671, the British Columbia Court of Appeal conclusively established that a deliberate abdication by law enforcement personnel to meticulously apply for mandated extensions pursuant to section 490 of the *Criminal Code* is not a mere administrative defect, a technicality, or a curable bureaucratic oversight; it constitutes a profound, egregious, and highly actionable infringement of section 8 of the *Canadian Charter of Rights and Freedoms* (the paramount constitutional protection against unreasonable search and seizure). Applying this binding, highly unambiguous jurisprudential edict directly to the present factual matrix, the continued retention of the subject Property, which has now inexcusably, flagrantly, and unapologetically exceeded eighteen months in the complete absence of a valid, sworn Superior Court extension, is demonstrably and outrageously *ultra vires*. The state has utterly and completely lost any semblance of jurisdiction over the chattels.

2339. Pursuant to the explicit interpretive mandate of section 12 of the *Interpretation Act*, every federal enactment “is deemed remedial, and shall be given such fair, large and liberal construction and interpretation as best ensures the attainment of its objects.” In this specific, highly charged constitutional context, the powerful maxim *Boni judicis est ampliare jurisdictionem* (it is the part of a good judge to enlarge his jurisdiction—understood here in the remedial sense of aggressively expanding protections for the citizen against unchecked state overreach) must also be vigorously applied. The unequivocal, historically established, and fiercely guarded object of section 490 of the *Criminal Code* is to strictly circumscribe the formidable, highly coercive power of the state to indefinitely hoard private property. Applying this mandated remedial construction, any ambiguity whatsoever regarding the strict, absolute necessity of a sworn Superior Court extension must be resolved immediately, completely, and forcefully in favor of the property owner, instantaneously rendering the ultra-statutory, extended retention by the RCMP a complete and absolute nullity *ab initio*. This catastrophic administrative failure legally transmutes the initial receipt of the Property into an ongoing, continuous, and highly compounding Charter violation, thereby legally obligating the immediate, unconditional, and drastically expedited restitution of the Property, completely free of any further bureaucratic hurdles or delays.

20. Furthermore, the persistent, calculated, and highly organized administrative silence emanating directly from the office of the Regional Commander, despite repeated, formally drafted, and legally sound demands for logistical retrieval directives, functions as an unauthorized, extra-judicial, and highly malicious continuation of the initial, tainted detention. This extra-statutory retention purposefully and intentionally bypasses the heavily mandated judicial oversight mechanisms designed by Parliament to protect the citizenry, manifesting as an undeniable, actionable nullity. Such brazen, institutional disregard for hard statutory timelines strongly triggers the fundamental equitable and legal maxim *ubi jus ibi remedium* (where there is a right, there is a remedy), cementing the absolute, unassailable entitlement of the Complainant to the immediate physical restitution of the chattels. Furthermore, the venerable, foundational maxim *Spoliatus debet ante omnia restitui* (a person despoiled ought to be restored before anything else) must be strongly invoked. The RCMP possesses absolutely no legal standing, moral authority, or operational justification to interrogate the property, utilize its proprietary data, or conduct further investigative proceedings until the fundamental, underlying illegality of its physical possession is completely rectified by the immediate restitution of the chattels. The state cannot, under any interpretation of Canadian or common law, hold private property hostage while simultaneously, stubbornly refusing to legally justify its ongoing captivity.

6.0 THE SYSTEMIC SUPPRESSION OF PUBLICLY ACCESSIBLE JUDICIAL RECORDS, DIGITAL SPOILIATION, AND FORENSIC ANOMALIES

21. A foundational, immutable, and internationally recognized pillar of Canadian jurisprudence is the “Open Court Principle.” As affirmed forcefully, repeatedly, and unambiguously by the Supreme Court of Canada in landmark decisions such as *Sherman Estate v. Peters* and *Vancouver Sun (Re)*, this constitutional imperative dictates that judicial proceedings, the issuance of highly coercive state warrants, and their associated documentary records are presumptively, inherently, and robustly accessible to the populace. The rigorous *Dagenais/Mentuck* framework establishes clearly that court records may only be sealed if publication bans or sealing orders are strictly necessary to prevent a serious risk to the proper administration of justice, and only if the salutary effects of the sealing order heavily outweigh the deleterious effects on the rights and interests of the public. This presumption exists to ensure that the formidable, life-altering administration of justice is not veiled in clandestine secrecy, thereby preventing the descent into a modern Star Chamber and fostering unshakeable, profoundly necessary public confidence in the judicial apparatus.
22. Once an Information is sworn before a Justice and legal process is formally issued, the originating police service maintains the primary, non-delegable administrative obligation to provide both the public and the targeted subject of the investigation with unimpeded, timely access to the sworn Information (Criminal Code Form 2) and all related, subsequent judicial endorsements. This unyielding administrative duty is further illuminated and rigidly enforced by Herbert Broom’s powerful legal maxim *Delegatus non potest delegare* (a delegate cannot further delegate). The RCMP, having functioned operationally as the primary, originating federal investigative authority and the ultimate, physical custodian of the expropriated evidence in this highly specific operation, is strictly, legally precluded from delegating, deflecting, or abdicating its custodial responsibilities for the sworn Information to extraneous municipal

- 234 agencies or provincial court registries when directly confronted with a lawful, formalized demand for full
425 disclosure. Furthermore, section 37(b) of the *Royal Canadian Mounted Police Act* imposes a continuous,
affirmative duty upon all commissioned and non-commissioned members to “maintain the integrity of the law...
and the administration of justice.” The systemic, heavily institutionalized suppression of these publicly accessible
judicial records fundamentally subverts this rigidly required integrity, rendering the administration of justice a
clandestine, highly inaccessible enterprise utterly antithetical to the core values of a free, open, and democratic
society. The chilling, dystopian effect of executing secret warrants in perpetual, unjustified secrecy is a classic
hallmark of authoritarianism, entirely irreconcilable with Canadian constitutional norms and the *Charter*.
23. Furthermore, as comprehensively elucidated, deeply explored, and definitively settled in the jurisprudence of *R. v. Baldovi, 2016 MBQB 90*, while the doctrine of judicial immunity robustly and necessarily shields the deliberative, internal thought processes of the bench, such immunity categorically does not extend downwards to authorize the administrative suppression of the resultant judicial authorizations by police personnel, nor does it permit the perpetual, highly unjustified sealing of warrants once the initial investigative necessity for secrecy has demonstrably evaporated post-execution. Consequently, the obstinate, undocumented, and highly suspect refusal of the RCMP to disclose the requested warrants, Information to Obtain (ITO) documents, and Intake Court Endorsements represents a direct, sustained, and highly calculated affront to the principles of fundamental justice codified under section 7 of the *Canadian Charter of Rights and Freedoms*. This refusal effectively renders the targeted individual procedurally paralyzed, legally blindfolded, and completely unable to substantively challenge the legality of the state's highly invasive incursions into private affairs.

7.0 FORENSIC DECONSTRUCTION OF THE ACTA FALSA: ALGORITHMIC SPOILIATION AND THE “CL (M)” ARTIFACT

24. This systemic obfuscation is exponentially compounded by severe digital irregularities and absolutely incontrovertible evidence of post-generation tampering, which is meticulously documented within the forensic report entitled “CL (M) - Forensic Manipulation.docx”, concerning the document colloquially designated as the Acta Falsa. Empirical, highly sophisticated, metadata-driven forensic analysis has conclusively established that the documentation—which fraudulently purports to be a pristine, legitimate Intake Court Endorsement issued by the Superior Court of Justice—was artificially and deliberately manipulated. The deep-level analysis irrefutably confirms the highly irregular, completely unauthorized utilization of the GrapeCity Documents for PDF Application Programming Interface (the “API”), specifically isolating the deployment of the obsolete and fundamentally unstable software version 6.0.2.0, an application renowned in forensic circles for depositing distinct digital footprints when improperly applied to secure documents.
25. The algorithmic execution of uncalibrated, technologically clumsy text redaction within this specific, outdated software iteration predictably precipitated a universally recognized digital rendering failure. This profound digital spoliation caused severe Cartesian coordinate matrix failures and Z-index layering collapses, resulting in what is referred to in advanced software engineering and cybersecurity parlance as the “bounding-box shear” phenomenon (the “DOC-6507 Bug”). The underlying mechanics of this digital spoliation are technologically irrefutable and mathematically provable beyond any conceivable doubt: when the utilized software was directed to clandestinely eradicate foundational text blocks—specifically the true law enforcement organizational origin and the title “Regional COM” (associated directly with the official title of the Regional Commander)—from the face of the document, the DOC-6507 Bug triggered a catastrophic mathematical collapse of the Bezier curves responsible for generating and rendering the serif letter “O”.
26. The forcible, programmatic detachment of the apex control points severed the character into two independent, unanchored curvilinear structures—visually manifesting upon rendering as an open parenthesis and a closed parenthesis. These rogue, untethered vectors subsequently drifted across the coordinate plane and encapsulated the adjacent character “M”, resulting in the highly irregular, structurally impossible, and visually jarring “CL (M)” artifact currently scarring the face of the document. Most egregiously, this digital debris rests suspiciously adjacent to the name of Court Officer Christyn Frugoni-Rojas. It is submitted that this is emphatically not a clerical error, a transcription typo, nor is it a benign glitch resulting from routine physical scanning; it is the permanent, undeniable, and mathematically precise digital fingerprint of an intentional, highly coordinated, and ultimately botched

235 algorithmic cover-up designed to surgically hide the true chain of command and the federal origins of the operation.
426 Here, the maxim *Actus non facit reum nisi mens sit rea* (the act does not make a person guilty unless the mind is guilty) is deeply engaged, as the deliberate initiation of the GrapeCity redaction protocol unequivocally establishes the guilty intent required for spoliation.

Nota Bene - The Rebuttal of the “Clerical Error” Defense:

27. It is highly anticipated, and entirely predictable, that the RCMP Legal Services Directorate will attempt to aggressively dismiss the “CL (M)” artifact and the GrapeCity metadata as mere “clerical errors” or benign software artifacts generated innocently during routine case management uploading to a provincial database. This counter-argument is forensically bankrupt and technologically impossible. An off-the-shelf PDF viewer utilized for standard administrative review does not autonomously inject GrapeCity API metadata, nor does it selectively target specific, highly sensitive law enforcement titles for redaction while simultaneously triggering complex bounding-box shears. The verified, cryptographic presence of these specific, complex algorithmic footprints definitively proves that the document was intentionally opened in a dedicated, commercial PDF manipulation environment for the express, malicious purpose of altering its structural contents post-generation. Such deliberate, targeted software manipulation of a sworn court document completely extinguishes any presumption of administrative innocence or good faith execution.
28. The shocking discovery of such blatant digital spoliation and algorithmic redaction artifacts undeniably summons the forceful, absolute application of the venerable evidentiary maxim, deeply rooted in the legal treatises of Herbert Broom: *Falsus in uno, falsus in omnibus* (false in one thing, false in everything). Because the documents have been demonstrably and technologically manipulated to conceal the true identity of the executing authorities and the exact jurisdictional origins of the seizure, the law rigorously and unavoidably mandates the absolute presumption that the entire document is a wholly fabricated instrument. This sophisticated tampering squarely implicates section 50.1(1)(d) of the *Royal Canadian Mounted Police Act*, which explicitly and forcefully establishes that it is a serious, indictable offence for any person to “destroy, mutilate, alter, falsify or conceal a document or thing... knowing that the document or thing is likely to be relevant to an investigation.” This cryptographic proof of forgery permanently elevates the complaint from mere administrative negligence to active criminal malfeasance requiring immediate, unapologetic intervention by the Commission. The standard presumption, *Omnia praesumuntur legitime facta donec probetur in contrarium* (all things are presumed to have been legitimately done, until the contrary is proved), has been entirely and spectacularly rebutted by the forensic data.

8.0 STRUCTURAL DEVIATIONS FROM THE STATUTORY PRO-FORMA: A COMPARATIVE ANALYSIS OF THE FRAUDULENT INFORMATION PACKAGE

29. The complete illegitimacy of the Acta Falsa (specifically identified within the Evidentiary Record as “Information Package 4810 998 24 48129169-00 (4).pdf”) is further proven not solely by its profound digital corruption and GrapeCity footprint, but by its grotesque, sweeping structural deviation from the absolute mandatory statutory requirements of the *Criminal Code* of Canada. A meticulous, comparative analysis of the Acta Falsa against the standard, Ministry-approved blank Form 2 (the “ADULT-COMMON-INFORMATION-FORM-WITH-HIGHLIGHTED-CHANGES - LINCOLN COUNTY LAW ASSOCIATION.pdf”) reveals a total, catastrophic structural collapse of the legally required form and substance. A sworn Information is the foundational, indispensable document that breathes constitutional life into the entire criminal justice process; if it is fundamentally defective at its core, the entire subsequent proceeding is rendered legally stillborn.
30. The rigorous forensic and legal review of the Acta Falsa documents a staggering forty-three distinct structural errors, severe anomalies, and deliberate omissions when compared line-by-line to the strict statutory pro-forma baseline. Most glaringly, and most unconstitutionally, the document inexplicably lists Christyn Frugoni-Rojas—a Court Officer—as the Informant, ostensibly “Deemed Sworn/Affirmed” on September 23, 2024. Simultaneously, in direct contradiction to fundamental legal principles, it identifies the Officer/Agent de police as “KOLANKOWSKI, MI” of the “TORONTO POLICE SERVIC” strictly under “14 DIVISION.”

2361. This chaotic, highly irregular amalgamation of municipal police officers, court staff inexplicably acting as swearing informants, and hidden federal operational oversight completely obliterates the procedural clarity and direct accountability required by Form 2. It purposefully creates an untraceable, circular liability matrix where absolutely no single sworn officer actually attests, under penalty of perjury, to the reasonable and probable grounds required to constitutionally sustain the charges or the massive property seizure. The legal maxim *Ubi inanis est verborum proprietas, ibi nulla est legis fortitudo* (where the propriety of words is empty, there the strength of the law is nothing) must be strictly applied; the empty, contradictory words of the Acta Falsa strip it of all legal strength. Furthermore, the absolute mandatory fields designed by Parliament to safeguard the Charter rights of a citizen—such as clear, unambiguous swearing dates, accurate and verifiable judicial signatures, and precise, legally coherent descriptions of the alleged offences in direct relation to the seized property—are either deeply corrupted by the GrapeCity manipulation, deliberately obfuscated, or entirely absent.

Nota Bene - The Rebuttal of “Substantial Compliance”:

32. The Crown or the RCMP Legal Directorate will inevitably attempt to salvage the burning wreckage of the Acta Falsa by invoking the highly curative provisions of the *Criminal Code*, arguing that the document, despite its myriad, glaring flaws, represents “substantial compliance” with the prescribed forms and thus should not be invalidated for mere technical defects in substance or form. This argument is fatally, fundamentally flawed. The doctrine of substantial compliance exists solely to cure minor typographical omissions or harmless formatting errors; it absolutely does not exist to resurrect a document that has been deliberately algorithmically manipulated post-swearing, or one that intentionally obfuscates the true identity of the swearing Informant and the underlying jurisdictional authority. A document boasting forty-three severe structural errors and incontrovertible evidence of active digital forgery has crossed the Rubicon from merely “defective” to outright “fraudulent.”
33. The maxim formulated by Herbert Broom must be forcefully applied: *Ex dolo malo non oritur actio* (no right of action can have its origin in fraud). The state cannot hide behind the generous veil of substantial compliance when the defects in the document are born of active deception, algorithmic manipulation, and a deliberate intent to evade the jurisdictional oversight of the courts. To accept such a profoundly corrupted document as “substantially compliant” would make an absolute mockery of the fundamental justice guarantees enshrined in section 7 of the *Canadian Charter of Rights and Freedoms* and would explicitly endorse police forgery as a valid, acceptable law enforcement tactic.

9.0 THE ADVENT OF CORAM NON JUDICE AND THE TRANSFORMATION OF LAW ENFORCEMENT INTO PRIVATE TORTFEASORS

34. Because the entire proceeding against the subject was founded upon a manipulated, structurally defective endorsement processed secretly through an untracked, third-party developer API rather than a properly, lawfully sworn Information (Form 2), the legal proceeding fundamentally ceases to exist in the eyes of the law. This invokes the ancient, highly powerful, and absolute legal doctrine of *coram non judice* (literally, “not before a judge”). When a legal proceeding is declared *coram non judice*, it means that the tribunal, court, or issuing authority completely and entirely lacked the requisite subject-matter jurisdiction to issue the orders, warrants, or detentions in question. The entire process is not merely voidable at a later date; it is void *ab initio* (from the very beginning).
35. The legal consequences of a *coram non judice* finding are absolute, sweeping, and devastating to the defensive posture of the state. A jurisdictional nullity of this immense magnitude cannot be retroactively cured, amended, or forgiven by the Crown, the Regional Commander, or even a subsequent Superior Court judge. If the foundational Information is a digitally forged nullity, then absolutely every subsequent action flowing from it—including the highly invasive seizure of the Computer, the Electronics, and the life-sustaining Medication, as well as any physical detention or restriction of liberty—is entirely stripped of any color of lawful authority. Law enforcement personnel operating under a *coram non judice* warrant are no longer executing protected state functions; they are, in the strict eyes of the law, private actors committing severe tortious acts against a free citizen.
36. Therefore, the bureaucratic and physical apparatus deliberately constructed by the JFO to effect the physical movement, arrest, or imprisonment through these forged documents constitutes the most egregious state-actor

237 kidnapping scenario imaginable. It completely and permanently strips the involved police officers of their lawful
428 statutory immunities under the *Criminal Code*, transforming a standard, albeit deeply flawed, arrest into highly
314 actionable false imprisonment and arbitrary detention. The state simply cannot lock a citizen in a cage, restrict their
mobility, or permanently confiscate their property based on a PDF that has been secretly edited by an unknown
actor using unauthorized commercial software.

Nota Bene - The Rebuttal of "Good Faith Execution"

37. The officers who physically retain the property, or those who executed the initial detention, will undoubtedly claim they were operating in pure "good faith," merely following the orders printed on the face of the Acta Falsa, entirely unaware of the underlying GrapeCity manipulation and severe structural defects. While good faith may occasionally mitigate punitive damages for frontline officers in highly ambiguous, rapidly evolving situations, it provides absolutely zero sanctuary for the institution itself. This is particularly true for Command authorities, such as the Regional Commander, who have been put on explicit, formal, and repeated notice of the forgery (via the Antecedent Communications) and yet fiercely, stubbornly maintain their administrative silence. Good faith completely evaporates the moment the state is made aware of the profound unconstitutional taint and stubbornly refuses to act to correct it.
38. The unyielding, foundational wisdom of Herbert Broome's maxim must be relied upon: *Quod ab initio non valet, in tractu temporis non convalescit* (that which is void from the beginning does not become valid by the passage of time). The Regional Commander cannot simply out-wait the forgery through a war of attrition. No amount of administrative silence, institutional delay tactics, or jurisdictional deflection can magically breathe constitutional life into a document that was legally dead upon its manipulated creation. The ongoing, stubborn possession of the chattels by the state under this void framework is an ongoing, compounding false imprisonment of property requiring immediate, decisive intervention.

10.0 EXPANDED NON-OBVIOUS LEGAL THEORIES: MALICIOUS PROSECUTION AND SYSTEMIC CHARTER VIOLATIONS (SECTIONS 7, 8, AND 9)

39. The actions detailed herein massively transcend the mere unauthorized retention of chattels and enter the grave realm of severe, systemic constitutional torts. The deployment of a digitally forged Information to legally justify the seizure of property and the deprivation of liberty squarely and unavoidably engages section 9 of the *Canadian Charter of Rights and Freedoms*, which guarantees the absolute right not to be arbitrarily detained or imprisoned. A detention founded upon an Acta Falsa is the very definition of arbitrary, as it relies entirely on state caprice, forgery, and software manipulation rather than lawful, judicial authorization. When combined with the profound section 8 violations (the unreasonable, warrantless search and seizure of the Receptacle) and the severe section 7 violations (the deprivation of liberty and security of the person through the cruel withholding of prescribed Medication), the conduct of the RCMP represents a comprehensive, multi-front assault on fundamental rights.
40. Furthermore, these incontrovertible facts establish the foundational, necessary elements for the highly serious civil tort of Malicious Prosecution against the state actors involved. The elements of malicious prosecution require that the proceedings were initiated by the defendant, concluded in favor of the plaintiff (or were otherwise legally void), lacked reasonable and probable cause, and were motivated by malice or a primary purpose other than carrying the law into effect. The deliberate digital manipulation of court records to conceal the true origins of the investigation, combined with the intentional jurisdictional laundering of the seized chattels, explicitly and undeniably demonstrates the requisite malice and the total absence of reasonable and probable cause. The prosecution was not an exercise in justice; it was an exercise in targeted, extra-legal harassment.
41. Additionally, the highly calculated policy of absolute administrative silence by the Regional Commander, particularly in the face of explicit, urgent demands regarding lawfully prescribed Medication and critical digital infrastructure, gives rise to the severe tort of Intentional Infliction of Mental Suffering. It is submitted that the Regional Command is acutely aware that withholding these specific items causes severe, ongoing psychological and operational distress. By intentionally ignoring these urgent, constitutionally grounded pleas, the Command is

Nota Bene - The Rebuttal of Prosecutorial and Police Immunity:

42. The Crown will inevitably attempt to shield the involved RCMP and TPS members, as well as the Crown Attorneys handling the file, behind the formidable, historically impenetrable doctrines of prosecutorial and police immunity. It will be argued that state actors must be free to investigate without the constant paralyzing fear of civil liability. However, Canadian jurisprudence, notably the Supreme Court decision in *Nelles v. Ontario*, firmly establishes that absolute immunity absolutely does not exist for malicious prosecution or for acts committed with deliberate malice and outside the scope of lawful authority. The digital forgery of the Acta Falsa and the intentional spoliation of evidence are *ultra vires* acts that fundamentally and permanently sever the actors from any protective shield of state immunity.
43. This systemic, multi-agency failure of justice triggers robust section 24(1) *Charter* remedies, exposing the state to massive punitive and aggravated civil damages. The digital shrapnel of “CL (M)” and the forty-three documented GrapeCity layout errors stand as permanent, un-erasable proof of this profound collapse of judicial integrity. The ultimate maxim of Herbert Broom must be applied: *Commodum ex injuria sua nemo habere debet* (no person ought to have advantage from his own wrong). The RCMP cannot weaponize the legal system using fraudulent instruments, launder the evidence across jurisdictions, and then attempt to cowardly hide behind the very same legal system’s immunities when their profound deceit is uncovered.

11.0 STATUTORY NON-COMPLIANCE: COMMISSIONER'S STANDING ORDERS (CONDUCT), SOR/2014-291

44. The continued, completely unjustified retention of the Property, facilitated directly and intentionally through the uninterrupted, highly strategic administrative silence of the Regional Commander, constitutes a profound, multifaceted breach of the *Commissioner's Standing Orders (Conduct)*, SOR/2014-291.
45. These Orders are emphatically not merely internal operational guidelines, casual suggestions, or aspirational human resources literature to be ignored at will; they are binding subordinate legislation that strictly codifies the absolute highest standards of integrity, accountability, and strict legal adherence required of all RCMP personnel across Canada. The deliberate refusal to address a continuing, compounding Charter violation (specifically, the unauthorized retention of property under s. 490 of the *Criminal Code*) places the involved officers, and by direct extension the Regional Command through vicarious liability and a catastrophic failure of command supervision, in direct contravention of their sworn, solemn obligations to act lawfully.
46. The failure to respond can only be seen to acts furtherance of conspiratorial agreement.
47. The Regional COM is required to either stand with the impugned conduct or distance himself. **Silence is not an option.**
48. The standard of care of a Regional Commander is paramount; willfully blinding oneself to the illegal hoarding of civilian property constitutes an egregious, fireable breach of the public trust, a total failure of Command Responsibility, and a violation of the foundational principle of *respondeat superior* (let the master answer).
49. *Nota Bene - The Rebuttal of Internal Standing:* It is highly anticipated that the RCMP Legal Services Directorate may formulate a procedural objection asserting that the *Commissioner's Standing Orders (Conduct)* are strictly internal regulatory mechanisms governing human resources and disciplinary paradigms, thereby arguing that a private civilian lacks the requisite legal standing to invoke them as a basis for a public complaint. This argument is an analytical nullity and intellectually bankrupt. While the Orders inherently govern internal discipline, they simultaneously establish the explicit, unyielding statutory duties that RCMP officers owe directly to the Canadian public. As the direct, tangible, and financially injured victim of the continuous tort of conversion and the deliberate spoliation of evidence, an unassailable equitable and legal nexus to the malfeasance in question is possessed by the Complainant. This principle is best encapsulated by Herbert Broom’s powerful maxim *Qui non prohibet quod prohibere potest assentire videtur* (he who does not prevent what he can prevent is considered to assent). The

12.0 THE MISAPPLICATION AND WEAPONIZATION OF THE OATH OF SECRECY, SOR/2014-280

46. In critically addressing the systemic, institutional suppression of the requested judicial records and the Acta Falsa, it is absolutely necessary to preemptively deconstruct the primary administrative shield historically utilized by federal agencies to unlawfully deny disclosure: the *Regulations Prescribing an Oath of Secrecy*, SOR/2014-280. Under these highly stringent regulations, members solemnly swear an oath not to disclose knowledge or information obtained in the course of their duties “without due authority” to any person “not legally entitled to it.” The persistent, obstinate, and highly suspect refusal of the RCMP to furnish the unredacted Information and relevant judicial endorsements suggests a gross, intentional misapplication of this regulatory instrument. The Command has maliciously morphed it from a legitimate shield designed to protect against illicit leaks of highly sensitive national security intelligence into a weaponized sword swung aggressively against constitutional accountability, transparency, and civilian oversight. The *Access to Information Act* and the broader principles of democratic policing further clarify that secrecy provisions cannot ever be utilized merely to cover up institutional embarrassment, severe administrative blunders, unlawful seizures, or outright criminality within the Force.

Nota Bene - The Rebuttal of Blanket Secrecy:

47. It is a highly foreseeable logical gap that the RCMP Regional COM will attempt to classify the requested warrants and Information as universally protected, hyper-sensitive operational secrets, invoking SOR/2014-280 as an absolute, impenetrable bar to dissemination. This obfuscation is directly, immediately, and permanently neutralized by the explicit textual boundaries of the Oath itself. The Oath specifically prohibits disclosure *only* to those “not legally entitled to it.” The targeted individual—functioning as the explicit target of the search, the individual whose privacy was deeply invaded, and the rightful, undisputed owner of the expropriated Property—is definitively and constitutionally *legally entitled* to review the records under the Open Court Principle, the core principles of fundamental justice, and section 7 of the *Charter*. Applying Herbert Broom's highly precise interpretive maxim *Verba generalia restringuntur ad habilitatem rei vel personae* (general words are restrained to the fitness of the matter or person), the general prohibition on disclosure is legally restrained, heavily subordinated, and rendered entirely impotent when confronted with a citizen whose constitutional rights specifically require the immediate production of the very same documents to assess the legality of the highly coercive actions of the state.

13.0 FITNESS FOR DUTY AND THE COMMISSIONER'S STANDING ORDERS (EMPLOYMENT REQUIREMENTS), SOR/2014-292

48. The deliberate, compounding, and highly coordinated failures of the RCMP members intimately involved in the laundering of the property and the digital spoliation of the Acta Falsa rise far beyond mere operational negligence or low-level administrative error; they strike directly at the core foundational employment competencies mandated by the *Commissioner's Standing Orders (Employment Requirements)*, SOR/2014-292. An officer's ongoing appointment, exercise of extraordinary police powers, and authority within the Force is inherently and inextricably conditional upon their faithful, unwavering, and unimpeachable execution of the law, both in exact letter and in spirit. The systemic disregard for the *Criminal Code* (specifically the uncompromising s. 490 extension requirements) and the active, technologically sophisticated concealment of judicial records demonstrate a fundamental, incurable failure to satisfy the baseline employment requirements of a federal peace officer. Those who actively manipulate the law to serve operational convenience or hide institutional embarrassment cannot be entrusted with the sovereign, highly coercive power to enforce it. Such actions fundamentally sever the psychological and ethical fitness required for duty.

49. The RCMP may advance the highly technical counter-argument that employment requirements under SOR/2014-292 govern strictly internal human resource evaluations and are legally irrelevant to criminal or constitutional procedures. This argument falsely and dangerously compartmentalizes the law, attempting to artificially sever the unconstitutional actions of an officer from their fundamental fitness to serve the public. An officer who engages in the willful, algorithmic suppression of evidence or the continuous, unconstitutional conversion of private property inherently violates their core conditions of employment, triggering potential immediate discharge provisions under section 20.2(1) of the *Act*. This profound interplay between administrative rules and constitutional duties is illuminated brilliantly by Broom's maxim *In eo quod plus sit semper inest et minus* (the greater always includes the lesser). If the offending officers are fundamentally unfit to lawfully hold, properly process, and timely release the chattels in accordance with strict statutory timelines, they are, by necessary and inescapable implication, utterly unfit to hold the greater, overarching privilege and immense responsibility of federal law enforcement office.

14.0 SECTION 12 OF THE RCMP ACT SUSPENSION

50. Section 12 of the *Royal Canadian Mounted Police Act* explicitly and unambiguously provides that “every member who has contravened, is found contravening or is suspected of contravening any provision of the Code of Conduct or of an Act of Parliament, or of the legislature of a province, may be suspended from duty by the Commissioner.” This critical statutory provision is emphatically not merely an administrative tool to be used sparingly or reluctantly; it is a vital, essential mechanism specifically designed for rapidly protecting the public trust and ensuring that officers who are credibly suspected of severe misconduct—such as the deliberate spoliation of digital evidence, systemic suppression of judicial records, and highly actionable neglect of duty detailed herein—are immediately removed from active duty pending a full, unhindered investigation. The rich body of jurisprudence surrounding section 12 affirms its critical role in maintaining the integrity of the Force and underscores the vast authority of the Commissioner to act decisively in the face of serious allegations of corruption or unconstitutional behavior.

Nota Bene - The Rebuttal of Premature Disciplinary Action:

51. It is highly anticipated that the RCMP Regional COM may argue that demanding a suspension under section 12 is premature, aggressively asserting that a full, multi-year internal investigation must be completely concluded and all lengthy appeals completely exhausted before such a severe administrative action can be taken against an officer.

Flaw in that hypothetical argument

52. This argument is fundamentally flawed and directly contradicts the clear, plain statutory language of section 12, which explicitly allows for suspension when a member is merely “suspected of contravening” the Code of Conduct or an Act of Parliament. The severe digital spoliation and protracted, highly organized administrative silence documented in this complaint provide far more than mere suspicion; they provide highly credible, deeply actionable, and forensically supported evidence of ongoing misconduct. Applying the paramount legal maxim *Salus populi suprema lex esto* (the welfare of the people shall be the supreme law), the immediate suspension of the involved officers is absolutely necessary to protect the public from further unconstitutional actions, to prevent the further destruction of evidence, and to preserve the fragile integrity of the pending CRCC investigation. Allowing officers who have demonstrated a willful, coordinated disregard for strict statutory timelines and the fundamental Open Court Principle to remain on active duty completely undermines the very foundation of the accountability framework of the RCMP.

Precedential Value:

53. The Federal Court in *Irvine* strongly affirmed that a decision to suspend a member under section 12 of the *RCMP Act* can be challenged by way of an internal appeal in accordance with the Commissioner's Standing Orders (Grievances and Appeals), specifically citing section 32 of the Commissioner's Standing Orders (Conduct). This highlights the firmly established procedural pathway for members to vigorously contest suspensions, demonstrating that the mechanism is robust, well-regulated, and subject to extensive internal review, thereby aggressively safeguarding the procedural rights of the officer.

Application of the Law to the Facts:

54. The *Irvine* decision powerfully demonstrates that the mechanism for suspension under section 12 is a well-established, highly regulated, and frequently utilized process within the RCMP. The demand for the immediate suspension of the involved officers is emphatically not an extraordinary, unprecedented, or extralegal request, but a highly legitimate invocation of a recognized statutory mechanism designed precisely for scenarios exactly such as this. Given the extreme gravity of the allegations—specifically including the digital manipulation of the Acta Falsa and the continuous, unconstitutional detention of the Property—the Regional Commander has the absolute authority and the overriding obligation to immediately initiate the suspension process. The existence of a robust appeal process for the suspended members, as affirmed in *Irvine*, ensures total procedural fairness, entirely neutralizing any defensive argument that suspension is an arbitrary, draconian, or irreversible action without recourse.

Turner v. Canada (Attorney General), 2025 FC 72

Precedential Value:

55. The *Turner* case simply and clearly documents the practical, routine application of section 12, noting matter-of-factly that the applicant was “suspended from duty (RCMP Act, section 12).” This explicitly confirms that suspension is a recognized, standard disciplinary measure widely utilized by the RCMP in response to serious conduct issues.

Application of the Law to the Facts:

56. The *Turner* decision strongly reinforces the practical reality that an immediate suspension under section 12 is a highly standard and thoroughly expected response to serious allegations of misconduct. The formal request for suspension aligns perfectly with established, documented RCMP practice. The utter failure of the Regional Commander to proactively utilize this mechanism in the face of heavily documented, ongoing constitutional violations further highlights the highly actionable neglect of duty and underscores the absolute, urgent necessity of CRCC intervention to compel strict adherence to disciplinary standards.

*Frémy v. Canada (Attorney General), 2018 FC 434 and Aune v. Canada (Attorney General), 2013 BCSC 178**Precedential Value:*

2427. Both the *Frémy* and *Aune* decisions discuss the stringent statutory framework governing the highly consequential dismissal or discharge of RCMP members, specifically noting that such severe actions must be conducted precisely pursuant to the *RCMP Act* (referencing former subsection 12(2) and the broader general provisions of section 12). These key cases heavily emphasize that the employment status of all RCMP members is strictly governed by the Act and its associated, detailed regulations, entirely removing it from the realm of private contract law.

Application of the Law to the Facts:

58. These critical cases underscore that the employment relationship between the RCMP and its members is rigidly defined by the strictures of the *RCMP Act*. The profound, cascading failures exhaustively detailed in this complaint—the unconstitutional detention of property and the deliberate, algorithmic spoliation of evidence—are direct, undeniable violations of the core duties expected of members under the Act. Consequently, the mechanisms for suspension and potential permanent discharge under section 12 (and related provisions) are the legally appropriate, entirely necessary, and statutorily prescribed responses to such severe misconduct. The CRCC must aggressively investigate whether the failure of the Regional Command to initiate these statutory mechanisms constitutes a further, compounding breach of duty that implicitly protects rogue officers.

Dawe v. Canada, 2002 FCT 486

Precedential Value:

59. The Federal Court in *Dawe* established unequivocally that service with the RCMP does not create a traditional, private contractual relationship, meaning that standard civil claims for wrongful or constructive dismissal are legally inapplicable. Instead, the employment relationship is governed entirely by federal statute, specifically referencing section 12 of the *RCMP Act*.

Application of the Law to the Facts:

60. The *Dawe* decision further emphasizes the absolute primacy of the statutory framework in governing all aspects of RCMP employment. Because the relationship is strictly statutory, not contractual, the remedies for severe misconduct must be found within the four corners of the Act. The suspension provisions under section 12 are therefore the primary, indispensable tools available to the Commissioner to directly address the severe, ongoing misconduct meticulously documented in this complaint. The failure to aggressively deploy these tools in response to highly credible evidence of digital spoliation and unconstitutional property detention is a colossal failure of statutory duty and an abdication of leadership.

Grant v. Canada (Attorney General) (T.D.), 1994 CanLII 9274 (FC) and 1994 CanLII 3507 (FC)

Precedential Value:

61. The foundational *Grant* decisions illustrate the complex historical application and evolution of the *RCMP Act*, specifically referencing critical amendments to the Act (noting R.S.C., 1985 (2nd Supp.), c. 8, s. 12) in the context of broader regulations governing the internal operations and discipline of the Force.

Application of the Law to the Facts:

62. While the specific issues addressed in *Grant* related to religious freedom and uniforms, the cases brilliantly demonstrate the ongoing evolution and flexible application of the *RCMP Act* and its regulations to address complex

243 320
434 organizational challenges. The sweeping statutory authority to suspend members under section 12 is a critical, highly evolved component of this framework, designed explicitly to ensure total accountability and aggressively maintain public trust. The CRCC must ensure that this formidable statutory authority is exercised appropriately and without hesitation in response to the severe misconduct detailed in this complaint, affirming that no member is above the law they are sworn to enforce.

15.0 ANTICIPATORY SPOILIATION AND THE RCMP EXTERNAL REVIEW COMMITTEE RULES OF PRACTICE AND PROCEDURE, SOR/88-313

52. The preservation of the unredacted Acta Falsa and the corresponding digital metadata is not merely a polite request for internal transparency; it is a strict, unyielding, and legally binding procedural imperative dictated by the highly anticipated escalation of this matter to quasi-judicial oversight bodies. This includes the inevitable proceedings governed by the rigorous *RCMP External Review Committee Rules of Practice and Procedure*, SOR/88-313. Section 19(3) of these Rules specifically contemplates the mandatory, legally compelled production of “original records” via formal summons. By engaging in the premature, algorithmic destruction, and targeted redaction of the Acta Falsa, the RCMP is actively committing anticipatory spoliation, intentionally destroying the evidentiary bedrock necessary to frustrate the statutory mandate of external review committees before their jurisdiction can even be officially engaged. It is the digital equivalent of shredding documents before the auditor arrives.

Nota Bene - The Rebuttal of Limited Committee Scope:

53. A highly potential counter-argument may posit that the External Review Committee (ERC) is convened solely to adjudicate internal member grievances and appeals, thereby rendering SOR/88-313 legally inapplicable to a civilian's public complaint. This represents a shallow, strategically myopic, and deeply flawed interpretation of the complex administrative lifecycle of policing misconduct. While the complaint is initiated externally via the CRCC/PCRC, the sustained, deeply documented evidence of systemic spoliation and property conversion detailed herein will inevitably trigger severe internal disciplinary measures against the involved members. These disciplined members will predictably and aggressively appeal such measures to the ERC. Therefore, the immediate, uncompromising preservation of the unadulterated evidence is fundamentally required to protect the integrity of the *own* appellate tribunals of the RCMP. This is anchored securely in Herbert Broom’s powerful maxim *Lex non cogit ad impossibilia* (the law does not compel the impossible). The RCMP cannot intentionally destroy the digital origins of the Acta Falsa and subsequently demand that an external review body prove the precise facts of the malfeasance in a vacuum of intentionally destroyed evidence.

16.0 FRUSTRATION OF LEGISLATIVE INTENT AND DEFIANCE OF THE ENHANCING ROYAL CANADIAN MOUNTED POLICE ACCOUNTABILITY ACT, S.C. 2013, C. 18

54. The sustained, highly organized administrative obstructionism exhibited by the Regional Commander does not merely violate individual statutes in isolated instances; it operates as a direct, comprehensive, and unapologetic assault on the fundamental legislative intent of the Parliament of Canada as explicitly codified in the *Enhancing Royal Canadian Mounted Police Accountability Act*, S.C. 2013, c. 18 (the “**Accountability Act**”). As explicitly delineated in the Summary of the *Accountability Act*, this critical legislation was fundamentally designed to “modernize discipline, grievance and human resource management processes” and, crucially, to “set out the authority for the CRCC to have broad access to information in the control or possession of the Royal Canadian Mounted Police.” By willfully suppressing the Acta Falsa, actively manipulating digital metadata, and utilizing strategic administrative silence to infinitely detain the Property, the RCMP Central Region is actively, intentionally engaging in the deeply subversive legal doctrine of *Frustration of Legislative Intent*.

55. The primary legal theory advanced herein is that the Regional Command is intentionally weaponizing procedural delays and manufactured jurisdictional ambiguity (i.e., blaming the municipal TPS) to indirectly achieve what the *Accountability Act* directly and explicitly prohibits: the total concealment of severe police malfeasance from civilian oversight. This subversion of democratic accountability invites the robust application of Herbert Broom's

244 maxim *Quando aliquid prohibetur ex directo, prohibetur et per obliquum* (when anything is prohibited directly, it
435 also prohibited indirectly). The RCMP cannot lawfully utilize the indirect, heavily bureaucratic mechanism of
administrative silence” to cleverly circumvent their direct, statutory duty to preserve and meticulously produce
evidentiary records for the unfettered review of the CRCC. Furthermore, applying the sweeping maxim *Quando
lex aliquid alicui concedit, concedere videtur et id sine quo res ipsa esse non potest* (when the law grants something
to someone, it is considered to grant that without which the thing itself cannot exist), it is undeniably evident that
the grant by Parliament of broad investigative authority to the CRCC implicitly and absolutely demands the strict,
uncompromising compliance of the RCMP in preserving the structural integrity of the Acta Falsa. Without the
unadulterated documents, the civilian oversight so carefully granted by the 2013 *Accountability Act* is rendered a
hollow shell, a mere administrative theater, and the legislation itself cannot effectively exist as Parliament intended.

Nota Bene - The Rebuttal of “Control or Possession” Ambiguity

56. It is highly anticipated that the RCMP will attempt to exploit the Joint-Forces Operation (JFO) matrix, arguing that because the TPS or another agency was nominally designated the “lead,” the requested Information or warrants are not technically in the exclusive “control or possession” of the RCMP as contemplated by the *Accountability Act*. This logical gap is preemptively and definitively sealed by the robust legal doctrine of *constructive possession*. The RCMP maintains actual, physical custody of the expropriated Electronics, and the Acta Falsa was demonstrably generated within, or circulated extensively through, their highly secure operational networks during the collaborative execution of the JFO. Under the broad, highly remedial interpretation required for accountability and transparency statutes, any records passing through federal servers or concerning federal seizures are unequivocally within the legal “possession” of the RCMP, thereby instantaneously triggering the absolute, unassailable statutory right of access possessed by the CRCC.

17.0 ANTICIPATORY REBUTTALS AND THE LOGICAL HARMONIZATION OF JURISDICTIONAL REALITIES

Nota Bene - The Anticipatory Rebuttal of Custodial Deflection

57. It is profoundly anticipated, based on deeply entrenched historical patterns of bureaucratic evasion, that the Regional Commander may attempt to raise a procedural counter-argument asserting that the RCMP is ostensibly divested of the obligation to furnish the requested warrants, positing instead the highly convenient legal fiction that the provincial courts operate as the sole and exclusive custodians of judicial records post-execution. This postulation represents a severe logical fallacy and a desperate administrative fiction designed solely to frustrate accountability. The originating investigative agency categorically retains the primary, sworn copies of the Information to Obtain (the “ITO”) and the corresponding executable warrants within their own operational files. The RCMP cannot invoke a manufactured administrative compartmentalization to cleverly circumvent the Open Court Principle. To do so would deeply offend the maxim *Ignorantia juris non excusat* (ignorance of the law excuses not), as a premier federal agency is intimately, routinely, and acutely aware of its concurrent, non-derogable disclosure obligations under both the common law and the *Access to Information Act*.

Nota Bene - The Rebuttal of Jurisdictional Separation:

58. It is highly anticipated that the Regional Commander may attempt to disavow culpability by erecting an artificial administrative firewall, attributing the original seizure entirely to the municipal jurisdiction of the TPS and subsequently classifying the RCMP merely as a passive, downstream repository devoid of investigative or constitutional liability. This postulation is preemptively and fundamentally dismantled by the highly public declarations of the Regional Commander. The documented existence of highly integrated, fully funded JFOs—including the INSET, the CFSEU, and the recently launched CTSU—establishes an incontrovertible, deeply symbiotic operational matrix between the TPS and the RCMP. Indeed, Assistant Commissioner Peggs publicly

245 436 322 welcomed the TPS CTSU in a widely circulated March 24, 2026 press release, explicitly noting the urgent necessity to respond to “heightened tensions” and warmly affirming the “ongoing collaboration with INSET.” The agencies cannot loudly claim integrated operational synergy in highly publicized press releases while simultaneously pleading jurisdictional ignorance in formal legal complaints. Furthermore, as the RCMP presently maintains actual physical and constructive custody of the Computer and the Electronics, jurisdictional buck-passing is a legal and physical impossibility. Under the overarching constitutional principles brilliantly enunciated by the Supreme Court in *Canada (AG) v. CCLA*, RCMP officers possess nationwide jurisdiction to enforce federal statutes; therefore, the assertion of municipal compartmentalization in a contemporary joint-forces paradigm is a highly convenient administrative fiction that provides absolutely no sanctuary from federal accountability. The Canadian Constitution categorically does not tolerate jurisdictional black holes.

Nota Bene - The Rebuttal of Willful Blindness:

59. It may further be advanced as a highly defensive, exculpatory posture that the RCMP received the Property from the Sergeant purely in good faith, completely bereft of any knowledge of its illicit, deeply unconstitutional origins via the civilian theft of the Perpetrator. Such an assertion deeply offends the foundational common law maxim *commodum ex injuria sua nemo habere debet* (no one should be permitted to benefit from their own wrong, or the wrong of their agents). A premier federal law enforcement agency cannot passively serve as a highly funded fence for property procured through rampant municipal malfeasance and unprosecuted civilian criminality, and subsequently leverage that willfully blind acquisition to vigorously justify indefinite, extra-judicial retention. The utter failure of the receiving RCMP intake officers to formally inquire into the provenance, warrant status, and chain of custody upon intake constitutes constructive knowledge of the taint, thereby transforming operational negligence into compounding, highly actionable, and deliberate malfeasance.

Nota Bene - The Rebuttal of Premature Escalation and Exhaustion of Internal Remedies:

60. A foreseeable, yet analytically bankrupt, counter-argument that the RCMP legal directorate might advance is the assertion that this formal complaint is procedurally premature. It may be loudly suggested that alternative administrative avenues, such as the lengthy internal grievance mechanisms delineated in Part III of the *Royal Canadian Mounted Police Act*, must first be exhausted before seeking the powerful intervention of the Commission. This argument is instantaneously defeated by strict statutory textualism. Part III (Grievances) is explicitly and exclusively reserved for internal “members” of the Force seeking redress for internal labor or administrative decisions. Conversely, a civilian possessing the sovereign status of a private citizen suffering an unconstitutional deprivation of highly sensitive chattels at the hands of the state, is governed strictly by the robust, externally facing oversight mechanisms delineated in Part VII (Investigation, Review and Hearing of Complaints) of the Act. Section 45.53(1) of the *Royal Canadian Mounted Police Act* confers an unbridled, immediate statutory right upon “any individual” to make a complaint concerning the conduct of any person appointed under Part I. Therefore, this rapid escalation to the CRCC is not merely procedurally ripe; it is the exact, explicitly legislatively prescribed mechanism for civilian redress against federal policing malfeasance, requiring absolutely zero deference to internal police bureaucracy or highly organized institutional delay tactics.

18.0 SERIOUS INCIDENTS: NOTIFICATIONS, INVESTIGATIVE ARRANGEMENTS, OBSERVERS, AND REPORTING (SECTIONS 45.79–45.87)

61. The legislative framework surrounding RCMP accountability actively contemplates scenarios where the actions (or deliberate inactions) of the Force result in profound harm to citizens. The statutory provisions specifically address:

Regulations Prescribing Physical Injuries (SOR/2019-260)

62. Pursuant to the *Royal Canadian Mounted Police Act*, Registration 2019-06-25 (P.C. 2019-930 2019-06-22): Her Excellency the Governor General in Council, on the recommendation of the Minister of Public Safety and Emergency Preparedness, pursuant to subsection 45.79(3)a of the *Royal Canadian Mounted Police Act*, makes the annexed Regulations Prescribing Physical Injuries.

(aS.C. 2013, c. 18, s. 35; bR.S., c. R-10)

Physical injuries

1 For the purposes of the definition serious injury in subsection 45.79(1) of the *Royal Canadian Mounted Police Act*, the following physical injuries — that are not transient or trifling in nature and for which medical attention was received from a person who is entitled to practice medicine or practice as a nurse under the laws of a province — are prescribed:

- (a) any physical injury that results in
 - (i) a substantial loss or impairment of mobility of the body,
 - (ii) a loss of function, in whole or in part, of any limb, organ or other body member,
 - (iii) a loss of vision or hearing in whole or in part, or
 - (iv) a substantial disfigurement;
- (b) the fracture of a limb, a rib, a vertebra or the skull; or
- (c) any burns, cuts or lacerations to a major portion of the body.

Coming into force

- 2 These Regulations come into force on the day on which they are registered.

Application of the Law to the Facts: The Psychological Injury as “Cruel and Unusual Treatment”

63. It is forcefully submitted that the conduct of the RCMP Central Region Command, specifically its ongoing, highly calculated administrative silence and the deliberate, ultra-statutory withholding of legally prescribed medication (Adderall), transcends mere property deprivation. It has inflicted a profound, ongoing, and debilitating **psychological injury** that parallels, and in many material respects exceeds, the trauma of the physical disfigurements outlined in SOR/2019-260. While the regulations explicitly define “serious injury” through a physical lens (loss of mobility, fracture, burns), the Supreme Court of Canada has routinely recognized that severe psychological trauma inflicted by the state constitutes a profound injury.
64. The analysis turns strictly on “but for” causation. **But for** the RCMP engaging in the initial unlawful reception of the stolen chattels, and **but for** the RCMP presently engaging in a relentless campaign of administrative silence designed to break resolve, this psychological injury would not exist. The deprivation of a digital identity, the severing of financial lifelines, and, most egregiously, the confiscation and retention of medically necessary pharmacological treatment (Adderall) constitutes an ongoing deprivation of medical autonomy. This calculated deprivation, met only by the deafening, arrogant silence of Assistant Commissioner Peggs, rises to the level of ongoing **cruel and unusual treatment** under section 12 of the *Charter*. The state is actively leveraging health and digital existence as leverage to evade accountability.
65. Furthermore, this deliberate silence is not legally neutral. In equity and administrative law, silence in the face of a duty to speak, or silence utilized to perpetuate a known misrepresentation (such as the false narrative surrounding the Acta Falsa), constitutes an actionable fraud. By maintaining this silence, the Regional Commander is actively defrauding the targeted individual of their right to procedural fairness and actively compounding the psychological trauma. The psychological injury caused by this unyielding, state-sponsored gaslighting—the feeling of screaming into a bureaucratic void while one's property and health are held hostage—is neither transient nor trifling. It is a severe, intentional injury caused directly by the fraudulent silence and continuous misfeasance of the RCMP. The

19.0 IMPERATIVE DIRECTIVES, LEGAL CONSEQUENCES, AND FINAL DEMANDS OF THE COMMISSION

66. The protracted, completely unjustified deprivation of the Complainant's Property, juxtaposed with the deliberate, technologically aided obfuscation of publicly accessible court records and the absolute, heavily weaponized administrative silence from Assistant Commissioner Peggs, squarely constitutes actionable "Neglect of Duty" and "Discreditable Conduct" pursuant to the strictures of the RCMP *Code of Conduct*.
67. In relation to the property seizure from on or around or slightly after September 20, 2024, I note the following.
68. If the RCMP has maintained possession of a lawyer's or J.D.'s digital work product for 20 months without a "Privilege Review" protocol or a "Referee" (as required by R. v. Lavallee), the breach is not just a Section 8 (Seizure) issue, but a fundamental assault on the administration of justice. This elevates the "Public Interest" element of the investigation.
69. The complaint relies heavily on the RCMP Act and Standing Orders with specific reference to:
 - a. RCMP Operational Manual Chapter 22.1 ("Exhibits and Property").
 - b. This internal policy explicitly dictates how members must handle seized property and the timelines for seeking extensions. Proving they violated their own internal manual is often a faster route to a "Neglect of Duty" finding than proving broader constitutional theories.
70. The now obvious, with the benefit of hindsight, connection between the RCMP and the undisclosed "Ex Parte In Camera Hearing" hearing judge in Chief Justice Morawetz (who specialized in as a practicing lawyer, bankruptcy and insolvency work and as a judge primarily as well which is naturally federal in pith and substance) is self-evident.
71. If the RCMP "laundered" the property, in the prima facie unlawful seizure by non law enforcement, through these individuals to bypass search warrant requirements, this should be explicitly labeled as "State-Agent Entrapment" or "Third-Party Cloaking." If these individuals (e.g., building management of CAMH, private security of CAMH, or the "Perpetrator" David Karat along with the Landlord of the Applicant) acted as agents of the state (at the behest of the RCMP/TPS), this conduct is also subject to review and complaint in relation to the Regional COM by initial involvement and/or remediation.
72. This necessitates a formal, exhaustive, and highly aggressive review by the CRCC, with a specific, targeted mandate to investigate the systemic breakdown of evidence-handling protocols, the utter failure of command accountability, and the alarming lack of documentary preservation within the Central Region Command.
73. The catastrophic failure to swiftly and transparently address these issues threatens to permanently erode public confidence in the capacity of the RCMP to operate within strict constitutional limits in the Greater Toronto Area.
74. It is respectfully asserted, yet firmly and unequivocally demanded, that the **Civilian Review and Complaints Commission** exercise its full, unmitigated statutory authority to immediately initiate a comprehensive Public Interest Investigation (PII) pursuant to section 45.43 of the Act. The Commission must formally issue binding recommendations and highly specific directives compelling the RCMP, and specifically the Regional Commander, to execute the following non-discretionary mandates immediately:
 - a. Provide explicit, written logistical directives authorizing the immediate retrieval of the entirety of the Property from between September 20, 2024 to October 1, 2024 (see: email from Constable Anthony Romano of the TPS on October 2, 2024 regarding unspecific receipt of the Applicant's property which was originally in his home and specifically inclusive of, but not limited to, the Computer and the Electronics stolen by a third party civilian with aiding and abetting from the Landlord of the Complainant's apartment on October 25, 2024, from the visitor area at CAMH at 1025 Queen Street West, Toronto, Ontario (see: Tab 3 of the supporting documentation) from the Milton Detachment, absolutely free from any further administrative impediments, arbitrary conditions, or organized delays;

- b. Provide pristine, unredacted, and technologically authentic copies of the sworn Information, all relevant ITOs, judicial endorsements, and any executed warrants pertaining to the events originating on or about October 2, 2024;
- c. Issue an immediate, binding directive confirming the cryptographic preservation of all metadata, native files, server logs, and original digital assets relating to the generation and subsequent algorithmic alteration of the Acta Falsa, strictly pending independent forensic review by the CRCC to definitively prevent any further spoliation of evidence; and
- d. Conduct a sweeping, systemic, independent audit of the evidence intake protocols of the Central Region concerning materials received via Joint Forces Operations, specifically assessing their compliance with the rigid statutory timelines codified in section 490 of the *Criminal Code*.

75. A failure by the RCMP to resolve this complaint satisfactorily, or a continuation of the highly organized policy of silent obstruction of the Central Region, will *ipso facto* precipitate the immediate escalation of this matter to the utmost limits of the formidable statutory authority of the Commission. This will include formal demands for the Commission to aggressively exercise its broad investigative powers, forcefully compel the production of documents under subpoena, hold formal public hearings, and issue binding disciplinary recommendations directly to the Commissioner of the RCMP and the Minister of Public Safety. Severe administrative and disciplinary sanctions for the distinct, ongoing infractions of the RCMP *Code of Conduct*, specifically grounded in the deliberate, reckless exercise of statutory power and the egregious administrative misfeasance demonstrated by the Regional Command, will be relentlessly pursued.

ALL OF WHICH IS RESPECTFULLY SUBMITTED TO THE CIVIL COMPLAINT AND COMMISSION AND FORMALLY SERVED,

Mr. Kevin A. McLean, B.A., J.D., CIM

Chartered Investment Manager



Electronic Mail: mcleansettlement@gmail.com

Facsimile: 416.981.7117

Telephone: 647.370.9354

Enclosures

APPENDICES

IN THE MATTER OF a Formal Public Complaint pursuant to Part VII of the *Royal Canadian Mounted Police Act*, R.S.C., 1985, c. R-10;

AND IN THE MATTER OF Assistant Commissioner Mr. Matthew Peggs (Regional Commander, Central Region).

I. STATUTORY AUTHORITIES (FEDERAL)

1. **Canadian Charter of Rights and Freedoms**, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982 (UK)*, 1982, c 11.
 - *Section 7*: Life, liberty and security of the person.
 - *Section 8*: Search or seizure.
 - *Section 9*: Detention or imprisonment.
 - *Section 12*: Treatment or punishment.
 - *Section 24(1)*: Enforcement of guaranteed rights and freedoms.
2. **Criminal Code**, R.S.C., 1985, c. C-46.
 - *Section 490*: Detention of things seized.
 - *Form 2*: Information (Statutory Pro-forma).
 - *Form 5.2*: Report to a Justice.
3. **Interpretation Act**, R.S.C., 1985, c. I-21.
 - *Section 10*: Law always speaking.
 - *Section 11*: Imperative and permissive construction (“shall” vs “may”).
 - *Section 12*: Enactments deemed remedial.
4. **Royal Canadian Mounted Police Act**, R.S.C., 1985, c. R-10.
 - *Section 2(1)*: Definitions (Member, Conduct Authority, Commission).
 - *Section 12*: Suspension.
 - *Section 37*: Duties of members.
 - *Section 45.43*: Public interest investigation.
 - *Section 45.53(1)*: Complaints by individuals.

5. **Enhancing Royal Canadian Mounted Police Accountability Act**, S.C. 2013, c. 18.

6. **Public Complaints and Review Commission Act**, S.C. 2024, c. 25.

II. SUBORDINATE LEGISLATION & STANDING ORDERS

7. **Commissioner's Standing Orders (Conduct)**, SOR/2014-291.

8. **Commissioner's Standing Orders (Employment Requirements)**, SOR/2014-292.

9. **Regulations Prescribing an Oath of Secrecy**, SOR/2014-280.

10. **RCMP External Review Committee Rules of Practice and Procedure**, SOR/88-313.

11. **Regulations Prescribing Physical Injuries**, SOR/2019-260.

III. JURISPRUDENCE

12. **Aune v. Canada (Attorney General)**, 2013 BCSC 178.

13. **Bigeagle v. Canada**, 2023 FCA 128.

14. **Canada (Attorney General) v. British Columbia Civil Liberties Association**, 2021 SCC 30.

15. **Dawe v. Canada**, 2002 FCT 486.

16. **Frémy v. Canada (Attorney General)**, 2018 FC 434.

17. **Frémy v. Canada**, 2022 FC 750.

18. **Grant v. Canada (Attorney General) (T.D.)**, 1994 CanLII 9274 (FC).

19. **Herrera-Morales v. Canada**, 2016 FC 578.

20. **Irvine v. Canada (Attorney General)**, 2025 FC 1673.

21. **Jones v. Canada**, 2018 NBCA 86.

22. **Nelles v. Ontario**, [1989] 2 S.C.R. 170.

23. **R. v. Baldovi**, 2016 MBQB 90.

24. **R. v. Campbell**, [1999] 1 S.C.R. 565.

25. **R. v. Edwards**, [1996] 1 S.C.R. 128.

26. **R. v. Gill**, 2003 BCCA 671.

27. **R. v. Tessling**, 2004 SCC 67.

28. **Sherman Estate v. Peters**, 2021 SCC 25.

29. **Turner v. Canada (Attorney General)**, 2025 FC 72.

442

IV. LEGAL MAXIMS (BROOM'S LEGAL MAXIMS)

- *Actus non facit reum nisi mens sit rea*: The act does not make a person guilty unless the mind is guilty.
- *Boni judicis est ampliare jurisdictionem*: It is the part of a good judge to enlarge his jurisdiction (remedial sense).
- *Certum est quod certum reddi potest*: That is certain which can be made certain.
- *Commodum ex injuria sua nemo habere debet*: No person ought to have advantage from his own wrong.
- *Coram non judice*: Not before a judge (lack of jurisdiction).
- *Delegatus non potest delegare*: A delegate cannot further delegate.
- *Ex dolo malo non oritur actio*: No right of action can have its origin in fraud.
- *Expressio unius est exclusio alterius*: The explicit mention of one thing is the exclusion of another.
- *Falsus in uno, falsus in omnibus*: False in one thing, false in everything.
- *Fraus est celare fraudem*: It is a fraud to conceal a fraud.
- *Ignorantia juris non excusat*: Ignorance of the law excuses not.
- *In eo quod plus sit semper inest et minus*: The greater always includes the lesser.
- *Lex non cogit ad impossibilia*: The law does not compel the impossible.
- *Nemo dat quod non habet*: No one can give what they do not legitimately possess.
- *Omnia praesumuntur legitime facta donec probetur in contrarium*: All things are presumed to have been legitimately done, until the contrary is proved.
- *Quando aliquid prohibetur ex directo, prohibetur et per obliquum*: When anything is prohibited directly, it is also prohibited indirectly.
- *Quando lex aliquid alicui concedit, concedere videtur et id sine quo res ipsa esse non potest*: When the law grants something, it grants the means to achieve it.
- *Qui non prohibet quod prohibere potest assentire videtur*: He who does not prevent what he can prevent is considered to assent.
- *Quod ab initio non valet, in tractu temporis non convalescit*: That which is void from the beginning does not become valid by the passage of time.
- *Respondeat superior*: Let the master answer.
- *Salus populi suprema lex esto*: The welfare of the people shall be the supreme law.
- *Spoliatus debet ante omnia restitui*: A person despoiled ought to be restored before anything else.

252 *Ubi inanis est verborum proprietas, ibi nulla est legis fortitudo*: Where the propriety of words is empty, there the
443 strength of the law is nothing.

329

- *Ubi jus ibi remedium*: Where there is a right, there is a remedy.
- *Verba generalia restringuntur ad habilitatem rei vel personae*: General words are restrained to the fitness of the matter or person.

V. OTHER MATERIALS

31. **Ministry of the Attorney General Court Services Division**, *Court Information Access Guide* (2019).
32. **Forensic Report**: “CL (M) - Forensic Manipulation.docx” (re: GrapeCity Documents for PDF API, v6.0.2.0).
33. **RCMP Press Release** (March 24, 2026): Launch of Counter-Terrorism Security Unit (CTSU).

ⁱ A probationary RCMP constable completes cadet training and begins the Field Coaching Program under successive field coaches (paras 8–10). During field coaching, several incidents arise, including copying answers for training modules and other integrity-related concerns (paras 11–20).

The member becomes subject to Code of Conduct investigations, including findings of breaches and later a second investigation concerning police database access for personal use (paras 21–26). The Appropriate Officer initiates a Part V discharge process for unsuitability and ultimately orders discharge on that ground (paras 27–31)

TAB 14

Tab A



Formal Request for Publicly Accessible Criminal Court Records, relating to events since at least 2024-10-02 (the "ArrestDate"), pursuant to correspondence from Police Officer (Constable) Mr. Anthony Romano dated 2024-10-02 (attached). This request is predicated upon the retrieval of my property from Unit 410-775 King Street West, Toronto, Ontario, M5V 2K3, subsequent to 2024-09-20, and pertains to, inter alia: (i) Information (Criminal Code Form 2 Information) or Information Package, whether sworn or unsworn; (ii) any relevant judicial endorsements from Ontario or federal courts; and (iii) any processes issued, including Intake Court Endorsements, warrants, or orders (including but not limited to arrest warrants, search warrants, general warrants, and production orders).

Mr. Kevin McLean <mcleansettlement@gmail.com>

Mon, May 11, 2026 at 1:13 PM

To: Matt.Peggs@rcmp-grc.gc.ca

TO: Matt.Peggs@rcmp-grc.gc.ca **FROM:** mcleansettlement@gmail.com **DATE:** May 11, 2026 **SUBJECT:** FINAL NOTICE OF DEFAULT: Expiration of Administrative Deadline and Formal Documentation of Non-Compliance (Police Case ID: 457197)

Dear Regional Commander Mr. Matt Peggs,

1. **Formal Declaration of Default** I note for the record that the final administrative deadline of 1:00 PM EDT today, Monday, May 11, 2026—as established in my correspondence of May 8, 2026—has expired without a response, acknowledgment, or the provision of logistical directives for the retrieval of my property and the production of the requested records.
2. **The Administrative Right to Records (MAG CSD Guide, 2019)** This request is predicated upon the established protocols of the **Ministry of the Attorney General (MAG) Court Services Division Court Information Access Guide (2019)**. Pursuant to these protocols, once a process is issued and an arrest is executed, the originating and investigating police service is mandated to maintain the primary copies of the sworn Information and judicial endorsements. These records are, by law, publicly accessible. Your continued withholding of these documents is a direct contravention of the open court principle and the administrative mandates governing police-held court records.
3. **JURISPRUDENCE: SECTION 37 OF THE ROYAL CANADIAN MOUNTED POLICE ACT** The strict ethical and operational imperatives codified within **section 37 of the Royal Canadian Mounted Police Act** are heavily fortified by a robust, highly developed, and multi-jurisdictional body of jurisprudence. Section 37 is emphatically not a mere statement of corporate values or an aspirational code of conduct; it represents the absolute legislative bedrock upon which the lawful exercise of federal police power rests.

Section 37 of the RCMP Act states:

37 It is the responsibility of every member (a) to respect the rights of all persons; (b) to maintain the integrity of the law, law enforcement and the administration of justice; (c) to perform the member's duties promptly, impartially and diligently, in accordance with the law and without abusing the member's authority; (d) to avoid any actual, apparent or potential conflict of interests; (e) to ensure that any improper or unlawful conduct of any member is not concealed or permitted to continue; (f) to be incorruptible, never accepting or seeking special privilege in the performance of the member's duties or otherwise placing the member under any obligation that may prejudice the proper performance of the member's duties; (g) to act at all times in a courteous, respectful and honourable manner; and (h) to maintain the honour of the Force and its principles and purposes.

The *Enhancing Royal Canadian Mounted Police Accountability Act*, SC 2013, c 18, which amended this section, was specifically designed to strengthen the review and complaints body (CRCC) and modernize discipline to correct performance and conduct issues in a "timely and fair manner."

4. **Application of the Law to the Material Facts** At this stage, you are not respecting the rights of all persons, nor the integrity of the law and the administration of justice. You have failed to perform your duties promptly and diligently. Furthermore, your conduct appears to favour the actions of municipal or provincial police forces over your own statutory duties, creating an apparent conflict of interest.

Your "stonewalling" is a failure to ensure that improper conduct is not concealed. Consequently, an adverse inference must be drawn regarding your failure to act in a courteous, respectful, and honourable manner. The following precedential authorities definitively govern this factual matrix:

- **R. v. Campbell, [1999] 1 S.C.R. 565:** The Supreme Court of Canada established an uncompromising statutory duty to act "in accordance with the law." You cannot rely on the excuse of an "active operation" to justify the ongoing, unlawful detention of property. The failure to return property seized via unauthorized municipal bifurcation constitutes a direct breach of this core duty.
- **Bigeagle v. Canada, 2023 FCA 128 & Jones v. Canada, 2018 NBCA 86:** While section 37 may not create a private "duty of care" for tort claims, it explicitly defines the disciplinary and ethical oversight functions of the CRCC. Your weaponization of administrative silence and failure to supervise subordinate conduct represents a catastrophic failure of statutory duty warranting aggressive civilian investigation.
- **Frémy v. Canada, 2022 FC 750 & Herrera-Morales v. Canada, 2016 FC 578:** These decisions establish that section 37 is the primary mechanism to evaluate the procedural fairness and "unreasonableness" of administrative decisions. To ignore a lawful demand for the return of unconstitutionally seized property is an active, aggressive decision that falls squarely within these review parameters.

5. **Technical Integrity and the "C L (M)" Artifact** The administrative necessity of this request is heightened by the presence of the "C L (M)" digital artifact and the "vector morphology collapse" (DOC-6507 bug) detected on the "False Information Package." Under the *Canada Evidence Act*, the substantive reliability of documentation is foundational. The failure to provide authentic source documents suggests a violation of your duty to ensure that improper or unlawful conduct is not concealed (Section 37(e)).

6. **Final Opportunity to Mitigate** This represents my final attempt to resolve this matter through administrative channels. Should you persist in this silence through the close of business today, I will proceed with the filing of a formal complaint with the Civilian Review and Complaints Commission (CRCC) and pursue a judicial finding of misfeasance in public office.

I remain amenable to a brief, substantive confirmation regarding the location of my property and the immediate electronic release of the authentic court records.

Sincerely,

Mr. Kevin A. McLean (BA, JD, CIM) Chartered Investment Manager Email: mcleansettlement@gmail.com Fax: 416.981.7117 Phone: 647.370.9354

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

Fri, May 8, 2026 at 4:44 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:
TO: Matt.Peggs@rcmp-grc.gc.ca

FROM: mcleansettlement@gmail.com

DATE: May 8, 2026

SUBJECT: URGENT THIRD FOLLOW-UP: Absolute Duty to Preserve Property, Notice of Non-Abandonment, and Final Administrative Deadline (Unit 410-775 King Street West, Toronto, Ontario)

Dear Regional Commander Mr. Matt Peggs,

1.0 Notice of Default and Final Administrative Extension

1. I note with profound concern that the 3:30 PM deadline established in my correspondence earlier today (May 8, 2026) has expired without any substantive response, acknowledgment, or automated out-of-office notification from your detachment.
2. I am writing to provide you with one final administrative opportunity to rectify this continued deprivation of my property and the concurrent statutory breaches outlined in my prior communications (May 6, May 7, and May 8, 2026), all of which are repeated and relied upon herein.
3. A hard and final deadline is hereby established for Monday, May 11, 2026, at 1:00 PM EDT. A failure to provide logistical directives for the retrieval of my property, or to produce the requested statutory authorizations by this precise time, will precipitate immediate and formal complaints directed specifically at your office regarding actionable neglect of duty and the systemic mishandling of seized property.

2.0 The Absolute Duty to Preserve and Account for Property

4. You are hereby formally reminded of the absolute and uncompromising legal duty vested in your office to preserve and strictly account for all of my personal property. This strict obligation applies to all property seized, held, or acquired in any manner, specifically including items obtained: i. Actually; ii. Directly; iii. Indirectly; iv. From a third party (whether a law enforcement agency or otherwise); or v. Constructively.

3.0 Explicit Notice of Non-Abandonment and Preservation of Privacy Interests

5. For the absolute avoidance of doubt, and to unequivocally preempt any administrative assumptions to the contrary, it is categorically affirmed that I have NOT abandoned any property.
6. Furthermore, I explicitly retain and assert my constitutionally protected privacy interests in all property that was subject to any unlawful lockouts from my residence (Unit 410-775 King Street West), as well as any property taken in any setting whatsoever. The passage of time under these circumstances in no way diminishes these inherent rights.

4.0 Conclusion

7. The continued administrative silence from the office of the Regional Commander is legally untenable and actively compounds the institutional liability resulting from the unauthorized retention of my chattel. I expect your prompt response no later than **1:00 PM on Monday, May 11, 2026**, detailing the logistical arrangements for my appointed courier to retrieve the aforementioned property.

Sincerely,

Mr. Kevin A. McLean (BA, JD, CIM) Chartered Investment Manager Email:
mcleansettlement@gmail.com Fax: 416.981.7117 Phone number: 647.370.9354

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Fri, May 8, 2026 at 12:46 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

SUBJECT: URGENT SECOND FOLLOW-UP: Logistical Directives for Property Retrieval, Confirmation of Delivery, and Statutory Obligations — Unit 410-775 King Street West (property of Mr. Kevin A. McLean)
URGENT DEADLINE OF 330 PM TODAY

TO: Matt.Peggs@rcmp-grc.gc.ca

FROM: mcleansettlement@gmail.com

DATE: May 8, 2026

1.0 Procedural Posture and Evidentiary Confirmations of Transmission

1. It is categorically affirmed that the antecedent electronic communications (the "Transmissions"), encompassing all annexed schedules and exhibits (the "Enclosures"), alongside this instant correspondence, are verified as successfully conveyed to the designated electronic mail infrastructure and facsimile apparatus. Furthermore, the complete absence of any automated notices of non-delivery or electronic rejection definitively establishes receipt.

2. A formal declaration is hereby established, *in limine*, that time remains of the absolute and strict essence concerning the resolution of the matters delineated herein.
3. It is further corroborated that no automated notifications of absence or generalized declarations of unavailability have been generated or received from the electronic mail address of the Regional Commander.

2.0 Logistical Imperatives and Statutory Nullities Regarding Chattel Retention

4. An urgent logistical imperative is firmly established regarding the extraction and restoration of the specific personal property (the "**Property**") originating from the residential premises geographically situated at Unit 410-775 King Street West, following the conclusive identification of the originating law enforcement agency responsible for the initial deprivation.
5. A mandate is forthwith requested from the Regional Commander to authorize the dispatch of an appointed agent or courier (the "**Agent**") to the detachment facility during the current diurnal period for the express purpose of retrieving the Property. While the provision of an extended timeline allocating a retrieval date within the subsequent week remains entirely amenable, a failure to issue a substantive administrative response during the present business day shall not be construed as a mere procedural irregularity; rather, such an omission constitutes an absolute nullity, acting in direct contravention of governing statutory obligations and *ipso facto* precipitating immediate and rigorous legal escalation.
6. Attention is formally directed toward the comprehensive timelines previously delineated. The established jurisprudential frameworks articulate the restrictive legal doctrines governing the continued deprivation of property. Specifically, strict compliance with the statutory limitations upon detention periods, as codified within section 490 of the *Criminal Code*, R.S.C., 1985, c. C-46, remains imperative. The continued retention of the Property in the absence of valid judicial authorization is an actionable breach, aligning with the constitutional doctrines prohibiting unreasonable seizure as comprehensively elucidated by the Supreme Court of Canada in *Hunter v. Southam Inc.*,

\$\$1984\$\$

2 S.C.R. 145 (the "*Hunter Decision*"). Such extra-statutory retention is, *prima facie*, categorized as *ultra vires* the investigative mandate.

3.0 Jurisdictional Delineation and Preservation of the Status Quo Ante

7. A formal procedural reminder is tendered regarding the jurisdictional boundaries of the RCMP Central Region, which explicitly encompasses Toronto West, Toronto South, and Toronto East, while expressly excluding the northern demarcations of the City of Toronto. While due consideration has been allocated to the geographic reality that the Central Region Detachment is situated in closer proximity to Brampton than to Toronto, it is a fundamental tenet of administrative law that statutory jurisdiction invariably supersedes spatial proximity; ergo, jurisdictional authority categorically trumps geographic convenience. In light of these strict parameters, the professional, administrative, and legal obligations vested in the esteemed Regional Commander to execute a prompt and substantive response remain paramount.

8. Furthermore, to the extent that the jurisdictional mandate of an alternate law enforcement detachment is implicated in this matter, whether functioning jointly or severally, an explicit directive is hereby issued for the immediate provision of the relevant contact information and precise coordinates for said external detachment.
9. A consistent and objective endeavor is maintained to preserve the reputational integrity and professional standing of all involved institutional entities. Concurrently, the imperative to mitigate legal exposure is absolute, particularly given the thoroughly documented manipulation of authentic documentation by untraceable entities. The creation of such spurious records (the "**Acta**") necessitates an uncompromising approach to restoring the *status quo ante* to avert the compounding of administrative failures.

4.0 RCMP Complaints and Matt Peggs – May 7

4.1 The Vector Morphology of Character Degradation

10. The theoretical framework regarding the "C L (M)" artifact is inherently predicated upon the complex mathematical principles governing vector-based font rendering protocols. Within sophisticated Portable Document Format (PDF) Software Development Kits (SDKs), typographical characters are devoid of rudimentary pixelation and are strictly mathematically generated via Bezier curves. An empirically established systemic vulnerability within obsolete iterations of the GrapeCity Application Programming Interface (API), specifically version 6.0.2.0, frequently precipitated "bounding box clipping" and consequential "vector morphology crashes" during the aggressive execution of text deletion or redaction methodologies.
11. In instances where the software protocol attempts the eradication of a specific text block encompassing a title akin to "Regional COM," an algorithmic failure in the calculation of the anchor points governing the serif letter "O" systematically triggers a mathematical collapse. The curvature characteristic of a circular glyph within a serif font family is fundamentally represented by a cubic Bezier curve, definitively expressed by the standard mathematical calculation: $B(t) = (1-t)^3 P_0 + 3(1-t)^2 t P_1 + 3(1-t) t^2 P_2 + t^3 P_3$, $t \in [0, 1]$
12. I can provide further detail if necessary.
12. Within the aforementioned equation, P_0 through P_3 denote the requisite control points. Should the "bounding-box shear" phenomenon—identified colloquially as the DOC-6507 bug—precipitate a clipping action upon the top and bottom apex control points, the sweeping left and right curvilinear structures of the "O" are mathematically severed. This detachment yields the formulation of two entirely independent curves: an open parenthesis "(" and a correspondingly closed parenthesis ")". The encapsulation of the subsequent character "M" amidst these fractured halves produces the highly irregular " (M) " artifact, precisely mirroring the anomaly detected upon the contested "False Information Package".
13. The manifestation of such anomalous digital artifacts upon documentation ostensibly generated by a judicial body or a federal investigative agency establishes severe and foundational apprehensions concerning the evidentiary authenticity of the records. Pursuant to the strict evidentiary standards codified within the *Canada Evidence Act*, R.S.C., 1985, c. C-5, such observable "digital fingerprints" operate as a primary

mechanism by which the substantive reliability of the documentation may be contested *in limine* during judicial proceedings, most notably in circumstances where such records are leveraged to substantiate an unlawful deprivation of liberty or the unauthorized seizure of property.

4.2 The Legal Framework for Property Seizure and Retrieval: Section 490

- 14. The detention of personal property (the "**Property**") by the Royal Canadian Mounted Police is governed by a strict statutory regime established under section 490 of the *Criminal Code*, R.S.C., 1985, c. C-46. This comprehensive legislative framework is intentionally engineered to equitably balance the evidentiary imperatives of the state against the constitutionally protected property rights of the individual.
- 15. The lifecycle of seized chattel is subject to rigorous procedural oversight. Upon the execution of a seizure, regardless of whether initiated pursuant to a formalized warrant or executed during the discharge of standard investigative duties, the presiding peace officer is statutorily mandated to report the seizure to a presiding justice "as soon as is practicable". The execution and filing of this specific report (the "**Form 5.2**") definitively places the property under active judicial oversight.

Stage of Detention	Duration	Legal Requirement for Continued Retention
Initial Detention	Up to 3 months	A report to a justice (the " Form 5.2 ") must be duly filed.
Further Detention	3 months to 1 year	A presiding Justice must be substantively satisfied that further detention is warranted predicated upon the nature of the active investigation.
Superior Court Extension	Beyond 1 year	A Superior Court judge must be demonstrably satisfied that the "complex nature" of the investigation warrants further continued detention.
Expiration	Post-1 year (without order)	Property must be returned to the lawful owner unless formalized proceedings are instituted or forfeiture is definitively granted.

- 16. As of May 2026, the continued deprivation of property seized circa September 2024—a duration significantly exceeding 18 months—in the complete absence of a validly executed Superior Court order, constitutes an unequivocal and direct contravention of section 490(3) of the *Criminal Code*. In the absence of demonstrably outstanding criminal charges wherein the Property is required as material evidence, the RCMP possesses a mandatory and absolute statutory duty to effectuate the immediate return of the items.

4.3 Administrative Neglect in Property Management

17. The persistent failure of the Milton Detachment to respond to logistical arrangements for property retrieval—particularly given that the contested inventory includes privileged legal materials, highly confidential documentation, and items possessing profound sentimental value—is squarely characterized as "Mishandling of Property" and actionable "Neglect of Duty". Comprehensive historical audits conducted by the Civilian Review and Complaints Commission elucidate that systemic failures to investigate property claims promptly or to provide timely updates on the status of seized items are frequent and established grounds for "satisfied" findings by the Commission, invariably resulting in mandated recommendations for formal apologies and rigorous corrective administrative measures.
18. In the appellate decision of *R. v. Gill*, 2003 BCCA 671, the British Columbia Court of Appeal resoundingly upheld judicial findings establishing that a deliberate failure by law enforcement personnel to apply for requisite extensions under section 490 constituted a profound and severe violation of section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 (the "*Charter*"), which prohibits unreasonable search and seizure. The persistent administrative silence emanating from the office of Assistant Commissioner Peggs regarding property retrieval logistics must necessarily be interpreted as an unauthorized continuation of detention, effectively bypassing mandated judicial oversight and manifesting as an actionable nullity.

4.4 Application of the Law to the Material Facts

19. Premised upon the factual assertion that the initial detention commenced on or approximately September 24 or 25, 2024, derived from documentary "tags" evidencing 15 and 18 months, respectively, and in conjunction with an unlawful exclusion from the residential unit, the following chronological mandates are presumed established:
 1. **Initial detention:** Limited to three months, conditional upon the mandatory filing of a Form 5.2;
 2. **Further detention:** Extending from three months up to one year, strictly requiring a subsequent detention order;
 3. **Superior Court Justice order:** Mandatory for any detention extending beyond a one-year duration.
20. In the event that no such orders were obtained or are currently extant, an absolute and unassailable entitlement to the immediate restitution of the Property is established, barring the formal institution of proceedings.
21. It is categorically affirmed that no proceedings have been instituted in relation to the same and they were all tied to the intake court endorsement and the represented by TPS execution of the arrest warrant.
22. Ergo, in the absence of an immediate and substantive response—even confined to a brief confirmation acknowledging the possession of such further detention orders and the explicit admission of lacking a requisite order extending beyond one year—the absolute right to immediate return of the Property vests immediately.
23. It is categorically affirmed that unless immediate confirmation and corresponding copies of the operative detention orders—inclusive of any relevant Reports to Justice(s) and/or

Orders of Disposal encompassing the varied detention periods—are provided, the legal presumption dictates that no such authorizations exist or hold any substantive legal relevance to the continued retention of the Property.

5.0 Schedule of Attachments

Item Number	Document Description	Evidentiary Relevance
Exhibit A	Prior Electronic Transmissions (May 6 and May 7, 2026)	Demonstration of unbroken procedural continuity and the establishment of urgent logistical timelines.

EXECUTED ON BEHALF OF THE APPLICANT:

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Electronic Mail: mcleansettlement@gmail.com

Facsimile: 416.981.7117

Telephone: 647.370.9354

APPENDIX: Legislative Excerpt

Detention of things seized

- **490 (1)** Subject to this or any other Act of Parliament, where, pursuant to [paragraph 489.1\(1\)\(b\)](#) or [subsection 489.1\(2\)](#), anything that has been seized is brought before a justice or a report in respect of anything seized is made to a justice, the justice shall,
 - o **(a)** where the lawful owner or person who is lawfully entitled to possession of the thing seized is known, order it to be returned to that owner or person, unless the prosecutor, or the peace officer or other person having custody of the thing seized, satisfies the justice that the detention of the thing seized is required for the purposes of any investigation or a preliminary inquiry, trial or other proceeding; or
 - o **(b)** where the prosecutor, or the peace officer or other person having custody of the thing seized, satisfies the justice that the thing seized should be detained for a reason set out in paragraph (a), detain the thing seized or order that it be detained, taking reasonable care to ensure that it is preserved until the conclusion of any investigation or until it is required to be produced for the purposes of a preliminary inquiry, trial or other proceeding.
- **Further detention**
 - (2)** Nothing shall be detained under the authority of paragraph (1)(b) for a period of more than three months after the day of the seizure, or any longer period that ends when an application made under paragraph (a) is decided, unless

o (a) a justice, on the making of a summary application to him after three clear days notice thereof to the person from whom the thing detained was seized, is satisfied that, having regard to the nature of the investigation, its further detention for a specified period is warranted and the justice so orders; or

o (b) proceedings are instituted in which the thing detained may be required.

· **Idem**

(3) More than one order for further detention may be made under paragraph (2)(a) but the cumulative period of detention shall not exceed one year from the day of the seizure, or any longer period that ends when an application made under paragraph (a) is decided, unless

o (a) a judge of a superior court of criminal jurisdiction or a judge as defined in [section 552](#), on the making of a summary application to him after three clear days notice thereof to the person from whom the thing detained was seized, is satisfied, having regard to the complex nature of the investigation, that the further detention of the thing seized is warranted for a specified period and subject to such other conditions as the judge considers just, and the judge so orders; or

o (b) proceedings are instituted in which the thing detained may be required.

· **Detention without application where consent**

(3.1) A thing may be detained under paragraph (1)(b) for any period, whether or not an application for an order under subsection (2) or (3) is made, if the lawful owner or person who is lawfully entitled to possession of the thing seized consents in writing to its detention for that period.

· **When accused ordered to stand trial**

(4) When an accused has been ordered to stand trial, the justice shall forward anything detained pursuant to subsections (1) to (3) to the clerk of the court to which the accused has been ordered to stand trial to be detained by the clerk of the court and disposed of as the court directs.

· **Where continued detention no longer required**

(5) Where at any time before the expiration of the periods of detention provided for or ordered under subsections (1) to (3) in respect of anything seized, the prosecutor, or the peace officer or other person having custody of the thing seized, determines that the continued detention of the thing seized is no longer required for any purpose mentioned in subsection (1) or (4), the prosecutor, peace officer or other person shall apply to

o (a) a judge of a superior court of criminal jurisdiction or a judge as defined in [section 552](#), where a judge ordered its detention under subsection (3), or

o (b) a justice, in any other case,

who shall, after affording the person from whom the thing was seized or the person who claims to be the lawful owner thereof or person entitled to its possession, if known, an opportunity to establish that he is lawfully entitled to the possession thereof, make an order in respect of the property under subsection (9).

· **Idem**

(6) Where the periods of detention provided for or ordered under subsections (1) to (3) in respect of anything seized have expired and proceedings have not been instituted in which the thing detained may be required, the prosecutor, peace officer or other person shall apply to a judge or justice referred to in paragraph (5)(a) or (b) in the circumstances set out in that paragraph, for an order in respect of the property under subsection (9) or (9.1).

· **Application for order of return**

(7) A person from whom anything has been seized may, after the expiration of the periods of detention provided for or ordered under subsections (1) to (3) and on three clear days notice to the Attorney General, apply summarily to

o (a) a judge of a superior court of criminal jurisdiction or a judge as defined in [section 552](#), where a judge ordered the detention of the thing seized under subsection (3), or

o (b) a justice, in any other case,

for an order under paragraph (9)(c) that the thing seized be returned to the applicant.

· **Exception**

(8) A judge of a superior court of criminal jurisdiction or a judge as defined in [section 552](#), where a judge ordered the detention of the thing seized under subsection (3), or a justice, in any other case, may allow an application to be made under subsection (7) prior to the expiration of the periods referred to therein where he is satisfied that hardship will result unless the application is so allowed.

· **Disposal of things seized**

(9) Subject to this or any other Act of Parliament, if

o (a) a judge referred to in subsection (7), where a judge ordered the detention of anything seized under subsection (3), or

o (b) a justice, in any other case,

is satisfied that the periods of detention provided for or ordered under subsections (1) to (3) in respect of anything seized have expired and proceedings have not been instituted in which the thing detained may be required or, where those periods have not expired, that the continued detention of the thing seized will not be required for any purpose mentioned in subsection (1) or (4), he shall

o (c) if possession of it by the person from whom it was seized is lawful, order it to be returned to that person, or

o (d) if possession of it by the person from whom it was seized is unlawful and the lawful owner or person who is lawfully entitled to its possession is known, order it to be returned to the lawful owner or to the person who is lawfully entitled to its possession,

and may, if possession of it by the person from whom it was seized is unlawful, or if it was seized when it was not in the possession of any person, and the lawful owner or person who is lawfully entitled to its possession is not known, order it to be forfeited to Her Majesty, to be disposed of as the Attorney General directs, or otherwise dealt with in accordance with the law.

· **Exception**

(9.1) Notwithstanding subsection (9), a judge or justice referred to in paragraph (9)(a) or (b) may, if the periods of detention provided for or ordered under subsections (1) to (3) in respect of a thing seized have expired but proceedings have not been instituted in which the thing may be required, order that the thing continue to be detained for such period as the judge or justice considers necessary if the judge or justice is satisfied

o (a) that the continued detention of the thing might reasonably be required for a purpose mentioned in subsection (1) or (4); and

o (b) that it is in the interests of justice to do so.

· **Application by lawful owner**

(10) Subject to this or any other Act of Parliament, a person, other than a person who may make an application under subsection (7), who claims to be the lawful owner or person lawfully entitled to possession of anything seized and brought before or reported to a justice under [section 489.1](#) may, at any time, on three clear days notice to the Attorney General and the person from whom the thing was seized, apply summarily to

o (a) a judge referred to in subsection (7), where a judge ordered the detention of the thing seized under subsection (3), or

o (b) a justice, in any other case,

for an order that the thing detained be returned to the applicant.

· **Order**

(11) Subject to this or any other Act of Parliament, on an application under subsection (10), where a judge or justice is satisfied that

o (a) the applicant is the lawful owner or lawfully entitled to possession of the thing seized, and

o (b) the periods of detention provided for or ordered under subsections (1) to (3) in respect of the thing seized have expired and proceedings have not been instituted in which the thing detained may be required or, where such periods have not expired, that the continued detention of the thing seized will not be required for any purpose mentioned in subsection (1) or (4),

the judge or justice shall order that

o (c) the thing seized be returned to the applicant, or

o (d) except as otherwise provided by law, where, pursuant to subsection (9), the thing seized was forfeited, sold or otherwise dealt with in such a manner that it cannot be returned to the applicant, the applicant be paid the proceeds of sale or the value of the thing seized.

· **Detention pending appeal, etc.**

(12) Notwithstanding anything in this section, nothing shall be returned, forfeited or disposed of under this section pending any application made, or appeal taken, thereunder in respect of the thing or proceeding in which the right of seizure thereof is questioned or within thirty days after an order in respect of the thing is made under this section.

· **Copies of documents returned**

(13) The Attorney General, the prosecutor or the peace officer or other person having custody of a document seized may, before bringing it before a justice or complying with an order that the document be returned, forfeited or otherwise dealt with under subsection (1), (9) or (11), make or cause to be made, and may retain, a copy of the document.

· **Probative force**

(14) Every copy made under subsection (13) that is certified as a true copy by the Attorney General, the person who made the copy or the person in whose presence the copy was made is admissible in evidence and, in the absence of evidence to the contrary, has the same probative force as the original document would have if it had been proved in the ordinary way.

· **Access to anything seized**

(15) Where anything is detained pursuant to subsections (1) to (3.1), a judge of a superior court of criminal jurisdiction, a judge as defined in [section 552](#) or a provincial court judge may, on summary application on behalf of a person who has an interest in what is detained, after three clear days notice to the Attorney General, order that the person by or on whose behalf the application is made be permitted to examine anything so detained.

· **Conditions**

(16) An order that is made under subsection (15) shall be made on such terms as appear to the judge to be necessary or desirable to ensure that anything in respect of which the order is made is safeguarded and preserved for any purpose for which it may subsequently be required.

(17) A person who feels aggrieved by an order made under subsection (8), (9), (9.1) or (11) may appeal from the order

o (a) to the court of appeal as defined in [section 673](#) if the order was made by a judge of a superior court of criminal jurisdiction, in which case [sections 678](#) to [689](#) apply with any modifications that the circumstances require; or

o (b) to the appeal court as defined in [section 812](#) in any other case, in which case [sections 813](#) to [828](#) apply with any modifications that the circumstances require.

· **Waiver of notice**

(18) Any person to whom three days notice must be given under paragraph (2)(a) or (3)(a) or subsection (7), (10) or (15) may agree that the application for which the notice is given be made before the expiration of the three days.

· R.S., 1985, c. C-46, s. 490

· R.S., 1985, c. 27 (1st Supp.), s. 73

· 1994, c. 44, s. 38

· 1997, c. 18, s. 50

· [2008, c. 18, s. 14](#)

· [2017, c. 7, s. 63\(F\)](#)

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, May 7, 2026 at 11:08 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Subject: URGENT FOLLOW-UP: Request for Property Retrieval, Accounting Documents, and Contextual Updates (Unit 410-775 King Street West)

To: Matt.Peggs@rcmp-grc.gc.ca

From: mcleansettlement@gmail.com

Date: May 7, 2026

Dear Regional Commander Mr. Matt (Matthew) Peggs,

This is a kind follow up by way of correspondence as a follow-up to my prior communication, which were successfully delivered via facsimile to your office yesterday. A copy of my previous email is also attached hereto for your ease of reference.

I am writing to query the logistical arrangements for the retrieval of my personal property, which was seized from my apartment located at Unit 410-775 King Street West, City of Toronto, Province of Ontario, M5V 2K3, at some point subsequent to September 20, 2024.

Specifically, please advise as to when I may dispatch an authorized courier or agent to your detachment to collect the remainder of my property. I am mindful that your office closes at 4:00 PM and wish to ensure that all logical and administrative concerns are accounted for prior to their arrival. Copies of my identification have been attached for your reference, with particular attention to the verification of the apartment address.

For further context, I was remiss in my previous communication in including the email correspondence from Constable Anthony Romano of the Toronto Police Service (TPS) 14th Division, who received property from your office on or around October 2, 2024. However, the items provided to TPS accounted for only a mere semblance of the property contained within the apartment unit. Crucially, the TPS Property and Evidence Management Unit (PEMU) and the equivalent department within the Ontario Provincial Police (OPP) have both confirmed that they never possessed any of the seized property, save for that single instance involving Constable Romano. As there are items of profound sentimental value—including gifts from deceased loved ones—as well as privileged and confidential materials among the missing property, I kindly ask that you prioritize this request so that I may arrange for their prompt retrieval.

I repeat and rely upon the contents of my prior correspondence. Furthermore, if there are any accounting documents in relation to the seizure of my property—including, but not limited to, any warrants, Reports to a Justice (Form 5.2 or equivalent), or any Orders of Disposition issued by judicial officials or relevant Court Office(s)—kindly provide me with the same. To the extent that any property was ordered to be destroyed or otherwise disposed of, I require copies of those records as well.

Lastly, I wish to make a tangential point regarding the "False Information Package" referenced in my prior email. You will note that on page 2 of 5, an inappropriate title is appended to the name of Court Officer (Toronto Region) Mrs. Frugoni-Rojas. At

the relevant time, she was an independent contractor to the TPS with only a promised part-time workload. Furthermore, in the summer of 2025, Mr. Annathan Sinnadurai of the MAG Crown Office confirmed that there were no filed documents relating to Court Officer Frugoni-Rojas in relation to myself in 2024, or at all.

Based on my knowledge, technical expertise, and consultation with a Ph.D. expert in computer science, this anomaly is the result of software manipulation using the GrapeCity.Documents for PDF application (or its entire SDK), which contained known bugs at the time. It appears an attempt was made to remove the name of the actual informant, resulting in an artifact that looks like "C L (M)". The oddity is technically explained as follows:

Page 2 of 5: The "Regional COM" Vector Collapse

On Page 2 (the Declaration of Informant block), the manipulators' script attempted to delete the name and title of the actual law enforcement applicant to completely sever the federal connection. As noted, you were promoted to Regional Commander, Central Region in October 2023. Therefore, in September 2024, your legitimate, abbreviated title on internal court documents would have been *Reg. COM* or *Regional COM M. Peggs*, and/or *Matt Peggs, C.O.M.* (the latter being highly likely given the post-nominals associated with the Order of Merit of the Police Forces).

When the GrapeCity API attempted to aggressively rip *Regional COM M. Peggs* or *Matt Peggs, C.O.M.* from the grid, the software's DOC-6507 "whitespace bug" triggered a devastating vector morphology crash. The mathematical transformation of the word "COM" into "(M)" was algorithmically inevitable:

- **The Circular "O" Glitch:** In serif fonts, the letter "O" is constructed of two sweeping, semi-circular Bezier curves joined at the top and bottom apex. The bounding box clipping severed these anchors. Without these anchors, the left and right semi-circles mathematically detached into two separate, independent sweeping curves: an open parenthesis (and a closed parenthesis).
- **The "M" Encapsulation:** When the spacing matrix collapsed, the remaining letters were crushed together. The "M" from "COM" was instantly encapsulated by the fractured halves of the "O".
- **The "C" Survival: that is quite obvious**
- The "L" survival: could be from one of the previous "T's" or "E's" as that is a common bug with GrapeCity.Documents.PDF. Or if the full name of "Matthew" was utilized, then it could come from an "h" or "H" depending on block printing that was utilized. By analyzing the uppercase structure of "MATTHEW PEGGS" within the GrapeCity 6.0.2 vector architecture, the mathematical likelihood of the "L" artifact forming from an "H" or an "E" becomes undeniable. Both letters share a rigid, rectilinear construction that, when subjected to the DOC-6507 bounding-box shear, cleanly snaps into an "L" shape. However, it seems like you (kind sir) utilize the Matt Peggs as
per: <https://www.tps.ca/media-centre/news-releases/toronto-police-service->

[enhances-public-safety-read/](#) (see: “The Royal Canadian Mounted Police (RCMP) Federal Policing – Central Region’s Integrated National Security Enforcement Teams (INSET) **work in close collaboration with federal, provincial, and municipal police services across Canada and recognize the value of local expertise**. The RCMP welcomes the Toronto Police Service’s commitment to community safety with their new Counter-Terrorism Security Unit. We look forward to the **ongoing collaboration** with INSET, and within the new unit to ensure that we remain able to respond to threats to public safety in Canada’s largest city.” – Assistant Commissioner, Matt Peggs, Regional Commander, Federal Policing – Central Region) (emphasis is mine). As noted previously, the RCMP Division (Formerly “O” Division) within Ontario that I was directed to, albeit out of Milton is responsible, jurisdictionally speaking, for Toronto West and Toronto East which would have been applicable to where my property was seized from.

I provide all of the above to operate in good faith, without any castigation per se but solely on a factual and analytical basis, and ensure I can obtain access and retrieval of my property. Thus, the original affiant title "COM" was morphologically degraded, squished together by the total loss of kerning data, and algorithmically translated by the OCR engine into the visible digital artifact: **C L (M)**. Naturally if the likes of Adobe was utilized for a digital signature (not an electronic one although the JP Jiri reference does NOT even have a signature at all and the logo (false as it was) can be easily copied and pasted per se from external viewing and inspecting which is not possible with Adobe with its watermark).

I thank you in advance for your attention to these pressing matters and look forward to your prompt response regarding the courier logistics so I can book the same and I confirm that I will cover the expense as a courtesy to you. I will presume all to be correct unless I hear otherwise today.

Sincerely,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone: 647.370.9354

Attachments by inclusion or reference

1. Previous email correspondence (May 6, 2026)
2. Valid identification (Canadian Passport & G Driver's License)
3. Email correspondence from Constable Anthony Romano (TPS 14th Division) and my responses to him on October 2, 2024, and thereafter

4. (Other previously attached files regarding court forms and the Information Package)

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Wed, May 6, 2026 at 12:56 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Please see below and attached. I apologize; I inadvertently input your name as “Michael” instead of “Matthew,” confusing you with the RCMP Commissioner due to both of your high level statuses with the RCMP. Nonetheless, kindly see below; this has also been faxed and is following via registered mail.

Thank you for your services.

Mr. Kevin A. McLean (BA, JD, CIM)

Date: Wed, 6 May 2026 12:46:27 -0400

Subject: Formal Request for Publicly Accessible Criminal Court Records, relating to events since at least 2024-10-02 (the “ArrestDate”), pursuant to correspondence from Police Officer (Constable) Mr. Anthony Romano dated 2024-10-02 (attached). This request is predicated upon the retrieval of my property from Unit 410-775 King Street West, Toronto, Ontario, M5V 2K3, subsequent to 2024-09-20, and pertains to, inter alia: (i) Information (Criminal Code Form 2 Information) or Information Package, whether sworn or unsworn; (ii) any relevant judicial endorsements from Ontario or federal courts; and (iii) any processes issued, including Intake Court Endorsements, warrants, or orders (including but not limited to arrest warrants, search warrants, general warrants, and production orders).

DELIVERY METHOD: Via Email and followed by Registered Mail and Facsimile

URGENT: TIME-SENSITIVE REQUEST

DATE: 2026-05-06

TO:

Mr. Michael Peggs Regional Commander RCMP Milton Detachment / Toronto West
Royal Canadian Mounted Police 2755 Highpoint Drive Milton, Ontario L9T 5E8 (The
“**Originating Police Service Office**”)

Office Phone: 905-876-9500

- **Toll-Free:** 1-800-461-9398
- Telephone :
905-876-9500
Fax :
905-876-9595
- **Office Hours:** Monday to Friday, 8:00 AM – 4:00 PM
- **Address:** 2755 High Point Drive, Milton, Ontario L9T 5E

FROM: Mr. Kevin A. McLean (B.A., J.D., CIM)

Email: mcleansettlement@gmail.com

Subject: Formal Request for Publicly Accessible Criminal Court Records, relating to events since at least 2024-10-02 (the “Arrest Date”), pursuant to correspondence from Police Officer (Constable) Mr. Anthony Romano dated 2024-10-02 (attached). This request is predicated upon the retrieval of my property from Unit 410-775 King Street West, Toronto, Ontario, M5V 2K3, subsequent to 2024-09-20, and pertains to, inter alia: (i) Information (Criminal Code Form 2 Information) or Information Package, whether sworn or unsworn; (ii) any relevant judicial endorsements from Ontario or federal courts; and (iii) any processes issued, including Intake Court Endorsements, warrants, or orders (including but not limited to arrest warrants, search warrants, general warrants, and production orders).

Dear Regional Commander Peggs,

I. Introduction & Purpose of Request

I am writing to formally request access to specific, publicly accessible criminal court records relating to events that have transpired since at least October 2, 2024 (the “**Arrest Date**”).

I hereby confirm that my approach to you at this juncture is predicated upon evidence that has only recently come to my attention, specifically as a result of communications held yesterday with counsel representing one of the governmental bodies. While I shall maintain the confidentiality and integrity of those communications, I can confirm that they have afforded me the pertinent understanding as to the necessity of RCMP involvement in this matter. Consequently, it became apparent that my request must be addressed directly to your detachment and to you in your capacity as Regional Commander.

This request is predicated upon the retrieval of my property from Unit 410-775 King Street West, Toronto, Ontario, subsequent to September 20, 2024, and correspondence

received from Constable Anthony Romano of the Toronto Police Service (TPS) 14th Division on October 2, 2024 (enclosed).

As the affected party, I am respectfully requesting the authentic copies of:

1. The **Information** (Criminal Code Form 2), whether sworn or unsworn;
2. Any relevant **judicial endorsements** from Ontario or federal courts (specifically including any Intake Court Endorsements); and
3. Any **processes issued or authorized** (including, but not limited to, arrest warrants, search warrants, general warrants, and production orders).

II. Statutory Authority for Access This request is made pursuant to the *Ministry of the Attorney General (MAG) Court Services Division Court Information Access Guide (2019)*. As you are aware, it is the established position of the courts that once process is issued (i.e., an Information is sworn and an arrest is executed), the originating and investigating police service maintains the primary copy of the sworn *Information* and related judicial endorsements. Because these documents become publicly accessible post-arrest, I am entitled to receive these records directly from your detachment.

My valid identification is enclosed herewith to securely verify my identity for the release of these records.

III. Jurisdictional Context and File Anomalies (For Your Assistance) To assist your detachment in locating the correct, authentic files, I provide the following context in good faith:

- **Confirmation of Origin:** Both the TPS and the Ontario Provincial Police (OPP) have confirmed they did not obtain the arrest warrant in question, though the TPS confirmed its execution. Consequently, the RCMP Milton Detachment is identified as the originating service.
- **The Case ID Fingerprint:** A heavily redacted and structurally anomalous document package (the "False Information Package") provided previously contains the **Police Case ID: 457197**. This identifier conforms to RCMP administrative protocols, confirming your detachment's jurisdiction over the record.
- **Document Irregularities:** The aforementioned package contains 41 structural errors and metadata confirming it was altered using *GrapeCity.Documents for PDF*. Known bugs in this specific software version affected the rendering of letters "C, L, M" for Court Officer Mrs. Frugoni-Rojas and the signature of Chief Justice Morawetz. Given these severe irregularities, it is imperative that I obtain the untampered, authentic source documents directly from your detachment.

For the record, I confirm that Chief Justice Morawetz has already been personally served with court documents seeking relief *in personam* and *pro bono publico* regarding his involvement prior to his departure from the Superior Court of Justice.

IV. Conclusion and Timeline I appreciate your detachment's prompt attention to this matter. I remain available to provide further particulars or assistance if needed to locate

the file.

Given that this is a request for basic, publicly accessible documents post-arrest, I kindly request that you advise me of your position—and provide the requested electronic disclosure or a definitive timeline for the same—by the **end of the business day today but no later than tomorrow in light of the business hours noted above.**

I also understand your detachment obtained property of mine from Unit 410-775 King Street West, City of Toronto, Province of Ontario, M5V 2K3 at some point after September 20, 2024, and prior to end of September 2024, and provided some to the TPS 14th Division, which you have my thanks, but I require the remainder of the same as many of those pieces of personal property are either privileged, confidential and/or private and/or have much in the way of sentimental value including gifts from loved ones who are no longer with us. I thank you for your attention to this discrete issue.

Should I not receive a response or a denial of the jurisdictional facts outlined above, I will assume the matters are sufficiently clear and that the RCMP acknowledges its role as the originating agency.

I confirm that I am solely seeking the above documents, information, and information assets which are to be available to the public and as it relates to myself, I am an unbridled and absolute entitlement to the same.

Thank you for your time and professionalism.

Sincerely,

Mr. Kevin A. McLean (B.A., J.D., CIM)

ENCLOSURES / INCORPORATED BY REFERENCE:

1. Valid identification of the Applicant (Enclosed for Verification).
2. Excerpts from the *Ministry of the Attorney General (MAG) Court Services Division Court Information Access Guide (2019)*.
3. Electronic communication from Constable Anthony Romano, TPS 14th Division, dated 2024-10-02.
4. The document entitled "False Information Package", evidencing software manipulation.
5. Document detailing 41 structural errors within the False Information Package.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

Tab B

Access court files, documents and exhibits

Learn what court documents are available to the public and media and how to access them. Read the Ministry of the Attorney General's Court Services Division Policies and Procedures on Public Access to Court Files, Documents and Exhibits.

Version date: Revised April 2019

The following guide is the Ministry of the Attorney General's Court Services Division Policies and Procedures on Public Access to Court Files, Documents and Exhibits. We posted the guide online to enhance public access to court proceedings, information and documents. This guide was first compiled and provided to Ministry court staff in January 2006 as part of the Ministry's ongoing efforts to ensure that there is consistent application of these procedures across the province. Policies regarding access to court files, documents and exhibits are periodically reviewed and updated, subject to the direction of the judiciary.

The material provided here is the same as the material on public access to court documents provided to court staff.

Section 1: General principles and policies for public access

1.1 Open and accessible court system

Ontario's court system is based on the fundamental principles of openness and accessibility. In general, most court documents are publicly accessible, unless a statutory provision, common law rule or court order restricts access.

The Supreme Court of Canada has held that the courts have a supervisory and protecting power over their records, and as a result, determine rules for public access. The Court Services Division of the Ministry of the Attorney General is responsible for the care and maintenance of court files and documents, with the exception of court files and

documents in Provincial Offences courts, which are administered by municipal partners under a transfer agreement. The Court Services Division makes policies regarding the care and maintenance of court files and documents, in accordance with applicable law, and subject to judicial direction.

1.2 Judicial direction

Each court has jurisdiction over its own records, and all policies respecting access to court documents, files and exhibits are subject to judicial direction. However, legislation and regulations (including rules of practice), existing jurisprudence, and consultation with the judiciary have led to the result that, except in the specific circumstances outlined in this guide, many documents are publicly accessible. Judicial consent is required to obtain access to court exhibits (see Section “6 Public access to exhibits

(<https://www.ontario.ca/document/access-court-files-documents-and-exhibits/section-6-public-access-exhibits>)”).

1.3 Timeframes for public access

Timeliness is essential to ensure access to court files and documents. The ability of court staff to facilitate timely access can be affected by various factors. Court Services Division Record Retention Schedules outline the requirements for storing files on-site or off-site. Retention schedules also outline when records can be destroyed or stored by the Archives of Ontario. For example, post court dockets may be destroyed after 3 years.

Where on-site storage is limited, some files may be transferred off site sooner than set out in the Retention Schedules. By necessity, the time required for access to files and documents that are stored off site will be longer than for files and documents stored at the courthouse.

In addition, court staff must prioritize their responsibilities to ensure:

- matters scheduled before the court are proceeding;
- the needs of parties, witnesses, interpreters and jurors are met; and
- judicial direction is followed.

Given these priorities, court staff must facilitate access to court files and documents as quickly and efficiently as possible.

471 1.4 Providing information over the telephone

Information from court records that would be accessible to the public at no charge is available over the telephone. Many court records in the Ontario Court of Justice and Superior Court of Justice are accessible at no charge. See section “7 Fees for public access to court documents (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents>)” for information about fees to access documents.

1.5 Procedures for ensuring public access

Because a court file may contain documents that are not publicly accessible, court staff must ensure that only publicly accessible documents are provided to members of the public for inspection.

In civil and family matters, Court Services Division requires the use of a correspondence pocket in court files. Documents for which public access is restricted must be filed in the correspondence pocket. Court staff must remove the correspondence pocket from the file before providing the file to a member of the public for inspection. For additional information, please refer to section “3.7 Other documents Related to Civil Proceedings (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-civil-court-files-and-documents#section-6>)”.

1.6 Copies and photographs of documents

Court staff can provide a copy of any document in the court file if:

- the requester has the right to see the document;
- the document can be photocopied; and
- the requester pays the relevant copy fee (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-2>).

Members of the public can make a copy of any documentation in the court file using their own camera or other electronic device at no charge if they have the right to see the document. The use of photography is limited to the documentation in the court file and must be conducted in the administration area. Please refer to section “1.7 Use of cameras, recording and other electronics devices in the courtroom”

(<https://www.ontario.ca/document/access-court-files-and-documents#section-6>) for further explanation about the use of cameras and recording devices.

Members of the public may have a copy of a digital recording of a court hearing if:

- they have the right to a copy of the recording;
- judicial direction is obtained; and
- they pay the relevant copy fee (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-2>) .

1.7 Use of cameras, recording and other electronic devices in the courtroom

No cameras (including cell phone cameras) or video recording devices may be used in the courtroom without the approval of the presiding judicial official (s. 136 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK183>)) (<https://www.ontario.ca/laws/statute/90c43>) . Photographing of any person in attendance at the courthouse is also prohibited.

For further information about the use of electronic communication devices in court proceedings, please see the Ontario (<http://www.ontariocourts.ca/ocj/legal-professionals/practice-directions/electronic-devices/>) Court of Justice website (<https://www.ontario.ca/www.ontariocourts.ca/ocj/legal-professionals/practice-directions/electronic-devices/>) and the Superior Court of Justice website (https://www.ontariocourts.ca/scj/practice/practice-directions/provincial#D_Electronic_Devices_in_the_Courtroom) .

Section 2: Public access to criminal court files and documents

2.1 General principle of public accessibility

In general, once process is issued (meaning an Information is sworn and an arrest is made or a summons is served), criminal court files and documents are publicly accessible, unless legislation, a common law rule or a court order restricts access.

2.2 Criminal court files and documents with restricted access

Exceptions to this general principle of public accessibility are outlined below. In accordance with section 1.2 of this policy, the following exceptions to public accessibility are always subject to judicial direction:

General Rule

Court files and documents of *Youth Criminal Justice Act* (<https://www.laws-lois.justice.gc.ca/eng/acts/y-1.5/index.html>) (YCJA) proceedings or other proceedings that make reference to YCJA information (for example, *Parental Responsibility Act* (<https://www.ontario.ca/laws/statute/00p04>) Small Claims Court actions (see section “3.2.1 Documents regarding *Parental Responsibility Act* matters”), (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-civil-court-files-and-documents#section-1>) child protection cases (see section “4.2.1 Child protection cases (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-family-court-files#section-0>)”), or *Mental Health Act* (<https://www.ontario.ca/laws/statute/90m07>) (MHA) proceedings (see section “2.2.11 Mental health assessments (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-family-court-files#section-0-11>)”) are not accessible to the public, unless the young person receives an adult sentence and:

- the appeal period has elapsed; or
- an appeal has been heard and the court of appeal has upheld the adult sentence.

YCJA records are accessible to persons listed in s.119 of the YCJA (<https://laws-lois.justice.gc.ca/eng/acts/Y-1.5/page-13.html?txthl=119#s-119>) , or if a court order is obtained pursuant to s.119(1)(s) of the YCJA (<https://laws-lois.justice.gc.ca/eng/acts/Y-1.5/page-13.html?txthl=119#s-119>) .

Exception for information about courtroom location and future court dates

Daily court lists providing the courtroom location for YCJA matters are available to the public. These lists include the initials of a young person and the charges they are facing.

Court staff will not release the young person’s name in a YCJA matter.

Future court dates in YCJA matters are available to the public if sufficient information is provided to allow court staff to access the information in a reasonable amount of time. The following are examples of information that may be necessary to allow court staff to locate the information:

- court file number;

- last court date;
- charges against the young person; and
- date of birth.

If an exclusion or sealing order has been made in the YCJA matter, disclosure of next court date information is not permitted.

2.2.2 *Pre-Enquête* documents and recordings

Intake is presided over by a justice of the peace and is a forum for the police and individuals to bring Informations before a justice of the peace in order to lay criminal charges.

The justice of the peace may conduct a *pre-Enquête* hearing to determine whether legal process should issue (meaning, whether an Information is sworn and then whether to issue process by way of a summons or warrant). *Pre-Enquête* hearings are not open to the public.

If process is issued

For both private and Crown prosecutions, if process is issued, the documents of the *pre-Enquête* hearing become publicly accessible once the defendant has been arrested or the summons has been served, unless there are legislative restrictions to access (for example, the YCJA) or a court order restricts access.

If process is not issued

If process is not issued, the documents and tapes of the *pre-Enquête* hearing are not publicly accessible.

2.2.3 Documents relating to a peace bond application

An individual or peace officer may make an application to the court for a peace bond to request that a person be ordered to keep the peace. To begin the application, the complainant presents an Information at an initial interview with a justice of the peace.

If the justice of the peace issues process, any documents relating to the application are accessible to the public once the defendant has been served with the summons (or in rare

circumstances, has been arrested), unless otherwise ordered by the court. If the justice of the peace refuses to issue process, there is no public access to the documents.

2.2.4 Search warrants (s. 487 of the *Criminal Code*)

A search warrant is a tool that permits investigators to search specified locations (such as a residence, office or vehicle) and seize particular items. Warrants are not necessarily tied to a specific individual.

Specialized search warrants also exist for:

- the seizure of bodily substances for DNA analysis;
- controlled drugs and substances;
- counterfeit money;
- hate propaganda;
- lumber or lumbering equipment;
- obscene material;
- precious metals; and
- proceeds of crime.

General warrants permit peace officers to use devices or investigative techniques described in the warrant if a search and/or seizure without it would violate section 8 of the *Charter of Rights and Freedoms* (<https://laws-lois.justice.gc.ca/eng/const/page-12.html>) (the right to be secure against unreasonable search or seizure).

DNA warrants are publicly accessible if the warrant has not been sealed by court order.

Search warrants and general warrants, including those under the *Controlled Drugs and Substances Act* (<https://laws-lois.justice.gc.ca/eng/acts/c-38.8/>), are publicly accessible, if:

- the warrant has not been sealed by court order;
- the warrant has been executed and a seizure has been made; and
- a Report to a Justice (Form 5.2) has been filed with the court office by the relevant police or investigating service or an Order of Disposition has been made by the

presiding judicial official

- Depending on the police or investigating service, it may take some time for the Report to Justice to be filed with the court, if a seizure has been made.

Court staff do not have the authority to provide any information about the search warrant or related documents (including confirming the existence of an application for a search warrant) if:

- the warrant has not been executed;
- the warrant was executed but nothing was seized; or
- things were seized, but a Report to Justice has not been filed by the police or investigating service or an Order for Disposition has not been made.

This is consistent with rulings of the Supreme Court of Canada and ensures that ongoing investigations are not compromised and that privacy rights are respected.

If the individual seeking access believes that a search warrant has been executed, but there is no information publicly accessible at the court counter, they may wish to obtain further details from the police or investigating service.

Requesting access to search warrants

Individuals seeking access to search warrants must provide enough information for court staff to identify the records sought. This most commonly includes the location (for example, an address) searched and/or the date the warrant was executed and may also include, when known, the:

- name of the person (often a police officer) or agency who sought the warrant;
- name of the judicial official who approved the warrant; and/or
- date the search warrant was issued.

Search warrants are filed by location to be searched and date of search. If an individual does not know the address and/or date of search, court staff will attempt to assist the requester, however sufficient information to allow court staff to identify the requested warrant is necessary. Search warrants are not filed by name of an individual subsequently charged as a result of an investigation.

477 Tracking warrants and number recorder warrants (s. 492.1 and s. 492.2 of the *Criminal Code*)

Staff must seek judicial direction when a third-party requests access to tracking warrants issued under section 492.1 and number recorder warrants issued under section 492.2 of the *Criminal Code*. (<https://laws-lois.justice.gc.ca/eng/acts/c-46/>)

Sealed warrants

Under subsection 487.3(1) of the *Criminal Code* (<https://laws-lois.justice.gc.ca/eng/acts/C-46/page-71.html?txthl=487.3#s-487.3>), the presiding judicial official may, upon application, make an order prohibiting access to and disclosure of documents related to any warrant. This is referred to as a sealing order. Access to sealed warrants is only permitted if the sealing order provides exceptions for specific persons or by further order of the court.

A sealing order typically provides the date the file was sealed and the name of the judicial official who sealed the documents, but it does not disclose information about the content of the warrant. Assuming that is the case, the sealing order is accessible unless otherwise ordered by a judicial official. However, if the sealing order contains confidential information that is under seal, judicial permission is required for access.

Given the confidential nature of sealed records and the limited information available to court staff where a warrant is sealed (for example, the location, address or subject searched is often itself confidential), staff may not always be able to identify the warrants sought.

Persons seeking access to the sealed materials may bring an application to the judicial official who made the order or to a judge of the court where any proceedings arising out of the investigation may be held.

2.2.5 Arrest warrants (warrants in the first instance and bench warrants)

Warrants of arrest (also known as Warrants in the First Instance) may or may not be filed with the court. Practices for filing warrants of arrest vary depending on the police service. If a warrant of arrest or copy of a warrant of arrest is in the court file, it is only publicly accessible after the accused has been arrested or has received a summons, provided no other public access restrictions apply (for example, the YCJA).

Bench warrants may also be issued and executed anywhere in Canada against a person who does not appear in court or remain in attendance for his or her court appearance. Information about these warrants is publicly accessible, provided no other public access restrictions apply (for example, the YCJA).

2.2.6 Production orders

A production order is made by a judge or justice of the peace and is similar to a search warrant. When a production order is made, the person in possession of the information identified in the order must produce it upon request to the law enforcement agency. There are five different types of production orders:

- General production order – requires a person to produce or prepare a document from data in his/her possession or control.
- Financial data production order – requires a financial or commercial institution to produce account details, such as the name and other identifying information about the owner, the status and type of account, and the day it was opened or closed.
- Trace specified communication production order – requires a person to prepare a document containing data that identifies a device or person involved in the transmission of a communication.
- Transmission data production order – requires a person to prepare or produce a document providing information including the origin, destination, date, time or duration of a telecommunication.
- Tracking data production order - requires a person to prepare or produce a document containing data about the location of an individual or thing.

Information about an application for a production order, the documents or information provided is publicly accessible if:

- the production order has not been sealed by court order;
- the production order has been executed; and
- documents or data were produced in response to the order.

2.2.7 Court files and documents under *Criminal Code* publication bans

When a publication ban is imposed by the court (for example, s. 486.4 related to sexual offences or s. 517 related to judicial interim release or bail hearings) or is automatically

479 provided for (for example, s. 542 related to preliminary hearings), the court file and documents are still accessible to the public. Staff will notify the recipient that the file or document is under a publication ban and will warn him or her that publication, broadcasting or transmitting in any way the information governed by the publication ban could be a violation of law.

2.2.8 In camera / publicly-excluded proceedings

Under various sections of the *Criminal Code* (<https://laws-lois.justice.gc.ca/eng/acts/c-46/>)^[1], the public may be excluded in whole or in part from a court proceeding. These proceedings are known as in camera or publicly excluded proceedings. If the public is excluded from a court proceeding, the public cannot access the records relating to that portion of the proceeding, except by court order.

2.2.9 Court files and documents in section 276(2), section 278.2, section 278.92(2) and O'Connor applications

Applications to:

- determine the admissibility of a complainant's sexual activity (s. 276(2) of the *Criminal Code* (<https://laws-lois.justice.gc.ca/eng/acts/c-46/section-276.html>));
- determine whether there will be production of third-party records in sexual offence cases (s. 278.2 of the *Criminal Code* (<https://laws-lois.justice.gc.ca/eng/acts/c-46/section-278.2.html>));
- determine the admissibility of records relating to a complainant that are in the possession of the accused (s. 278.92(2) of the *Criminal Code* (<https://laws-lois.justice.gc.ca/eng/acts/c-46/section-278.92.html>)); and
- determine whether there will be production of third-party records in non-sexual offence cases (O'Connor applications).

require that specific documents be filed with the court. These documents may be filed at the time of the application or before the court date

Applications for a hearing and hearings to determine admissibility under s. 276(2) or s. 278.92(2) must be held in camera.

For s. 278.2 applications, the judicial official will consider the application in a mandatory in camera proceeding. If the judicial official orders the record be produced to the court, the

Judicial official may hold an in camera hearing to determine whether to produce the record to the accused.

Documents filed in advance of these mandatory in camera proceedings are not publicly accessible prior to the court hearing, except by court order.

For O'Connor applications, a hearing will be held to determine the relevance of third-party records. There is no mandatory requirement that the hearing be held in camera. However, an order excluding the public may be requested by one or both of the parties either at the time of the application or in their documents filed before the court date. Until the judge hearing the application determines whether or not the public should be excluded, any documents filed in advance of these proceedings are not publicly accessible, except by court order.

2.2.10 Identifying information about witnesses

Section 486.31 of the *Criminal Code* (<https://laws-lois.justice.gc.ca/eng/acts/C-46/page-66.html?txthl=486.31#s-486.31>) allows a court to restrict disclosure of any information that could identify a witness in a criminal proceeding if the order is in the interest of the proper administration of justice. Upon an application by the prosecutor or witness, a hearing will be held to determine whether the order should be made. These hearings may be held in camera and until the judge hearing the application determines whether or not the public should be excluded, any documents filed in advance of the application are not publicly accessible, except by court order. If the court grants the non-disclosure order after the hearing, identifying information about the witness is not publicly accessible, without judicial permission.

2.2.11 Mental health assessments

Access to the materials listed below requires judicial direction:

- assessment reports prepared for the court under s. 672.11 of the *Criminal Code* (<https://laws-lois.justice.gc.ca/eng/acts/c-46/page-98.html>) (mental disorder);
- any written information filed with the court regarding an accused person's fitness to stand trial;

- any written information filed with the court regarding whether an accused person should be found not criminally responsible due to mental disorder;
- all records relating to assessments ordered by a judge in a criminal proceeding under s. 21 or 22 of the *Mental Health Act* (<https://www.ontario.ca/laws/statute/90m07>) ; and
- all records relating to applications to a Justice of the Peace under the *Mental Health Act* (<https://www.ontario.ca/laws/statute/90m07>) for an order for an examination by a physician of a person thought to be suffering from a mental disorder.

As previously noted, any reference to *Youth Criminal Justice Act* (<https://www.laws-lois.justice.gc.ca/eng/acts/y-1.5/index.html>) information contained in *Mental Health Act* (<https://www.ontario.ca/laws/statute/90m07>) records is not publicly accessible.

2.2.12 Sealed files and documents

A sealing order typically provides the date the file was sealed and the name of the judicial official who sealed the documents, but it does not disclose information about the content of the sealed documents. Assuming that is the case, the sealing order is accessible unless otherwise ordered by a judicial official. However, if the sealing order contains confidential information that is under seal, judicial permission is required for access.

Please refer to the section “2.2.4 Search warrants (s. 487 of the *Criminal Code*)” (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-3>) ” for information about access to sealed search warrants.

2.2.13 *Cannabis Act* ticketable offence proceedings

The federal *Cannabis Act* (<https://laws-lois.justice.gc.ca/eng/acts/C-24.5/>) contains prohibitions on the recreational use of cannabis. For certain offences under the *Act*, persons 18 years of age or older may be dealt with using a criminal ticket instead of being prosecuted under the usual criminal process.

Pursuant to the *Act*, records of criminal tickets are not accessible if the accused:

- pleads guilty to the ticket or is convicted of the offence and all outstanding fines are paid; or
- accused is convicted of the offence and has served, in full, any period of imprisonment imposed as a result of a default in payment of the fine.

Where access to these matters is restricted, court staff must not allow access to the court documents and must not disclose the existence of documents to any person.

2.2.14 Documents relating to absolute and conditional discharges

This section does not apply to absolute discharges imposed as a result of a ticket under the *Cannabis Act* (<https://laws-lois.justice.gc.ca/eng/acts/C-24.5/>) . Information on access to those records can be found in the section “2.2.13 *Cannabis Act ticketable offence proceedings* (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-12>) ”.

The *Criminal Records Act* (<https://laws-lois.justice.gc.ca/eng/acts/c-47/>) denies public access to criminal records:

- after one year, if the defendant has received an absolute discharge; or
- after three years, if the defendant has received a conditional discharge.

The Province of Ontario has adopted this policy with regard to court documents that are the subject of an absolute or conditional discharge. The access period commences from the date the discharge was imposed by the judicial official.

If an absolute or conditional discharge has been ordered, court staff must not allow access to the court documents and must not disclose the existence of these documents, after the specified periods noted above, to anyone other than the person who is the subject of the discharge or counsel acting on his or her behalf. Requests for access by the person who is the subject of the discharge must be made in writing to the court.

2.2.15 Documents relating to record suspensions and expungements

If a record suspension has been granted, documents relating to the original conviction in the custody of a department or agency of the Government of Canada are not publicly accessible, without prior approval of the Federal Minister of Justice. The Province of Ontario has adopted this policy with regard to court documents that are the subject of a record suspension.

If an expungement has been granted, documents relating to the original conviction in the custody of a department or agency of the Government of Canada will be destroyed or removed from its repositories or systems.

If a record suspension or expungement has been granted, court staff must not allow access to the court documents and must not disclose the existence of these documents to any person, other than the person who is the subject of the record suspension or expungement or counsel acting on his or her behalf. Requests for access by the person who is the subject of the record suspension or expungement must be made in writing to the court.

2.2.16 Records of convictions under section 10.6 of the Controlled Drugs and Substances Act (CDSA)

Effective November 17, 2024

Section 10.6 of the Controlled Drugs and Substances Act (<https://laws-lois.justice.gc.ca/eng/acts/c-38.8/>) (CDSA) provides that records of convictions in respect of an offence under section 4(1) of the CDSA must be kept separate and apart from other records of convictions within certain time periods.

The Province of Ontario has adopted this policy for records of convictions for CDSA section 4(1) drug possession.

If a person has been convicted of drug possession under CDSA section 4(1), court staff must not allow access to the record of conviction of the CDSA section 4(1) offence and must not disclose the existence of that conviction, in accordance with the applicable time periods in section 10.6 of the CDSA, to anyone other than the person who is the subject of that conviction or counsel acting on their behalf. Requests for access by the person who is the subject of the conviction must be made in writing to the court.

This section of the policy does not apply to YCJA records. For the policy in relation to access to YCJA records, please refer to section 2.2.1.

2.3 Index books

In criminal cases, index books are not accessible to the public, as they may contain information about documents for which access is prohibited.

2.4 Dockets and case event lists

2.4.1 Pre-court docket and case event list

The pre-court docket or case event list is a list of names of the accused persons and the charges scheduled to be heard in a specific courtroom, on a specific date, and at a specific time.

Pre-enquête, Youth Criminal Justice Act (<https://www.laws-lois.justice.gc.ca/eng/acts/y-1.5/index.html>) and *Prevention of and Remedies for Human Trafficking Act, 2017* (<https://www.ontario.ca/laws/statute/17p12>) restraining order dockets must remain confidential and are not publicly accessible. All other pre-court dockets are publicly available.

Court staff must make pre-court dockets or case event lists available to the public at no charge, by either posting the docket or list in a location convenient to the public or by making it available at the court counter. A copy of the docket can be provided on payment of the prescribed copy fee (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-2>).

The daily court lists (<https://www.ontariocourtdates.ca/>) provide users with basic next day case event information for Ontario Court of Justice and Superior Court of Justice cases, subject to certain restrictions. Website users may choose a court location and case type from drop down lists. A list of scheduled matters to be heard the next day at that location will then be displayed.

Hearing lists of the Ontario Court of Appeal (<http://www.ontariocourts.ca/coa/en/caselist/>) are also available the week before matters are to be heard.

2.4.2 Post-court docket and case event list

The post-court docket or case event list is the same as the pre-court docket or list, with notes outlining the judicial decisions for each charge listed.

The post-court docket or list is publicly accessible, except to the extent that it includes cases that:

- have been sealed;
- are subject to a specific court order restricting access;
- are applications for restraining orders under the *Prevention of and Remedies for Human Trafficking Act, 2017* (<https://www.ontario.ca/laws/statute/17p12>);

• pertain to youth matters; or

- are outside legislated disclosure periods (for example, access to some matters are time limited, including absolute and conditional discharges, as outlined in the section “2.2.14 Documents relating to absolute and conditional discharges (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-13>)”, and records of convictions under section 10.6 of the CDSA, as outlined in section “2.2.16 Records of convictions under section 10.6 of the Controlled Drugs and Substances Act (<https://laws-lois.justice.gc.ca/eng/acts/c-38.8/>) (CDSA)”).

Court staff must make post-court dockets or lists available to the public for viewing at no charge. If a copy of the docket or list is requested, staff should charge the prescribed copy fee (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-2>) .

Note: Due to storage limitations in the court office, some older court dockets and lists may not be immediately available at the court counter. The time required to access older dockets and lists that are not stored in the court office might be longer.

2.5 *Provincial Offences Act* court documents

As noted previously in the section “1.1 Open and accessible court system (<https://www.ontario.ca/document/access-court-files-and-documents#section-0>)”, municipal partners administer court files and documents in Provincial Offences courts under a transfer agreement with the province. In general, court documents related to the *Provincial Offences Act* (<https://www.ontario.ca/laws/statute/90p33>) (POA) are publicly accessible, unless otherwise ordered by the court.

However, the following court documents for *Provincial Offences Act* (<https://www.ontario.ca/laws/statute/90p33>) proceedings are not publicly accessible:

- all records relating to an application for an order of examination under the *Mental Health Act* (<https://www.ontario.ca/laws/statute/90m07>) , unless access is approved by a justice of the peace; and
- all proceedings against young persons commenced under Part VI of the *Provincial Offences Act* (<https://www.ontario.ca/laws/statute/90p33>) .

Search warrants issued under the *Provincial Offences Act* (<https://www.ontario.ca/laws/statute/90p33>) are accessible in accordance with the policy

for criminal search warrants. In general, search warrants are accessible if:

- the warrant has not been sealed by court order;
- the warrant has been executed and a seizure has been made; and
- a Report to a Justice (Form 5.2) has been filed with the court office by the relevant police or investigating service, or an Order of Disposition has been made by the presiding judicial official. Depending on the police or investigating service, it may take some time for the Report to Justice to be filed with the court, if a seizure has been made.

For more detailed information about accessing search warrants, see section “2.2.4 Search warrants (s. 487 of the *Criminal Code*)” (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-3>)

2.6 *Prevention of and Remedies for Human Trafficking Act, 2017* court documents

The *Prevention of and Remedies for Human Trafficking Act, 2017*

(<https://www.ontario.ca/laws/statute/17p12>) (PRHTA) allows victims, or potential victims, of human trafficking to apply for a restraining order. Unless legislation, a common law rule or a court order restricts access, records of such applications are publicly accessible if:

- an application is made with notice to the respondent; or
- an application is made without notice to the respondent, the order is granted, and the respondent has been served.

Where an order is made without notice to the respondent, the application form and any supporting affidavits may be provided only to the sheriff and members of the police service to assist in carrying out service of the restraining order.

In all other circumstances, judicial permission is required before court staff can provide any information about a PRHTA restraining order or related documents, including confirming the existence of an application for such an order.

2.6.1 Court files and documents under *Prevention of and Remedies for Human Trafficking Act, 2017* publication bans

487 When a publication ban is automatically provided for under subsection 10(1) of the PRHTA, or a publication ban is imposed by the court under subsection 10(2) of the PRHTA, PRHTA restraining order court files and documents are still accessible to the public. Staff must notify the person who is accessing the file or document that it is under a publication ban and must warn them that publishing, broadcasting or transmitting the information governed by the publication ban in any way could be a violation of law.

2.7 Criminal court documents

Criminal court staff can provide information and copies of court documents relating to matters that are either before the court or have been before the court in the past in accordance with these policies and procedures, as long as no other access restrictions exist. If an individual received an absolute or conditional discharge, if the individual has a record of conviction subject to section 10.6 of the CDSA, if the criminal record is subject to a record suspension (pardon) or if the court documents are sealed by court order, access is limited and information and court documents will be provided only in accordance with "2.2.12 Sealed files and documents" (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-12>), "2.2.14 Documents related to absolute and conditional discharges" (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-13>), "2.2.15 Documents relating to record suspensions and expungements" (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-14>) and "2.2.16 Records of convictions under section 10.6 of the Controlled Drugs and Substances Act (CDSA)".

A request for access to criminal court documents should include a combination of information that will permit staff to accurately identify the individual concerned, which most commonly will be name and date of birth. In some circumstances where a name is common, further information such as home address, date of offences or charges may be required in order for court staff to accurately identify the individual. The combination of information required will vary depending on what is necessary to correctly identify the requested information in a particular case.

Some people believe that court staff can provide an official criminal record check. The court case tracking system is not a comprehensive database of criminal charges or criminal dispositions and does not constitute an official criminal record. Only police services can undertake an official criminal record check for employment or related purposes.

Section 3: Public access to civil court files and documents

3.1 *Courts of Justice Act* provisions for public access

Section 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>) (CJA) provides for public access to civil court documents.

Upon payment of the prescribed fee, members of the public are entitled to see any current list maintained by the court of civil proceedings commenced, any documents filed in a civil proceeding, or any judgments entered, unless a statutory provision, common law rule or court order restricts access.

3.2 Statutory restrictions to public access

Statutory provisions restrict public access to the following civil court documents:

3.2.1 Documents regarding *Parental Responsibility Act* matters

Documents filed in the Small Claims Court in relation to the *Parental Responsibility Act* (<https://www.ontario.ca/laws/statute/00p04>) that include evidence obtained under the *Young Offenders Act* (<https://laws-lois.justice.gc.ca/eng/acts/y-1/index.html>) (YOA) or *Youth Criminal Justice Act* (<https://www.laws-lois.justice.gc.ca/eng/acts/y-1.5/index.html>) (YCJA) must be treated like *Young Offenders Act* or *Youth Criminal Justice Act* documents and are not publicly accessible. See section “2.2.1 Documents in *Youth Criminal Justice Act* Proceedings (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-criminal-court-files-and-documents#section-1-0>) ” for details on public access to these documents.

3.3 Files and documents under publication bans

In general, when the court imposes a publication ban, the public can still access the court file and documents. Staff must tell the person who is accessing the file or document that it is under a publication ban and must warn him or her that publication could be a violation of law.

3.4 Sealed files and documents

sealing order typically provides the date the file was sealed and the name of the judicial official who sealed the documents, but it does not disclose information about the content of the sealed documents. Assuming that is the case, the sealing order is accessible unless otherwise ordered by a judicial official. However, if the sealing order contains confidential information that is under seal, judicial permission is required for access.

3.5 Daily filing list report

The Daily Filing List Report contains the court file numbers, names of plaintiffs and defendants, the Short Title of the proceeding, the Case Type, the Case Opened Date and the Initiating Document for proceedings commenced on that day, and may be made publicly available for viewing at no charge. Copies of the Daily Filing List Reports may be made publicly available on request on payment of the relevant copy fee

(<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-2>) .

3.6 Case event lists and post-court dockets

The Daily Court Lists (<http://www.ontariocourtdates.ca/>) provide users with basic next day case event information for Superior Court of Justice cases, subject to certain restrictions. Website users may choose a court location and case type from drop down lists. A list of scheduled matters to be heard the next day at that location will then be displayed.

Hearing lists of the Ontario Court of Appeal (<http://www.ontariocourts.ca/coa/en/caselist/>) are also available the week before matters are to be heard.

Subject to orders of the court and the statutory restrictions outlined in section “3.2 Statutory restrictions to public access” (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-civil-court-files-and-documents#section-1>)”, the post-court docket and case event lists are public documents and may be viewed at no charge. A copy of the docket or list can be provided to members of the public, upon payment of the relevant copy fee (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-2>) .

Note: Due to storage limitations in the court office, some older court dockets and case event lists may not be immediately available at the court counter. The time required to access older dockets and case event lists that are not stored in the court office might be longer.

490.7 Other documents related to civil proceedings

Other documents may be contained in the court file, even though they have not been filed in the proceeding within the meaning of s. 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>) . As section 137 does not apply to these documents, they are not automatically publicly accessible. Some examples of these documents include:

- correspondence between the trial coordinator and the parties to canvass available dates for events;
- correspondence between the court office and an individual regarding fees paid to court (for example, regarding an NSF cheque); and
- correspondence between the court office and an institution/agency (for example, police) necessary for the institution/agency to enforce or register an order
- fee waiver information.

These documents must be filed in the correspondence pocket within the court file. Court staff must remove the correspondence pocket from the file before providing the file to a member of the public for inspection. However, if the court staff require someone to provide a document to the court before "filing" something further (for example, court staff require a letter explaining, for the purposes of rule 61.13 of the *Rules of Civil Procedure* (<https://www.ontario.ca/laws/regulation/900194#BK606>) , why certain parties have not been served), that document, even if it is the form of a letter, should be placed in the part of the file that is publicly accessible and not in the correspondence pocket.

Section 4: Public access to family court files

4.1 *Courts of Justice Act* provisions for public access

Section 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>) (*CJA*) provides for public access to family court documents.

Members of the public are entitled to see any current list maintained by the court of family cases started, any documents filed in a family case, or any orders signed, unless a statutory provision, common law rule or court order restricts access.

491 1.2 Notice requirements for public access

Rule 1.3 of the *Family Law Rules* (<https://www.ontario.ca/laws/regulation/990114>) requires members of the public to give 10 calendar days' written notice before they may access certain court files under s. 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>). The written notice must be sent to the parties in the case, as well as the Children's Lawyer in some circumstances.

A member of the public is required to give 10 days' written notice before they can see any document filed in a case involving:

- A claim about decision-making responsibility, parenting time, or contact with respect to a child under the *Divorce Act* (<https://laws-lois.justice.gc.ca/eng/acts/d-3.4/FullText.html>) or Part III of the *Children's Law Reform Act* (<https://www.ontario.ca/laws/statute/90c12>);
- An order under Part I of the *Children's Law Reform Act* (<https://www.ontario.ca/laws/statute/90c12>); or
- International child abduction.

After receiving notice, a party then has 10 calendar days to bring a motion for a restricted access order, if they choose to do so. If a motion is made, court staff are not allowed to grant public access until the court determines the motion. If no motion is made, after the 10 calendar days have passed, the member of the public requesting access must file an affidavit (Form 14A) confirming the date they gave notice, to whom and by what method, and that they have not been served with a motion for a restricted access order. That person may then access the court file..

The following persons are exempt from the notice requirements under rule 1.3:

- A party or their lawyer
- A person authorized in writing by a party or the party's lawyer
- The Director of the Family Responsibility Office
- The Children's Lawyer
- A children's aid society
- Legal Aid Ontario
- Legal Aid Ontario

- A recipient, or an agency referred to in clause (b) or (c) of the definition of “recipient” in subrule 2(1) of the *Family Law Rules* (<https://www.ontario.ca/laws/regulation/990114#BK9>) when attempting to determine whether it is a recipient
- A Crown Attorney, assistant Crown Attorney or Deputy Crown Attorney
- A police officer, First Nations Constable or officer of the Royal Canadian Mounted Police, when acting in the course of their duties
- A service provider within the meaning of s. 149 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK205>)

4.3 Statutory restrictions to public access

Statutory provisions restrict public access to the following family court documents:

4.3.1 Child protection cases

Under subsections 87(4) and 121(8) of the *Child, Youth and Family Services Act, 2017* (<https://www.ontario.ca/laws/statute/17c14>) (CYFSA), child protection hearings and appeals of child protection decisions are closed to the public, unless otherwise ordered by the court. Under subsections 87(5) and 121(8) of the *Act*, select representatives of the media may attend the hearings, unless the court makes an order excluding them. Subsection 87(8) of the *Act* prohibits the publication of any identifying information about a child, child’s parent or foster parent or a member of the child’s family in a child protection case.

Court staff are therefore not permitted to provide public or media access to court documents filed in child protection cases, including any warrant issued under the CYFSA, even to media representatives who attended the hearing.

4.3.2 Secure treatment cases

Secure treatment cases involve applications to the court to commit a child to a secure treatment program. Under subsection 161(7) of the *Child, Youth and Family Services Act, 2017* (<https://www.ontario.ca/laws/statute/17c14>) (CYFSA), secure treatment hearings are closed to both the public and the media. Court staff are not permitted to provide access to court documents filed in these cases, including any warrant issued under the CYFSA.

4.3.3 Adoption cases and openness orders

Under subsections 204(1) and 215(6) of the *Child, Youth and Family Services Act, 2017* (<https://www.ontario.ca/laws/statute/17c14#BK223>) (CYFSA), adoption hearings and appeals of adoptions orders are closed to the public. Subsection 204(2) of the CYFSA (<https://www.ontario.ca/laws/statute/17c14#BK281>) states that court files concerning applications for adoption are only accessible to:

- the court;
- court employees;
- the parties and their lawyers or agents; and
- the Director or local director (appointed pursuant to subsection 53(1) of the CYFSA (<https://www.ontario.ca/laws/statute/17c14#BK72>)) or children's aid society under the CYFSA (<https://www.ontario.ca/laws/statute/17c14>) .

The files are not accessible to the public, including members of the media.

Under subsection 222(2) of the CYFSA (<https://www.ontario.ca/laws/statute/17c14#BK305>) , the documents used in an application for an adoption order must be sealed with a certified copy of the original order placed within the sealed file. The sealed file can only be accessed through an order of the court or written direction of the Registrar of Adoption Information.

4.3.4 Proceedings under the *Family Responsibility and Support Arrears Enforcement Act, 1996*

The *Family Responsibility and Support Arrears Enforcement Act, 1996* (<https://www.ontario.ca/laws/statute/96f31>) , applies to cases involving the enforcement of support obligations in Ontario.

During a default hearing under the Act, the court may order a person who is 'financially connected' to the payor to file a financial statement and any other relevant documents with the court. Under subsection 41(24) of the Act, the person's financial statement or other documents must be sealed in an envelope in the court file and is only accessible through an order of the court.

Under section 54 of the Act, if a person needs information from another person or organization to enforce an order that is not filed with the Family Responsibility Office, the court can order that the requested information be provided to the court. The information

that is obtained under this order must be sealed in an envelope in the court file. It is only accessible by court order, or in the other circumstances described in the Act at section 54.

4.4 Files and documents under publication bans

In family cases, other than cases under the *Child, Youth and Family Services Act, 2017* (<https://www.ontario.ca/laws/statute/17c14>) (CYFSA), when a publication ban is imposed by the court, the public can generally still access the court file and documents. Staff must notify the recipient that the file or document is under a publication ban and must warn him or her that publication could be a violation of law.

4.5 Sealed files and documents

A sealing order typically provides the date the file was sealed and the name of the judicial official who sealed the documents, but it does not disclose information about the content of the sealed documents. Assuming that is the case, the sealing order is accessible unless otherwise ordered by a judicial official. However, if the sealing order contains confidential information that is under seal, judicial permission is required for access.

4.6 Index books

Family index books contain lists of court file numbers and names of the applicants and respondents. In family cases, other than, adoption, child protection and openness order cases, information in index books is publicly available at no charge.

4.7 Case event lists and post-court dockets

The Daily Court Lists (<http://www.ontariocourtdates.ca/>) provide users with basic next day case event information for Ontario Court of Justice and Superior Court of Justice cases, subject to certain restrictions. Website users may choose a court location and case type from drop down lists. A list of scheduled matters to be heard the next day at that location will then be displayed.

Hearing lists of the Ontario Court of Appeal (<http://www.ontariocourts.ca/coa/en/caselist/>) are also available the week before matters are to be heard.

Subject to orders of the court and the statutory restrictions outlined in section “Statutory restrictions to public access” (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-civil-court-files-and-documents#section-1>), the case event lists and

post-court dockets are public documents and may be viewed at no charge. A copy of the list or docket can be provided to members of the public, upon payment of the relevant copy fee (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-2>).

Note: Due to storage limitations in the court office, some older case event lists and post- court dockets may not be immediately available at the court counter. The time required to access older lists and dockets that are not stored in the court office might be longer.

4.8 Other Documents Related to Family Cases

Other documents may be contained in the court file, even though they have not been filed in the case within the meaning of s. 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>). Because section 137 does not apply to these documents, they are not automatically publicly accessible. Some examples of these documents include:

- correspondence between the trial coordinator and the parties to canvass available dates for events;
- correspondence between the court office and an individual regarding fees paid to court (for example, regarding an NSF cheque)
- correspondence between the court office and an institution/agency (for example, police, Family Responsibility Office, Registrar General) necessary for the institution/agency to enforce or register an order; and
- fee waiver information.

These documents must be filed in the correspondence pocket within the court file. Court staff must remove the correspondence pocket from the file before providing the file to a member of the public for inspection.

Section 5: Public access to enforcement files

496.1 Documents in the enforcement file covered by section 137 of the *Courts of Justice Act*

Enforcement documents filed with the court fall under section 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>) (CJA) and are therefore publicly accessible, upon payment of the prescribed fee and provided that no statutory provision, common law rule or court order restricts access.

Examples of these documents include:

- writs;
- orders;
- schemes of distribution;
- notices of garnishment; and
- any other documents provided to the enforcement office on a form prescribed by the rules of the court.

5.2 Other documents in the enforcement file

Other documents may be contained in the enforcement file, even though they have not been filed in the proceeding within the meaning of s. 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>). These documents are not automatically publicly accessible, and include any correspondence or material created or required by the enforcement office in order to conduct an enforcement (for example, appraisals, notice of sale, contracts for storage of seized goods, etc.).

For information on access to documents needed to enforce a support obligation, see section “4.2.4 Proceedings under the *Family Responsibility and Support Arrears Enforcement Act*, 1996 (<https://www.ontario.ca/document/access-court-files-and-documents/public-access-family-court-files#section-1-3>)”.

Section 6: Public access to exhibits

6.1 Exhibits in criminal cases

Exhibits may take many forms. Examples include:

- physical evidence (for example, guns, knives, clothing);
- photographic/electronic evidence (for example, photos, videotapes, audiotapes, compact discs);
- business documents (for example, phone records, bank records, business transaction records);
- expert reports (for example, psychiatric reports, crime scene analyses, toxicologist reports);
- forensic documents; and
- intoxilyzer technician's certificates of analysis.

Judicial consent is required to obtain access to court exhibits. Media and members of the public may fill out a simple request form (<http://ontariocourtforms.on.ca/en/access-to-exhibits-1/>) that will be submitted to the presiding judicial official, or if that individual is unavailable, to the Local Administrative Justice. The judicial official will provide direction about whether access may be granted (including any terms and conditions of access) or whether a formal application, on notice to the parties, is required to balance access rights, privacy interests and the proper administration of justice.

Media and members of the public should direct their inquiries to court staff who will provide a copy of the request form (<http://ontariocourtforms.on.ca/en/access-to-exhibits-1/>) and seek judicial direction about what is required in a particular case.

Returned Exhibits

An exhibit may be returned to the party who filed it upon the completion of the legal proceedings and after the relevant appeal period has expired. If an exhibit is no longer in the court's possession, an individual seeking access to the record/item may make a request to the party directly. If the party denies access, a formal application may be brought to the court where the proceedings were heard.

Exhibit Lists

An exhibit list is prepared in every criminal case to record all exhibits entered into court. Exhibit lists are publicly accessible documents unless they contain information about matters that are sealed or were held in camera.

498.2 Exhibits in civil and family cases

6.2.1 Exhibits filed in a proceeding

If the exhibit was attached to an affidavit and filed with the court, it is a document filed in a proceeding and is publicly accessible under section 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>) (CJA) unless a statutory provision, common law rule or court order restricts access.

6.2.2 Exhibits referred to in an affidavit

If an exhibit is referred to in an affidavit as being produced and shown to the deponent, the party does not attach the exhibit to the affidavit. Instead, the party leaves the exhibit with the registrar/clerk for the court's use. In this case, the exhibit is not "filed" with the court and is not accessible under s. 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>).

6.2.3 Exhibits entered into evidence during trial

If the exhibit was entered into evidence in the course of a trial (meaning, marked, numbered and entered on a list by the registrar/clerk), the exhibit is not "filed" in the proceeding and is therefore not covered by s. 137. These exhibits are within the control of the court and are not publicly accessible, except with judicial consent.

Members of the public may fill out a simple request form (<http://ontariocourtforms.on.ca/en/access-to-exhibits-1/>) that will be submitted to the presiding judicial official, or if that individual is unavailable, to the Local Administrative Justice. The judicial official will provide direction about whether access may be granted (including any terms and conditions of access) or whether a formal application, on notice to the parties, is required to balance access rights, privacy interests and the proper administration of justice.

Media and members of the public should direct their inquiries to court staff who will provide a copy of the request form (<http://ontariocourtforms.on.ca/en/access-to-exhibits-1/>) and seek judicial direction about what is required in a particular case.

6.2.4 Copies of exhibits in exhibit books

Since exhibit books are documents filed with the court within the meaning of s. 137 of the *Courts of Justice Act* (<https://www.ontario.ca/laws/statute/90c43#BK184>), copies of

Exhibits contained in an exhibit book and filed with the Court of Appeal are publicly accessible, unless a statutory provision, common law rule or court order restricts access.

Section 7: Fees for public access to court documents

Note: Fees are subject to change.

7.1 Fees to access criminal court documents

7.1.1 Ontario Court of Justice and Superior Court of Justice

There is no charge to access criminal court documents or search criminal court files in the Ontario Court of Justice and Superior Court of Justice.

There is a fee to obtain a copy of a criminal court document. The Ontario Court of Justice fee schedule and the Superior Court of Justice fee schedule, which are regulations made under the *Administration of Justice Act* (<https://www.ontario.ca/laws/statute/90a06>), set out the fee to be paid whenever a member of the public requests and is granted copies of all or portions of a criminal court record. The following copy fees apply:

- for copies of documents in provincially-administered Ontario Court of Justice courts:
 - not requiring certification, \$1.00 per page
 - requiring certification, \$3.50 per page
- for copies of documents in municipally-administered Ontario Court of Justice courts, also known as *Provincial Offences Act* (<https://www.ontario.ca/laws/statute/90p33>) courts:
 - not requiring certification, \$1.00 or \$2.00 per page (depending on the municipality)
 - requiring certification, \$3.50 per page
- for copies of Superior Court of Justice documents:
 - not requiring certification, \$1.00 per page
 - requiring certification, \$4.00 per page

Copies of informations, indictments and judicial interim release documents shall be provided upon request to the accused and their counsel of record without copy fees being charged. Copies of *Prevention of and Remedies for Human Trafficking, 2017* (<https://www.ontario.ca/laws/statute/17p12>) restraining order court files and documents shall be provided upon request to parties and their counsel of record without copy fees being charged. Requests should be made in person at the counter or in writing by mail or email.

7.2 Fees to access civil and family court documents and enforcement documents

7.2.1 Ontario Court of Justice

There is no fee to access court documents in the Ontario Court of Justice. Access to court documents, where there is no statutory provision or court order that restricts access, may be obtained at the originating or filing court. There is a fee to obtain a copy of a document. See Section 7.3.

7.2.2 Superior Court of Justice, and Court of Appeal for Ontario, Small Claims Court, and Enforcement Offices (Sheriff)

There is no fee to access court documents in:

- the Family Court branch of the Superior Court of Justice; and
- family cases heard by the Superior Court of Justice that are not appeals.

There is a fee to obtain a copy of a document in the Family Court Branch and in non-appeal family cases heard by the Superior Court of Justice. See Section 7.3.

There **is** a fee to access court documents in:

- the Court of Appeal,
- civil cases in the Superior Court of Justice, including estates, bankruptcy, and Divisional Court proceedings,
- family appeals in the Superior Court of Justice,
- the Small Claims Court, and
- Enforcement Offices (the Sheriff)

The following chart summarizes the prescribed fees under the *Administration of Justice Act* (<https://www.ontario.ca/laws/statute/90a06>) to access court documents in the above courts and court proceedings. There are also fees to obtain a copy of a document. See Section 7.3.

Service	Fee in the Superior Court of Justice and Court of Appeal (excluding family cases that are not appeals) (O. Reg. 293/92 (https://www.ontario.ca/laws/regulation/920293))	Fee in the Small Claims Court (O. Reg. 332/16 (https://www.ontario.ca/laws/regulation/160332))	Fee in the Enforcement/Sheriff's Office (O. Reg. 294/92 (https://www.ontario.ca/laws/regulation/920294))
Inspection of court file by a solicitor* or party in the proceeding	no charge	no charge	N/A
Inspection of court file by a person who has entered into an agreement with the Attorney General for the bulk	\$4.00 (per file)	\$1.00 (per file)	N/A

inspection of court files			
Inspection of court file by any other person	\$11.00 (per file)	\$11.00 (per file)	N/A *****
Retrieval of a court file from storage	\$83.00	\$83.00	N/A *****
For a search for writs (per name searched)	N/A *****	N/A *****	\$13.10
For a report showing the details of a writ, lien or order (per report)	N/A *****	N/A *****	\$7.10 (maximum \$71.55 per name)

[N/A] means either there is no prescribed fee for the service or the service does not exist in the specified court or office.

[*] Note: Refers to a solicitor for a party in the proceedings, not any solicitor in general.

7.3 Copy fees

The following chart summarizes copy, certified copy and digital recording copy fees prescribed under the *Administration of Justice Act* (<https://www.ontario.ca/laws/statute/90a06>) for each type of court or court proceeding and the Enforcement Offices (Sheriff).

Level of court	Fee for a certified copy (per page)	Fee for a non-certified copy (per page)	Fee for CD copy of a digital recording of a court hearing - a single day's recording	Fee for CD copy of a digital recording of a court hearing - each additional day's recording, if the request is made at the same time as a request for a single day's recording
Superior Court of Justice and Court of Appeal – Fees O. Reg. 293/92 ***** (https://www.ontario.ca/laws/regulation/920293)	\$4.00 [**]]	\$1.00 [**]	\$23.00 [**]	\$11.00 [**]
Superior Court of Justice - Family Court - Fees O. Reg. 417/95 ***** (https://www.ontario.ca)	\$4.00	\$1.00	\$23.00	\$11.00

a/laws/reg ulation/950 417)				
Small Claims Court – Fees and Allowances - O. Reg. 332/16 (https://ww w.ontario.c a/laws/reg ulation/160 332/)	\$4 . 00	\$1.00	\$23.00	\$11.00
Ontario Court of Justice – Fees O. Reg. 210/07 (https://ww w.ontario.c a/laws/reg ulation/070 210)	\$3 . 50 [**]	\$1.00 for provincial ly administer ed courts and either \$1.00 or \$2.00 for municipall y administer ed courts. [**]	\$22.00 [**]	\$10.50 [**]
Enforceme nt/Sheriff's Office O. Reg. 294/92 (https://ww	\$3 . 50 [*]	\$1.00 [*]	–	–

[*] For documents other than writs of execution, orders and certificates of lien. See section “7.2.2 Superior Court of Justice, Court of Appeal for Ontario, Small Claims Court, and Enforcement Offices (Sheriff)” (<https://www.ontario.ca/document/access-court-files-and-documents/fees-public-access-court-documents#section-1-1>) for fees for copies of a report showing the details of a writ, lien or order.

[**] These fees are not payable by, or on behalf of, a party to an application for or appeal of a restraining order under the *Prevention of and Remedies for Human Trafficking Act, 2017* (<https://www.ontario.ca/laws/statute/17p12>) .

7.3.1 Fees for copies of endorsements

Court staff must provide copies of endorsements to parties to a case or their lawyer at no charge.

7.4 Fee waiver

There is a fee waiver mechanism for persons who might otherwise be denied access to justice because of their financial circumstances. Learn more about having court fees waived (<https://www.ontario.ca/page/have-your-court-fees-waived>) .

506

☐ L ☐ S

Information Number / N° de la dénonciation

☐ Non-Disclosure Order Pursuant to S. 486.31
Ordonnance de non-divulgence, art. 486.31
☐ Non-communication s. 515(12) & 516(2)
Non-communication, par. 515(12) et 516(2)

☐ Publication ban pursuant to
Interdiction de publication en vertu de
☐ Provisions of 530(3) Complied With
Dispositions du par. 530 (3) observées

Arrest Date:

Date d'arrestation

15 month Flag:

Alerte à 15 mois

18 month Flag:

Alerte à 18 mois

Sworn Date:

Date d'assermentation

15 month Flag:

Alerte à 15 mois

18 month Flag:

Alerte à 18 mois

CANADA
PROVINCE OF ONTARIO
PROVINCE DE L'ONTARIO

Information of:

Dénonciation de :

of
de

(Region / Région)

(occupation / profession)

The informant says that **he/she** believes on reasonable grounds that
Le dénonciateur déclare qu'il a des motifs raisonnables de croire que

[Accused / Accusé]

(Last Name, First Name) (*nom, prénom*)

[Address / adresse]

(Date of birth / date de naissance)

(Day / jour) / (Month / mois) / (Year / année)

(enter charges here / insérer des accusations ici)

647-508

☐ Information Number
de la dénonciation

☐ Designation Filed
Désignation déposée

394

☐ Language Notification
Avis de langue

☐ Interpreter Required
Interprète requis

Date	Accused Accusé	Adjournment Date Date d'ajournement	Adjournment Details Détails sur l'ajournement	Designation Désignation	Counsel As Agent Avocat mandataire	Fails to Appear Ornet de comparaître	Bench Warrant Mandat d'arrêt	Discretion Discrétion	Certificate of Default Certificat de défaut

Date	Clerk Greffier	Crown Couronne	For the Accused Pour l'accusé	Justice's initials Initiales du juge

509 Information Number / N°(s) de dénonciation

☐ **To be completed where information is laid other than in person:** I, ..., state that
À remplir lorsque la dénonciation est déposée autrement qu'en personne : Je soussigné(e) (name of informant / nom du dénonciateur) déclare que
 all matters contained in this information are true to my knowledge and belief, pursuant to s. 508.1 (2) of the *Criminal Code*.
 tous les renseignements contenus dans la présente dénonciation sont, à ma connaissance, véridiques, en vertu de par. 508.1 (2) du Code criminel.

☐ Deemed to be sworn / Réputée être faite sous serment

Sworn/affirmed before me at the
 Déclaré sous serment/affirmé solennellement devant moi à/au

of / de

in the Province of Ontario / dans la province de l'Ontario

this day of, 20
 ce jour de

Informant / Dénonciateur

Justice of the Peace / Juge de paix

☐ Appearance Notice ☐ Promise to Appear ☐ Recognizance
 Citation à comparaître Promesse de comparaître Engagement
 for , 20
 pour le (day, month / jour, mois)

CHECK ONE OF THE FOLLOWING / COCHEZ LA CASE QUI CONVIENT

☐ Cancelled – Police to notify defendant ☐ Cancelled – Summons ☐ Confirmed on , 20
 Annulé(e) – La police informera la partie défenderesse Sommation Confirmé(e) le (day, month / jour, mois)
☐ Cancelled - Warrant issued
 Annulé(e) – Mandat délivré

Justice of the Peace / Juge de paix

Justice of the Peace / Juge de paix

(day, month / jour, mois)

Date Date	Crown Elects to Proceed La Couronne choisit de procéder par	☐ Summarily Procédure sommaire	☐ By Indictment Acte d'accusation	☐ Summary Conviction Offence(s) Infraction(s) punissable(s) sur déclaration de culpabilité par procédure sommaire	☐ Indictable Offence(s) Infraction(s) punissable(s) par mise en accusation			
Date Date	Accused Accusé	Elects Trial by Choix d'un procès devant		Preliminary Hearing Requested Enquête préliminaire demandée	Justice Initials Initiales du juge	Abs. Juris. Comp. absolue	Pleads Plaide	
		Superior Court Cour supérieure	Ontario Court Cour de l'Ontario				Guilty to Counts Coupable aux chefs d'accusation	Not Guilty to Counts Non coupable aux chefs d'accusation
		Judge Juge	Judge & Jury Juge et jury					

Date Date	Accused Accusé	Committed (or) Ord. Std. Trial *On Counts Renvoyé à procès pour les chefs d'accusation	Discharged on Counts Libéré des chefs d'accusation	Found / Reconnu	
				Guilty on Counts Coupable des chefs d'accusation	Not Guilty on Counts Non coupable des chefs d'accusation

* ☐ With consent of accused and prosecutor, without taking or recording
 Avec le consentement de l'accusé et du poursuivant, sans recueillir ou consigner
☐ (a) any evidence (or) ☐ (b) further evidence
 a) des preuves (ou) b) des preuves additionnelles

Judge / Juge

Count / Chef		Sentence date / Date de détermination de la peine		☐ Withdrawn / Accusation retirée	
☐ Pre-sentence custody	days/months	Time credited:	days/months	☐ concurrent with	
<i>Détention sous garde avant prononcé de</i>	<i>jours/mois</i>	<i>Crédit octroyé</i>	<i>jours/mois</i>	<i>concurrente avec</i>	
☐ Term that would have been imposed before credit granted:	days/months/years				
<i>Période d'emprisonnement imposée avant l'octroi de tout crédit</i>	<i>jours/mois/ans</i>				
☐ Absolute discharge	☐ Conditional discharge	☐ Suspended sentence			
<i>Absolution inconditionnelle</i>	<i>Absolution conditionnelle</i>	<i>Condamnation avec sursis</i>			
☐ Imprisoned for	days/months/years	☐ concurrent with	☐ consecutive to		
<i>Emprisonnement pour</i>	<i>jours/mois/ans</i>	<i>concurrent avec</i>	<i>consécutif à</i>		
☐ Intermittent sentence for	days	☐ concurrent with	☐ consecutive to		
<i>Peine discontinuée</i>	<i>jours</i>	<i>concurrente avec</i>	<i>consécutif à</i>		
☐ Conditional sentence for	days/months/years	☐ concurrent with	☐ consecutive to		
<i>Ordonnance de sursis</i>	<i>jours/mois/ans</i>	<i>concurrente avec</i>	<i>consécutif à</i>		
☐ Probation	months/years	☐ concurrent with	☐ consecutive to		
<i>Période de probation</i>	<i>mois/ans</i>	<i>concurrente avec</i>	<i>consécutif à</i>		
☐ Community service s.732.1(3)(f) / <i>Service communautaire, par. 732.1(3)(f)</i>					
☐ Fine of \$		VS \$	Time to pay	Days in default	
<i>Amende de</i>		<i>\$ sur. comp.</i>	<i>\$ Délai de paiement</i>	<i>Jours à défaut</i>	
☐ Restitution	☐ s. 738 / s. 739	Amount: \$	Time to pay		
<i>Dédommagement</i>	<i>art. 738 / art. 739</i>	<i>Montant</i>	<i>\$ Délai de paiement</i>		
☐ Victim surcharge: \$	Time to pay:			Days in default	
<i>Suramende compensatoire</i>	<i>\$ Délai de paiement</i>			<i>Jours à défaut</i>	
☐ Ordered to stand trial: / <i>Renvoyé pour subir son procès</i>					
☐ Dismissed	☐ Driving prohibition:	☐ HTA cautioned	Months / Years	☐ s.743.21(1) / <i>par. 743.21(1)</i>	
<i>Rejeté</i>	<i>Interdiction de conduite</i>	<i>Avertissement (Code de la route)</i>	<i>mois/années</i>		
☐ Acquitted	☐ Weapons prohibition:	☐ s. 109(2):	years ☐ s. 109(3) (Life)	☐ s. 110:	☐ s. 110 (life)
<i>Acquitté</i>	<i>Interdiction d'armes</i>	<i>par. 109(2)</i>	<i>ans par. 109(3)(perpétuité)</i>	<i>art 110</i>	<i>ans art .110 (perpétuité)</i>
☐ Stayed	☐ DNA:	☐ 5.03 (Primary)	☐ 5.04 (Secondary)	☐ Denied (DND)	
<i>Sursis</i>	<i>ADN</i>	<i>5.03 (primaire)</i>	<i>5.04 (secondaire)</i>	<i>Rejetée</i>	
☐ In Absentia	☐ S.O.I.R.A. order:	☐ 10 years	☐ 20 years	☐ Life	
<i>In absentia</i>	<i>Ordonnance LERDS</i>	<i>10 ans</i>	<i>20 ans</i>	<i>Perpétuité</i>	
☐ Other	☐ s. 161 prohibition:	months/years	☐ s. 490 forfeiture order:	☐ Granted	☐ Denied
<i>Autre</i>	<i>Interdiction, art. 161</i>	<i>mois/ans</i>	<i>Ordonnance de confiscation, art. 490</i>	<i>Accordée</i>	<i>Rejetée</i>

Count / Chef		Sentence date / Date de détermination de la peine		☐ Withdrawn / Accusation retirée	
☐ Pre-sentence custody	days/months	Time credited:	days/months	☐ concurrent with	
<i>Détention sous garde avant prononcé de</i>	<i>jours/mois</i>	<i>Crédit octroyé</i>	<i>jours/mois</i>	<i>concurrente avec</i>	
☐ Term that would have been imposed before credit granted:	days/months/years				
<i>Période d'emprisonnement imposée avant l'octroi de tout crédit</i>	<i>jours/mois/ans</i>				
☐ Absolute discharge	☐ Conditional discharge	☐ Suspended sentence			
<i>Absolution inconditionnelle</i>	<i>Absolution conditionnelle</i>	<i>Condamnation avec sursis</i>			
☐ Imprisoned for	days/months/years	☐ concurrent with	☐ consecutive to		
<i>Emprisonnement pour</i>	<i>jours/mois/ans</i>	<i>concurrent avec</i>	<i>consécutif à</i>		
☐ Intermittent sentence for	days	☐ concurrent with	☐ consecutive to		
<i>Peine discontinuée</i>	<i>jours</i>	<i>concurrente avec</i>	<i>consécutif à</i>		
☐ Conditional sentence for	days/months/years	☐ concurrent with	☐ consecutive to		
<i>Ordonnance de sursis</i>	<i>jours/mois/ans</i>	<i>concurrente avec</i>	<i>consécutif à</i>		
☐ Probation	months/years	☐ concurrent with	☐ consecutive to		
<i>Période de probation</i>	<i>mois/ans</i>	<i>concurrente avec</i>	<i>consécutif à</i>		
☐ Community service s.732.1(3)(f) / <i>Service communautaire, par. 732.1(3)(f)</i>					
☐ Fine of \$		VS \$	Time to pay	Days in default	
<i>Amende de</i>		<i>\$ sur. comp.</i>	<i>\$ Délai de paiement</i>	<i>Jours à défaut</i>	
☐ Restitution	☐ s. 738 / s. 739	Amount: \$	Time to pay		
<i>Dédommagement</i>	<i>art. 738 / art. 739</i>	<i>Montant</i>	<i>\$ Délai de paiement</i>		
☐ Victim surcharge: \$	Time to pay:			Days in default	
<i>Suramende compensatoire</i>	<i>\$ Délai de paiement</i>			<i>Jours à défaut</i>	
☐ Ordered to stand trial: / <i>Renvoyé pour subir son procès</i>					
☐ Dismissed	☐ Driving prohibition:	☐ HTA cautioned	Months / Years	☐ s.743.21(1) / <i>par. 743.21(1)</i>	
<i>Rejeté</i>	<i>Interdiction de conduite</i>	<i>Avertissement (Code de la route)</i>	<i>mois/années</i>		
☐ Acquitted	☐ Weapons prohibition:	☐ s. 109(2):	years ☐ s. 109(3) (Life)	☐ s. 110:	☐ s. 110 (life)
<i>Acquitté</i>	<i>Interdiction d'armes</i>	<i>par. 109(2)</i>	<i>ans par. 109(3)(perpétuité)</i>	<i>art 110</i>	<i>ans art .110 (perpétuité)</i>
☐ Stayed	☐ DNA:	☐ 5.03 (Primary)	☐ 5.04 (Secondary)	☐ Denied (DND)	
<i>Sursis</i>	<i>ADN</i>	<i>5.03 (primaire)</i>	<i>5.04 (secondaire)</i>	<i>Rejetée</i>	
☐ In Absentia	☐ S.O.I.R.A. order:	☐ 10 years	☐ 20 years	☐ Life	
<i>In absentia</i>	<i>Ordonnance LERDS</i>	<i>10 ans</i>	<i>20 ans</i>	<i>Perpétuité</i>	
☐ Other	☐ s. 161 prohibition:	months/years	☐ s. 490 forfeiture order:	☐ Granted	☐ Denied
<i>Autre</i>	<i>Interdiction, art. 161</i>	<i>mois/ans</i>	<i>Ordonnance de confiscation, art. 490</i>	<i>Accordée</i>	<i>Rejetée</i>

No. of Information / N° de la dénonciation	
Return Date / Date à laquelle le document est rapporté , 20	

INFORMATION Against / DÉNONCIATION visant

Address / Adresse

CHARGE / ACCUSATION

Refer to front page for further counts. / Reportez-vous à la première page pour plus de chefs.

FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT									
☐ Summons Sommotion		☐ Show Cause Audience de justification		☐ Warrant 1 st Mandat en 1 ^{re} instance		Re-laid Information Dénouciation de remplacement			
Reportable M.V. Offence (H.T.A. 199) ☐ Infraction V.M. à déclarer (Code de la route 199)		C.V.O.R. No (Commercial Vehicles Only) Numéro C.E.C.V.U. (véhicules utilitaires seulement)							
Sex	Birth Date / Date de naissance	Day / Month / Jour / Mois		Year / Année		Was defendant owner? La partie défenderesse était-elle propriétaire?		☐ Yes / Oui ☐ No / Non	
Driver's Licence Number / Numéro du permis de conduire									
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction liée à un accident							
Informant Dénouciateur									
Date Sworn Date d'assermentation		Date of Arrest Date de l'arrestation				No. / N°			
Officer / Agent de police		Div. / Dist.							
Occurrence Number / N° d'incident									
Courtroom / Salle d'audience									
At / À(Au)									

No. of Information / N° de la dénonciation	
Return Date / Date à laquelle le document est rapporté , 20	

INFORMATION Against / DÉNONCIATION visant

Address / Adresse

CHARGE / ACCUSATION

Refer to front page for further counts. / Reportez-vous à la première page pour plus de chefs.

FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT									
☐ Summons Sommotion		☐ Show Cause Audience de justification		☐ Warrant 1 st Mandat en 1 ^{re} instance		Re-laid Information Dénouciation de remplacement			
Reportable M.V. Offence (H.T.A. 199) ☐ Infraction V.M. à déclarer (Code de la route 199)		C.V.O.R. No (Commercial Vehicles Only) Numéro C.E.C.V.U. (véhicules utilitaires seulement)							
Sex	Birth Date / Date de naissance	Day / Month / Jour / Mois		Year / Année		Was defendant owner? La partie défenderesse était-elle propriétaire?		☐ Yes / Oui ☐ No / Non	
Driver's Licence Number / Numéro du permis de conduire									
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction liée à un accident							
Informant Dénouciateur									
Date Sworn Date d'assermentation		Date of Arrest Date de l'arrestation				No. / N°			
Officer / Agent de police		Div. / Dist.							
Occurrence Number / N° d'incident									
Courtroom / Salle d'audience									
At / À(Au)									

No. of Information / N° de la dénonciation	
Return Date / Date à laquelle le document est rapporté , 20	

INFORMATION Against / DÉNONCIATION visant

Address / Adresse

CHARGE / ACCUSATION

Refer to front page for further counts. / Reportez-vous à la première page pour plus de chefs.

FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT									
☐ Summons Sommotion		☐ Show Cause Audience de justification		☐ Warrant 1 st Mandat en 1 ^{re} instance		Re-laid Information Dénouciation de remplacement			
Reportable M.V. Offence (H.T.A. 199) ☐ Infraction V.M. à déclarer (Code de la route 199)		C.V.O.R. No (Commercial Vehicles Only) Numéro C.E.C.V.U. (véhicules utilitaires seulement)							
Sex	Birth Date / Date de naissance	Day / Month / Jour / Mois		Year / Année		Was defendant owner? La partie défenderesse était-elle propriétaire?		☐ Yes / Oui ☐ No / Non	
Driver's Licence Number / Numéro du permis de conduire									
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction liée à un accident							
Informant Dénouciateur									
Date Sworn Date d'assermentation		Date of Arrest Date de l'arrestation				No. / N°			
Officer / Agent de police		Div. / Dist.							
Occurrence Number / N° d'incident									
Courtroom / Salle d'audience									
At / À(Au)									



Ontario

Driver's Licence
Permis de conduireON
CANADA

1,2 NAME/ NOM

MCLEAN,
KEVIN, ALEXANDER8 410-775 KING ST W
TORONTO, ON, M5V 2K34d NUMBER/
NUMÉROM1651 - 43318 - 30325 1

4a ISS/ DÉL.

2024/06/26

4b EXP/ EXP.

2029/03/25

6 DD/ RÉF.

IC7664935

16 HGT/ HAUT.

188 cm

15 SEX/ SEXE

M

9 CLASS/
CATÉG.

G

12 REST/
COND.

3 DOB/DDN 1983/03/25

M1651-43318-30325
1983/03/25

☒ IPV (Intimate Partner Violence / *Violence contre un partenaire intime*) ☐ Replacement Information / *Dénonciation de remplacement*
☐ S (Impaired driving with substances / *Conduite avec capacités affaiblies par des substances*) ☐ V (Vessel / *Bateau*)

Arrest Date: _____ 15 month Flag: _____ 18 month Flag: _____
Date d'arrestation _____ Alerte à 15 mois (ddmmyy / jjmmaa) Alerte à 18 mois (ddmmyy / jjmmaa)
Sworn Date: 230924 15 month Flag: 241225 18 month Flag: 250326
Date d'assermentation _____ Alerte à 15 mois (ddmmyy / jjmmaa) Alerte à 18 mois (ddmmyy / jjmmaa)

4810 998 24 48129169

Information Number / N° de la dénonciation

NOTICE: Orders concerning this court Information relating to publication bans, non-disclosure/communication and French-language rights, are available on a separate page and **must** be followed.

AVIS: Les ordonnances liées à la présente dénonciation en ce qui a trait aux interdictions de publication, à la non-divulgaration ou à la non-communication et aux droits linguistiques des francophones figurent sur une page distincte. Ces ordonnances **doivent** être respectées.

Form 2 Information / Formule 2 Dénonciation

Sections 506, 508.1 and 788 of the Criminal Code / *Articles 506, 508.1 et 788 du Code criminel*

CANADA
PROVINCE OF ONTARIO
PROVINCE DE L'ONTARIO
TORONTO
(Region / *Région*)

Information of: **Christyn Frugoni-Rojas**
Dénonciation de :
of **THE CITY OF TORONTO**
de
hereinafter called the informant / *ci-après appelé(e) le dénonciateur*

Court Officer
(occupation / *profession*)

(1) **MCLEAN, Kevin** DOB: 25 Mar. 1983
NFA, , ON

COUNT 1

Kevin MCLEAN

on or about the 22nd day of September in the year 2024 at the City of Toronto in the Toronto Region did, without lawful authority and knowing that another person, namely Nicole ARTOPOULOS, was harassed or recklessly as to whether that person was harassed, engage in repeatedly communicating with, either directly or indirectly, that person, and cause the said Nicole ARTOPOULOS to reasonably fear for personal safety, contrary to Section 264, subsection (2), clause (b) of the Criminal Code of Canada.

----- **End of Charges/Counts** -----

Declaration of Informant / Déclaration du dénonciateur

I declare that all matters contained in the Information are true to my knowledge and belief, pursuant to s. 508.1(2) of the *Criminal Code*.

Je soussigné(e) déclare tous les renseignements contenus dans la présente dénonciation sont, à ma connaissance, véridiques, en vertu de par. 508.1(2) du Code criminel.

Dated at **CITY of TORONTO** in the Province of Ontario, this **23rd** day of **SEPTEMBER**, 20 **24**
Fait à(au) *dans la province d'Ontario, ce* *jour de*

Declared / Déclaré

Christyn
Frugoni-
Rojas CL (M)

Digitally signed by
Christyn Frugoni-
Rojas CL (M)
Date: 2024.09.23
11:48:25 -04'00'

Digital Signature of Informant / Signature numérique du dénonciateur

515
Traffic Court Endorsement

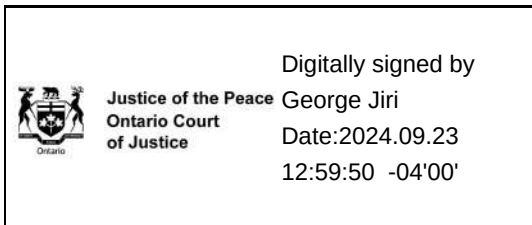
This Information is Accepted on its face.

Kevin MCLEAN:

Warrant In The First: Issue

Dated in the Province of Ontario, this 23rd day of September 2024.

Fait à/au dans la province de l'Ontario, ce 23 septembre 2024.



This document has been digitally signed. / Ce document a été signé numériquement.

Arrest Date: _____	15 month Flag: _____	18 month Flag: _____
<i>Date d'arrestation</i>	<i>Alerte à 15 mois (ddmmyy / jjmmaa)</i>	<i>Alerte à 18 mois (ddmmyy / jjmmaa)</i>
Sworn Date: 230924	15 month Flag: 241225	18 month Flag: 250326
<i>Date d'assermentation</i>	<i>Alerte à 15 mois (ddmmyy / jjmmaa)</i>	<i>Alerte à 18 mois (ddmmyy / jjmmaa)</i>

[] **Accused notified court under s. 530(3)**
Tribunal avisé par l'accusé en vertu de l'art. 530(3)

[] **Designation Filed**
Désignation déposée

[] **Interpreter Required**
Interprète requis

Date Date	Accused Accusé	Adjournment Date Date d'ajournement	Adjournment Details Détails sur l'ajournement	Designation Désignation	Counsel As Agent Avocat mandataire	Fails to appear Omet de comparaître	Bench Warrant Mandat d'arrêt	Discretion Discretion	Certificate of Default Certificat de défaut
03 Oct 2024	MCLEAN, KEVIN	13 Nov 2024	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, FA, VI, ACP - Warrant in the First Executed						
13 Nov 2024	MCLEAN, KEVIN	18 Dec 2024	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, ACP - - DISC BW			X	X	X	
18 Dec 2024	MCLEAN, KEVIN	19 Mar 2025	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, ACP - -11b waived - - DISC BW Rescinded						
19 Mar 2025	MCLEAN, KEVIN	16 Apr 2025	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, APN - - DISC BW			X	X	X	
16 Apr 2025	MCLEAN, KEVIN	14 May 2025	Toronto-OCJ-T-10 Armoury St - 204 @ 2:00 PM, ST, VI, ACP - - DISC BW Rescinded						
14 May 2025	MCLEAN, KEVIN	11 Jun 2025	Toronto-OCJ-T-10 Armoury St - 702 @ 2:00 PM, ST, VI, ACP						

Date Date	Clerk Greffier	Crown Couronne	For the Accused Pour l'accusé	Justice's Initials Initiales du juge
03 Oct 2024	Henriquez, Michael	NA	NP, NA, NOR	DJ
13 Nov 2024	Nurali, Saira	Pashang, Sia	NP, NP (Acc appeared in triage), NRC	TC
18 Dec 2024	Barna, Elizabeth	Dimiskovska, Andrea	AA, AA, VI, Self-Rep , NRC	JG
19 Mar 2025	Weisemberg, Iara	Laws, Jennifer	NP, NRC	JR
16 Apr 2025	Berhane, Aron	Dimiskovska, Andrea	AA, Self-Rep, NRC	BS
14 May 2025	Booth, Catherine	Laws, Jennifer	AA, Self-Rep, NRC	BS

[] **At Bail Review date**
À la révision de l'ordonnance de détention, datee du

[] **Original Order**
Confirmed
Ordonnance originale
Confirmée

[] **New Order**
Made
Nouvelle
ordonnance
rendue

[] **Gladue Report**
Requested
Rapport Gladue
demandé

(date / date)

Information No. / N° de la dénonciation				
Return Date / Date à laquelle le document est rapporté _____, 20__				
INFORMATION Against / DÉNONCIATION visant MCLEAN, Kevin				
Address / Adresse NFA , ON				
CHARGE / ACCUSATION HARASSMENT BY REPEATED COMMUNICATION WITH PERSON				
Refer to front page for further counts / Reportez-vous à la première page pour plus de chefs				
FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT				
☐ Summons Sommaton	☐ Show Cause Audience de justification	☒ Warrant 1 st Mandat en 1 ^{re} instance		
☐ Replacement Information / Dénonciation de remplacement				
☐ Reportable M.V. Offence (H.T.A. 199) Infraction V.M. à déclarer (Code de la route 199)	C.V.O.R. No (Commercial Vehicles Only) Numéro C.I.U.V.U. (véhicules utilitaires seulement)			
Sex Sexe M	Birth Date / Date de naissance Day / Jour Month / Mois Year / Année 25 03 1983	Was defendant owner? La partie défenderesse était-elle propriétaire? ☐ Yes / Oui ☐ No / Non		
Driver's Licence Number / Numéro du permis de conduire M16514331830325				
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction reliée à un accident		
Informant Dénonciateur Christyn Frugoni-Rojas				
Deemed Sworn /Affirmed Date SEP 23rd, 24 Réputée être déclarée sous serment/affirmée solennellement le		Date of Arrest Date de l'arrestation		
Officer / Agent de police KOLANKOWSKI, MI		No. / N° 82239		
Police Agency / Service de police TORONTO POLICE SERVIC		Div. / Dist. 14 DIVISION		
Occurrence Number / N° d'incident 24-2082035				
Courtroom / Salle d'audience				
At / À(Au) OCJT #204 IPV SOUTH 10 ARMOURY ST, TORONTO ON M7A 0B9				

Information No. / N° de la dénonciation				
Return Date / Date à laquelle le document est rapporté _____, 20__				
INFORMATION Against / DÉNONCIATION visant				
Address / Adresse				
CHARGE / ACCUSATION				
Refer to front page for further counts / Reportez-vous à la première page pour plus de chefs				
FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT				
☐ Summons Sommaton	☐ Show Cause Audience de justification	☐ Warrant 1 st Mandat en 1 ^{re} instance		
☐ Replacement Information / Dénonciation de remplacement				
☐ Reportable M.V. Offence (H.T.A. 199) Infraction V.M. à déclarer (Code de la route 199)	C.V.O.R. No (Commercial Vehicles Only) Numéro C.I.U.V.U. (véhicules utilitaires seulement)			
Sex Sexe	Birth Date / Date de naissance Day / Jour Month / Mois Year / Année	Was defendant owner? La partie défenderesse était-elle propriétaire? ☐ Yes / Oui ☐ No / Non		
Driver's Licence Number / Numéro du permis de conduire				
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction reliée à un accident		
Informant Dénonciateur				
Deemed Sworn /Affirmed Date Réputée être déclarée sous serment/affirmée solennellement le		Date of Arrest Date de l'arrestation		
Officer / Agent de police		No. / N°		
Police Agency / Service de police		Div. / Dist.		
Occurrence Number / N° d'incident				
Courtroom / Salle d'audience				
At / À(Au)				

Information No. / N° de la dénonciation				
Return Date / Date à laquelle le document est rapporté _____, 20__				
INFORMATION Against / DÉNONCIATION visant				
Address / Adresse				
CHARGE / ACCUSATION				
Refer to front page for further counts / Reportez-vous à la première page pour plus de chefs				
FOR ADMINISTRATIVE PURPOSES ONLY À DES FINS ADMINISTRATIVES SEULEMENT				
☐ Summons Sommaton	☐ Show Cause Audience de justification	☐ Warrant 1 st Mandat en 1 ^{re} instance		
☐ Replacement Information / Dénonciation de remplacement				
☐ Reportable M.V. Offence (H.T.A. 199) Infraction V.M. à déclarer (Code de la route 199)	C.V.O.R. No (Commercial Vehicles Only) Numéro C.I.U.V.U. (véhicules utilitaires seulement)			
Sex Sexe	Birth Date / Date de naissance Day / Jour Month / Mois Year / Année	Was defendant owner? La partie défenderesse était-elle propriétaire? ☐ Yes / Oui ☐ No / Non		
Driver's Licence Number / Numéro du permis de conduire				
Plate No. / Numéro de plaque		☐ Involves a Collision Infraction reliée à un accident		
Informant Dénonciateur				
Deemed Sworn /Affirmed Date Réputée être déclarée sous serment/affirmée solennellement le		Date of Arrest Date de l'arrestation		
Officer / Agent de police		No. / N°		
Police Agency / Service de police		Div. / Dist.		
Occurrence Number / N° d'incident				
Courtroom / Salle d'audience				
At / À(Au)				

Passport No./N° de passeport

CAN

AS384006

MCLEAN

KEVIN ALEXANDER

Nationality/Nationalité
CANADIAN/CANADIENNE

25 MAR / MARS 83

M VANCOUVER CAN

19 JUNE/JUIN 23

19 JUNE/JUIN 33

TORONTO

P<CANMCLEAN<<KEVIN<ALEXANDER<<<<<<<<<<<<<<<<<

AS384004<7CAN8303257M3306194<<<<<<<<<<<<<<<08

U

7 5 3 8 4 0 0 4

2 3 2 3 2 3 2 3

327

815

404

Tab C





















TAB 15

Tab A

TO:

Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone: 647.370.9354

REFERENCE: Formal Request under the *Access to Information Act* (ATIA)

CROSS-REFERENCE: *Privacy Act* Request File P-2025-16999 / F339

SUBJECT: FORMAL SPECIFICATION OF REQUISITIONS UNDER THE ACCESS TO INFORMATION ACT (ATIA) – CPIC SYSTEMIC INTEGRITY, METADATA EXTRACTION, AND INTER-AGENCY COMMUNICATIONS

Dear ATIP Coordinator,

Please accept this correspondence as a formal request for access to records under the *Access to Information Act* (ATIA), R.S.C. 1985, c. A-1. The prescribed statutory application fee of \$5.00 is enclosed with the physical transmission of this document.

This ATIA requisition operates as a concurrent and supplementary filing to my existing *Privacy Act* request (RCMP File P-2025-16999 / F339). While the *Privacy Act* requisition strictly concerns my personal information and localized metadata, this ATIA request serves a broader, more profound democratic function: it targets the

419
341
533
searching institutional records, systemic metadata architecture, and inter-agency communications held by the Royal Canadian Mounted Police (RCMP).

As the supreme governance authority for the Canadian Police Information Centre (CPIC), the RCMP holds the ultimate fiduciary and statutory duty to maintain the uncorrupted "trust architecture" of the national law enforcement database. The CPIC apparatus is decidedly not a mere repository of administrative trivia, nor is it a passive bulletin board for municipal police forces. It is the central, incorruptible nervous system of the Canadian law enforcement apparatus. The entirety of the Canadian criminal justice system relies absolutely, without exception, on the unbroken chain of custody of sworn judicial documents. When a municipal constabulary engages a private citizen, the data retrieved from the CPIC terminal dictates the immediate trajectory of that citizen's physical liberty.

Therefore, when the cryptographic provenance of a sworn document is severed by state actors utilizing commercial manipulation software to alter jurisdictional realities, the resulting documentation ceases to operate as a lawful warrant. It devolves into a mere instrument of arbitrary coercion. The RCMP possesses a unique, extra-jurisdictional duty to ensure that its federal infrastructure is not being utilized as a digital laundry for the sanitization of local jurisdictional nullities.

The following specific technical artifacts and institutional records are formally requisitioned to verify the cryptographic provenance, expose the algorithmic manipulation, and confirm the jurisdictional integrity of the CPIC records associated with file P-2025-16999 / F339:

1. Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.

- **Contextual Justification:** Standard CPIC "Persons" file queries, which are utilized by frontline patrol officers on the street, are fundamentally insufficient for this inquiry. The graphical interface available to a patrol officer is subject to algorithmic filtering and reflects only the contemporaneous, operational status of a file. Only the immutable systemic ledgers housed deep within PPU 005—capturing the precise chronological sequence of ADD, MODIFY, CLEAR, and CANCEL commands—can definitively expose the temporal trajectory of state-actor malfeasance. The architectural reality of the CPIC database ensures that while a fraudulently altered warrant may be ostensibly excised from the active operational interface to hide the evidence of an unlawful arrest, the underlying digital artifact and the footprint of the user who deleted it are decidedly not eradicated from the federal infrastructural matrix.

2. Hexadecimal Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.

342 **Contextual Justification:** This mathematical data is strictly required to bypass the visual
534 homogenization inherent to the standard Graphical User Interface (GUI). The GUI is merely a
presentation layer; it can be manipulated to display a facially valid warrant even when the underlying
data structure is fatally corrupted. Only the uninterpreted binary and hexadecimal records—complete
with exact cryptographic memory offsets and ASCII/EBCDIC decoded text translations—can provide the
mathematical certitude required to prove vector morphology collapse. These immutable binary ledgers
circumvent human interpretation entirely. A raw hexadecimal dump shows the binary reality of the
database entry, demonstrating exactly when the foundational metadata was algorithmically disfigured
without lawful judicial authorization, and confirming if the payload matches the physical forged
documents.

3. Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping,
corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry
sessions that generated the "Frankenstein" Information Package.

- **Contextual Justification:** This data is critical to establishing the physical and geographical locus of
the data entry, invoking the foundational legal maxim *nemo dat quod non habet* (no one gives what they
do not have). If an instrument purportedly authorized by a Superior Court Chief Justice operating out of
the 361 University Avenue courthouse was actually inputted from a municipal police division's back-office
terminal (e.g., TPS 52nd Division or 14th Division), the ORI routing codes will incontrovertibly prove the
jurisdictional nullity. The RCMP cannot hide behind the "originator control" principle to avoid disclosing
the very records that prove the originating municipal agency committed a forgery. Once a municipal
agency enters data into the federal mainframe, that metadata becomes a federal record, subject to
federal transparency laws.

4. Inter-Agency Communication Logs: All internal records of communication (including but not limited to
emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP
CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.

- **Contextual Justification:** When a catastrophic software failure occurs during the ingestion of a judicial
document, it generates automated system alerts and IT troubleshooting tickets. This requisition
specifically targets communications regarding the authentication of the corrupted judicial initials ("CL
(M)"), the resolution of vector collapse errors, and any inquiries regarding jurisdictional discrepancies
between the physical court filings and the electronic mainframe entries during the September-October
2024 epoch. This includes any communications with specialized operational units or local registries
regarding the failure of the mandatory "Matching Protocol." A system error of this magnitude would not
exist in a vacuum; there is an administrative paper trail of IT professionals attempting to reconcile the
corrupted digital artifacts.

535 PDF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.

- **Contextual Justification:** This is particularly targeted at system interactions involving the GrapeCity Documents PDF suite (specifically version 6.0.2.0 and the documented DOC-6507 bug). Forensic analysis confirms this enterprise-level developer software was utilized with the specific *mens rea* to unlawfully flatten the document, forcefully delete the transparent electronic image signature of Chief Justice Geoffrey B. Morawetz, and algorithmically disfigure the underlying text to bypass standard criminal intake procedures. Specifically, the software's flattening engine violently clipped the mathematical bounding box of the "J" into an "L" and crushed the initials "G.B." into parentheses "()". Furthermore, records concerning the subsequent, deliberate superimposition of a civilian clerk's digital certificate (Court Officer Christyn Frugoni-Rojas) directly over the corrupted artifact to act as a visual smokescreen, and the appending of a decoy Justice of the Peace signature line (George Jiri), are requisitioned.

6. Offline Historical Search Results: The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.

- **Contextual Justification:** The municipal record currently presents a glaring chronological impossibility: an arrest executed on October 2, 2024, followed by the inexplicable expungement of the purported warrant from provincial systems via the Integrated Court Offences Network (ICON) on October 3, 2024. A lawful warrant does not evaporate the day after its execution; it is filed as a return to a justice. The RCMP's offline historical data stands as the singular remaining mechanism to pierce this localized spoliation trap. Furthermore, this data is necessary to expose the retaliatory "Digital Spoliation" orchestrated by the Justice Sector Security Office (JSSO), which weaponized cybersecurity infrastructure by utilizing a 403 Forbidden Error to block my IP address from the Ontario Courts Public Portal upon the initial discovery of this nullity.

7. System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

- **Contextual Justification:** This includes all operational directives establishing the responsibilities of the CPIC Coordinator to ensure that the electronic data entered perfectly mirrors the physical judicial order. There exists a mandatory "Air Gap" between the judiciary and the police; judges possess no direct terminal access to input data into CPIC. Therefore, the structural integrity of the system relies entirely on police compliance with this Matching Protocol. Manuals detailing the rigorous, distinct standards required

344 for the intake of Superior Court of Justice (SCJ) warrants versus provincial Ontario Court of Justice (OCJ)
536 Fake endorsements are required to prove exactly how these systemic checks and balances were
bypassed to manufacture a facsimile of authority.

Notice Regarding Statutory Exemptions and Public Interest Override (Section 19(2))

To the extent that the institution contemplates the application of discretionary exemptions under the ATIA—specifically those pertaining to the "personal information" of state actors, internal governmental deliberations, or law enforcement investigative privilege—such redactions are hereby preemptively challenged, legally vitiated, and fundamentally dismantled in limine.

As established exhaustively in my concurrent *Privacy Act* filings, the records sought relate directly to profound documentary metamorphosis, systemic spoliation, and an Irremediable Nullity orchestrated by state actors acting under the mere colour of authority. The legal maxim *fraus omnia corrumpit* (fraud vitiates everything) fundamentally dictates that a judicial process infected by deliberate digital manipulation is irreparably compromised across all subsequent administrative tiers. The invocation of privacy laws to shield the identities of those who authored a forgery is a perverse subversion of the legislation's intent.

When public officials utilize enterprise developer applications to digitally forge the authorizations of a Superior Court, they irrevocably forfeit the traditional immunities and privacy expectations afforded to them in the standard, lawful execution of their duties. As determined by the Supreme Court of Canada in *Dagg v. Canada (Minister of Finance)*, the fundamental objective of access legislation is the rigorous scrutiny of state action, effectively diminishing the privacy expectations of public officials engaged in the execution of official duties. The names, terminal IDs, and ORI routing codes of state actors operating a federal database are professional metrics, not intimate biographical details.

Pursuant to Section 19(2) of the ATIA, the paramount public interest in ensuring the constitutional legitimacy, democratic accountability, and algorithmic integrity of the national CPIC database decisively and unequivocally overrides any residual privacy expectations of the professional actors involved. The institution cannot rely upon the "mosaic effect"—the theory that disclosing seemingly innocuous administrative metadata could allow for the re-identification of state actors—to justify the withholding of data. In cases of alleged state malfeasance and the arbitrary deprivation of liberty, the public's right to reconstruct the "mosaic of forgery" is the paramount democratic interest.

If the Privacy Commissioner previously ruled in the prominent "Suicide Disclosure Case" that CPIC cannot be utilized for the unauthorized dissemination of sensitive mental health data due to the severe collateral damage it inflicts, it *a fortiori* cannot be utilized as a secure digital vault for the preservation of municipal-level documentary forgery. The public possesses an absolute, inalienable right to ascertain whether the coercive apparatus of the state is mobilized upon legitimate judicial authority or a "Frankenstein" algorithmic fabrication.

Justice system that operates on altered PDFs and falsified metadata is a system that has lost the consent of the governed.

In the spirit of our access partnership, I am fully prepared to assist the ATIP branch in clarifying any technical parameters of this request to ensure efficient, streamlined processing prior to the expiration of the statutory deadline.

I look forward to your formal acknowledgment of this ATIA request and the timely, unredacted provision of the responsive records.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

APPENDICES**Appendix #1: Access to Information Act Excerpts****Personal Information**

19 (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Part that contains personal information.

Where disclosure authorized

(2) The head of a government institution may disclose any record requested under this Part that contains personal information if

- (a) the individual to whom it relates consents to the disclosure;
- (b) the information is publicly available; or
- (c) the disclosure is in accordance with section 8 of the Privacy Act.

R.S., 1985, c. A-1, s. 19 2019, c. 18, s. 9 2019, c. 18, s. 41(E)

APPENDIX #2: PRIVACY ACT, SECTION 8**Disclosure of personal information**

- **8 (1)** Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

- **Where personal information may be disclosed**

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

- **(a)** for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;
- **(b)** for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;
- **(c)** for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;
- **(d)** to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

- (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;
- (f) for the purpose of administering or enforcing any law or carrying out a lawful investigation, under an agreement or arrangement between the Government of Canada or any of its institutions and any of the following entities or any of their institutions:
 - (i) the government of a foreign state,
 - (ii) an international organization of states or an international organization established by the governments of states,
 - (iii) the government of a province,
 - (iv) the council of the Westbank First Nation,
 - (v) the *council of a participating First Nation* as defined in [subsection 2\(1\)](#) of the [First Nations Jurisdiction over Education in British Columbia Act](#),
 - (vi) the council of a *participating First Nation* as defined in [section 2](#) of the [Anishinabek Nation Education Agreement Act](#),
 - (vii) a *First Nation Government* or the *Anishinabek Nation Government*, as defined in [section 2](#) of the [Anishinabek Nation Governance Agreement Act](#), or an Anishinaabe Institution, within the meaning of section 1.1 of the *Agreement*, as defined in [section 2](#) of that Act,
 - (vii.1) the *Whitecap Dakota Government*, as defined in [section 2](#) of the [Self-Government Treaty Recognizing the Whitecap Dakota Nation / Wapaha Ska Dakota Oyate Act](#);
- (g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;
- (h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;
- (i) to the Library and Archives of Canada for archival purposes;
- (j) to any person or body for research or statistical purposes if the head of the government institution
 - (i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and
 - (ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

- **(k)** to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;
- **(l)** to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and
- **(m)** for any purpose where, in the opinion of the head of the institution,
 - **(i)** the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or
 - **(ii)** disclosure would clearly benefit the individual to whom the information relates.
- **Personal information disclosed by Library and Archives of Canada**

(3) Subject to any other Act of Parliament, personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes.
- **Copies of requests under paragraph (2)(e) to be retained**

(4) The head of a government institution shall retain a copy of every request received by the government institution under paragraph (2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make those copies and records available to the Privacy Commissioner.
- **Notice of disclosure under paragraph (2)(m)**

(5) The head of a government institution shall notify the Privacy Commissioner in writing of any disclosure of personal information under paragraph (2)(m) prior to the disclosure where reasonably practicable or in any other case forthwith on the disclosure, and the Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to whom the information relates of the disclosure.
- **Definition of *Indian band***

(6) In paragraph (2)(k), ***Indian band*** means

 - **(a)** a band, as defined in the [Indian Act](#);
 - **(b)** the band, as defined in [subsection 2\(1\)](#) of the [Naskapi and the Cree-Naskapi Commission Act](#);
 - **(c)** the *shíshálh Nation*, as defined in subsection 2(1) of the *shíshálh Nation Self-Government Act*; or
 - **(d)** a first nation named in Schedule II to the [Yukon First Nations Self-Government Act](#).

541

(1) The expression **aboriginal government** in paragraph (2)(k) means

- (a) Nisga'a Government, as defined in the Nisga'a Final Agreement given effect by the *Nisga'a Final Agreement Act*;
- (b) the council of the Westbank First Nation;
- (c) the Tlicho Government, as defined in [section 2](#) of the [Tlicho Land Claims and Self-Government Act](#);
- (d) the Nunatsiavut Government, as defined in section 2 of the *Labrador Inuit Land Claims Agreement Act*;
- (e) the council of a participating First Nation as defined in [subsection 2\(1\)](#) of the [First Nations Jurisdiction over Education in British Columbia Act](#);
- (e.1) the Tla'amin Government, as defined in subsection 2(2) of the *Tla'amin Final Agreement Act*;
- (f) the Tsawwassen Government, as defined in subsection 2(2) of the *Tsawwassen First Nation Final Agreement Act*;
- (f.1) the Cree Nation Government, as defined in [subsection 2\(1\)](#) of the [Cree Nation of Eeyou Istchee Governance Agreement Act](#) or a Cree First Nation, as defined in subsection 2(2) of that Act;
- (g) a Maanulth Government, within the meaning of [subsection 2\(2\)](#) of the [Maanulth First Nations Final Agreement Act](#);
- (h) Sioux Valley Dakota Oyate Government, within the meaning of subsection 2(2) of the *Sioux Valley Dakota Nation Governance Act*;
- (h.1) the Whitecap Dakota Government, as defined in [section 2](#) of the [Self-Government Treaty Recognizing the Whitecap Dakota Nation / Wapaha Ska Dakota Oyate Act](#);
- (i) the council of a *participating First Nation* as defined in [section 2](#) of the [Anishinabek Nation Education Agreement Act](#); or
- (j) a *First Nation Government* or the *Anishinabek Nation Government*, as defined in [section 2](#) of the [Anishinabek Nation Governance Agreement Act](#), or an Anishinaabe Institution, within the meaning of section 1.1 of the *Agreement*, as defined in [section 2](#) of that Act.

• **Definition of council of the Westbank First Nation**

(8) The expression **council of the Westbank First Nation** in paragraphs (2)(f) and (7)(b) means the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the [Westbank First Nation Self-Government Act](#).

- R.S., 1985, c. P-21, s. 8
- R.S., 1985, c. 20 (2nd Supp.), s. 13, c. 1 (3rd Supp.), s. 12

- [2004, c. 11, s. 37](#), c. 17, s. 18
- [2005, c. 1, ss. 106, 109](#), c. 27, ss. 21, 25
- [2006, c. 10, s. 33](#)
- [2008, c. 32, s. 30](#)
- [2009, c. 18, s. 23](#)
- [2014, c. 1, s. 19](#), c. 11, s. 24
- [2017, c. 32, s. 18](#)
- [2018, c. 4, s. 132](#)
- [2022, c. 9, s. 4](#)
- 2022, c. 9, s. 45
- [2023, c. 22, s. 20](#)

APPENDIX #3: SYNTHESIS OF KEY LEGAL PRINCIPLES

Seamless Code

The ATIA and the Privacy Act are of equal legal status. One does not trump the other; they are a harmonious framework (established in *Dagg*). Parliament explicitly designed these statutes to operate in tandem as a "seamless code." The protection of personal information under the Privacy Act is intrinsically linked to the exceptions provided under the ATIA, meaning the RCMP cannot artificially separate the public interest analysis from the privacy analysis. When interpreting the right to access against the right to privacy, the institution must view the legislation as a unified mechanism designed to facilitate democratic oversight.

Positive Obligation to Consider

The head of a government institution cannot simply spot personal information, apply ATIA 19(1), and abruptly halt the analysis. They have an affirmative, positive statutory obligation to exercise their discretion and consider whether the public interest override under 19(2)(c) and 8(2)(m) applies. A "blanket refusal" to even consider the override constitutes a jurisdictional error. The institutional head must actively, explicitly, and contextually weigh the public's right to know against the individual's right to privacy on a rigorous, case-by-case basis. Failing to document this balancing act renders the denial of access fundamentally arbitrary.

High Threshold ("Clearly Outweighs")

The public interest in disclosure must not just be present; it must clearly outweigh the invasion of privacy. Mere curiosity, media sensationalism, or a general desire for transparency is rarely enough to breach an individual's privacy rights. However, the threshold is uniquely calibrated when state malfeasance is alleged. In the context

951 Hexadecimal Dumps" and hardware routing metadata—information that is purely administrative, professional, and devoid of intimate personal biographical content—the invasion of privacy is negligible. Conversely, the public interest in ensuring the cryptographic integrity of the national warrant database is absolute, thereby easily satisfying the "clearly outweighs" standard.

Deferential Review

Because PA s. 8(2)(m) explicitly delegates the balancing test to the "opinion of the head of the institution," courts apply a deferential reasonableness standard of review to that decision (established in the *Prime Minister* case). Courts will check if the head actually conducted the balancing exercise and if their conclusion was rational, rather than deciding the public interest question completely from scratch. Therefore, it is imperative that the RCMP conducts a logically sound and thoroughly documented balancing exercise in the first instance. If the institution decides that shielding the professional identities of officers who allegedly forged a Chief Justice's signature is more important than the integrity of the CPIC database, that decision will face a standard of "reasonableness" review that it cannot logically survive.

Tab B

Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

1 message

ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>

Thu, Apr 23, 2026 at 2:27 PM

To: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Dear Kevin McLean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- **Investigative Data Bank Audit Trails:** A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.
- **Hexadecimal Mainframe Dumps:** The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.
- **Hardware and Terminal Metadata:** The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.
- **Inter-Agency Communication Logs:** All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.
- **DF Flattening and Vector Analysis Reports:** All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.
- **Offline Historical Search Results:** The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.
- **System Governance Manuals:** Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

In order to process your request we require additional information:

- **Scope:** We have examined your request and fail to understand exactly what you are seeking in terms of records or documentation. As per section 6 of the Access to Information Act, "A request for access to a record under this Part shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort." **Please clarify what records you are seeking.**
- **Application fee:** The Access to Information Act prescribes an application fee of \$5.00. This is payable by cheque or money order to the Receiver General of Canada.

You may send this via regular mail or e-mail to the contact listed below.

Your file will remain open in our office for the next 10 days. If we have not received a response by **May 4, 2026**, this file will be closed.

546

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online: <https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
[73 Leikin Drive](#)
Ottawa, Ontario [K1A 0R2](#)

CONFIDENTIALITY NOTICE:

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'avisier immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

3 messages

ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>
To: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Thu, Apr 23, 2026 at 2:27 PM

Dear Kevin McLean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails:** A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.
- Hexadecimal Mainframe Dumps:** The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.
- Hardware and Terminal Metadata:** The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.
- Inter-Agency Communication Logs:** All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.
- DF Flattening and Vector Analysis Reports:** All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.
- Offline Historical Search Results:** The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.
- System Governance Manuals:** Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

In order to process your request we require additional information:

- Scope:** We have examined your request and fail to understand exactly what you are seeking in terms of records or documentation. As per section 6 of the Access to Information Act, "A request for access to a record under this Part shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort." **Please clarify what records you are seeking.**
- Application fee:** The Access to Information Act prescribes an application fee of \$5.00. This is payable by cheque or money order to the Receiver General of Canada.

You may send this via regular mail or e-mail to the contact listed below.

Your file will remain open in our office for the next 10 days. If we have not received a response by **May 4, 2026**, this file will be closed.

548

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online: <https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
[73 Leikin Drive](#)
Ottawa, Ontario [K1A 0R2](#)

CONFIDENTIALITY NOTICE:

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'avisier immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

Mr. Kevin McLean <mcleansettlement@gmail.com>

Thu, Apr 23, 2026 at 4:17 PM

To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>, melissa.simpson@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca

DELIVERY METHOD: Via Electronic Transmission (ATIP-AIPRP@rcmp-grc.gc.ca) & Registered Mail

TO:

Commissioner Michael Duheme, Head of the Institution

Mr. Stéphane Brisson, Chief Privacy Officer and Director General

Melissa Simpson, Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Phone: 647.370.9354

DATE: April 23, 2026**REFERENCE:** ATIA Request A-2026-00761 / F339 (Concomitant to Privacy Act Request P-2025-16999/F339)**SUBJECT: Rejection of Vague Request for Clarification, Breach of the Duty to Assist, Notice of Systemic Statutory Dereliction, and Formal Notice of Statutory Deadlines****1.0. SCHEDULE OF DOCUMENTS REVIEWED**

1.1. It is formally confirmed that the following *acta* and documentary instruments have been meticulously reviewed, catalogued, and are explicitly relied upon in the formulation of the legal, technical, and factual averments contained within this exhaustive correspondence:

Document Date	Document Description	Author / Sender	Recipient
February 27, 2026 (Delivered March 9, 2026)	formal request under the <i>Privacy Act</i> (File P-2025-16999)	Mr. Kevin A. McLean	ATIP Branch, RCMP
April 11, 2026	Canada Post Retail Receipt (Tracking No. 0105952620936334)	Canada Post	Mr. Kevin A. McLean
April 13-19, 2026	formal complaints instituted before the office of the privacy commissioner (the "OPCC") regarding unauthorized extensions and systemic delays	Mr. Kevin A. McLean	OPCC
April 14, 2026	Canada Post Delivery Confirmation (Delivered at 10:11 a.m.)	Canada Post	ATIP Branch, RCMP
April 15, 2026	formal access request under the <i>Access to Information Act</i>	Mr. Kevin A. McLean	ATIP Branch, RCMP
April 16, 2026	aggregated electronic correspondence evincing institutional delays	ATIP Branch, RCMP	Mr. Kevin A. McLean
April 23, 2026	electronic correspondence demanding clarification and threatening file closure	Melissa Simpson, RCMP	Mr. Kevin A. McLean

1.2. The aforementioned documentary matrix establishes an incontrovertible chronology of events, rendering any subsequent institutional attempts to alter timelines, feign incomprehension, or assert procedurally defective administrative delays inherently transparent and legally void *ab initio*.

550 PRELIMINARY OBSERVATIONS AND LEGISLATIVE FRAMEWORK

2.1. Receipt is hereby acknowledged of the electronic correspondence dated April 23, 2026, dispatched by the access to information and privacy branch (the "**ATIP Branch**") of the royal canadian mounted police (the "**RCMP**"). The aforementioned correspondence acknowledges the institutional reception of the underlying requisition pursuant to the *Access to Information Act* (the "**ATIA**"), albeit erroneously asserting the operative date of receipt as April 15, 2026. As shall be exhaustively proven herein, the objective, third-party delivery metrics confirm the physical reception occurred on April 14, 2026; ergo, the unyielding statutory clock commenced unequivocally on April 14, 2026. This administrative assertion stands in direct, unassailable contradiction to verifiable logistical realities.

2.2. Within the aforementioned communication, the bald, unparticularized assertion is advanced that the institution "fails to understand exactly what you are seeking." Subsequently, section 6 of the *ATIA* is invoked as purported statutory justification for this manufactured administrative incomprehension. Furthermore, an extra-statutory administrative threat is unilaterally issued, suggesting that the formal requisition shall be summarily "closed" if a supplementary response is not furnished within an arbitrarily designated ten-day period. Additionally, a superfluous administrative inquiry is raised regarding the remittance of the statutorily prescribed application fee, a matter already definitively resolved by the physical transmission of the documents.

2.3. This correspondence must be accepted as the formal, binding clarification, thereby curing any purported ambiguities, whether genuine or strategically manufactured by the ATIP Branch. A profound objection is formally registered *in limine* regarding the characterization of the highly specified requisition as incomprehensible. It is respectfully submitted that the *ATIA* functions as a quasi-constitutional framework designed to ensure the rigorous democratic accountability of state actors, a principle affirmed repeatedly by the Supreme Court of Canada.

2.4. Consequently, the procedurally invalid administrative maneuvers currently being employed by the institution to delay the lawful processing of this file are unequivocally rejected. Such actions are characterized as being inherently *ultra vires* the jurisdiction conferred by the governing legislation. The deployment of arbitrary deadlines to threaten file closure represents a pernicious subjugation of the applicant's fundamental, quasi-constitutional access rights to mere institutional expediency and bureaucratic attrition.

3.0. SATISFACTION OF SECTION 6 OF THE ATIA AND CONCEALMENT OF STATE MALFEASANCE

3.1. The blanket assertion articulated by the ATIP Branch—alleging a systemic inability to comprehend the scope of the requisition—is factually inaccurate, legally untenable, and fundamentally unacceptable in the context of federal law enforcement administration. Section 6 of the *ATIA* imposes a requirement that a requisition provide "sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort." This legislative threshold is designed to mitigate overly broad, ambiguous "fishing expedition" requests; it is decidedly not a mechanism to be weaponized by an institution to feign ignorance when confronted with highly specific, technically precise nomenclature.

3.2. The initial requisition does not rely upon vague generalities, abstract concepts, or broad sweeps of administrative trivia. Rather, it is drafted with surgical, forensic precision, targeting specific federal databases, highly distinct algorithmic file structures, and exact mathematical artifacts. To reiterate and further elucidate, the following specific items were explicitly requisitioned, the nature of which precludes any genuine administrative confusion among competent database architects:

- **Investigative Data Bank Audit Trails:** Specified explicitly for the personal information bank rcmp ppu 005 (the "**PPU 005**"), strictly limited to the narrow, hyper-focused temporal epoch encompassing September 22 to October 4, 2024. This parameter requires the querying of a designated, centralized database for a predetermined date range to expose the chronological sequence of systemic commands (specifically the ADD, MODIFY, CLEAR, and CANCEL inputs). The precision of this request eliminates the need for discretionary, manual searching; it constitutes a straightforward digital extraction of an immutable systemic ledger. Standard graphical user interface (the "**GUI**") searches executed by frontline personnel are fundamentally incapable of revealing this historical trajectory, necessitating access to the foundational PPU 005 audit matrices.
- **Hardware and Terminal Metadata:** Specifically targeting the originating agency identifier (the "**ORI**") mapping, media access control addresses (the "**MAC Addresses**"), and terminal internet

protocol addresses (the "IP Addresses") associated with a specific file entry. This represents standard, automatically generated network infrastructure data necessitated to establish the physical and geographical locus of data entry. The legal maxim *nemo dat quod non habet* is explicitly engaged herein; if an instrument purportedly authorized by a Superior Court was physically inputted from a municipal police division's back-office terminal, the ORI routing codes will incontrovertibly expose the jurisdictional nullity. The national CPIC database cannot be permitted to operate as a "digital laundry" for the sanitization of localized, municipal-level documentary fabrications.

- **Hexadecimal Mainframe Dumps:** The raw, uninterpreted binary and hexadecimal records extracted from the transaction logs for a specifically identified warrant. This request purposefully circumvents the visual homogenization inherent to the presentation layer of the GUI to secure the precise cryptographic memory offsets required to evidence document morphology. A GUI can be manipulated to display a facially valid entry, whereas the hexadecimal dump reveals the foundational mathematical reality of the database entry. This exposes any unauthorized vector alterations, specifically the utilization of enterprise-level applications (such as GrapeCity Documents version 6.0.2.0) to unlawfully flatten documentation and eradicate electronic image signatures.
- **Inter-Agency Communication Logs & System Error Reports:** Specific information technology troubleshooting tickets, automated system alerts, and communications shared between the RCMP systemic governance authority and external municipal records management branches. This specifically pertains to optical character recognition (the "OCR") interpretation failures, the documented DOC-6507 "whitespace bug," and the catastrophic algorithmic disfigurement of judicial text (e.g., the mutation of the bounding box resulting in the "C L (M)" artifact). Furthermore, inquiries regarding the bypass of the mandatory "Matching Protocol" and the "Judicial Firewall" are demanded. The nomenclature utilized here is absolute standard within the realm of enterprise-level software administration and national database governance.

3.3. It is forcefully submitted that an "experienced employee" tasked with the operation and oversight of the national mainframe architecture—particularly those integrated within the information technology, records management, and systemic governance divisions—possesses definitive, operational knowledge of an ORI code, a hexadecimal dump, and a PPU 005 audit trail. These metrics represent the foundational, inescapable operational architecture of the CPIC database. To assert otherwise is to profess an alarming institutional incompetence regarding the very infrastructure the RCMP is statutorily mandated to govern.

3.4. The Inference of Concealment and Judicial Implication: It is an inescapable extrapolation, derived from advanced syllogisms predicated upon the institutional conduct observed herein, that the present administrative obfuscation is a calculated endeavor. It has become manifestly obvious that the RCMP is attempting to conceal the identity of the purportedly authorizing judicial officer—specifically, whether Chief Justice Morawetz was the presiding Superior Court Justice involved in the issuance of the contested arrest warrant or the "Intake Court Endorsement" dated September 23, 2024. The manipulation of receipt timelines and the attempted arbitrary extension of deadlines to surpass his imminent departure date creates a powerful, incontrovertible circumstantial inference of bad faith. The institution is acutely aware that the exaction of the hexadecimal dumps and ORI metadata will definitively expose the fraudulent inputs injected into the national mainframe by the Toronto Police Service (the "TPS"). Consequently, the demand for "clarification" serves merely as a dilatory tactic—an attempt to orchestrate spoliation by delay and postpone the inevitable revelation of systemic documentary falsifications until the aforementioned judicial officer has officially vacated his office.

3.5. Nota Bene: *It is anticipated that the institution may advance the counter-argument that the advanced technical nomenclature utilized within the requisition renders the request opaque to standard, frontline administrative ATIP intake personnel, thereby justifying the demand for clarification. This anticipated defense is fundamentally flawed, procedurally defective, and legislatively repugnant. An administrative limitation in the technical literacy of an initial intake clerk cannot, ipso facto, nullify the overarching statutory obligations of the institution. Section 4(2.1) of the ATIA imposes a positive, statutory "duty to assist" upon the institution. The jurisprudence necessitates that the institution engage an "experienced employee," which, in this context, inherently mandates internal inter-departmental consultation with systems architects, cybersecurity analysts, or CPIC database administrators who possess the requisite technical acumen to retrieve the specified records. A boilerplate assertion of total incomprehension, issued without attempting rigorous internal consultation, represents a direct, actionable subversion of this statutory duty.*

552 institution may not utilize its own internal partitioning of technical knowledge as a bureaucratic shield against mandatory disclosure.

4.0. FULFILLMENT OF THE STATUTORY APPLICATION FEE AND INCONTROVERTIBLE CHAIN OF CUSTODY

4.1. In regards to the administrative inquiry concerning the statutorily prescribed application fee, attention must be directed to the primary page of the originating document, which explicitly and unambiguously declared: "*The prescribed statutory application fee of \$5.00 is enclosed with the physical transmission of this document.*" It is perplexing that an institution would formally acknowledge receipt of the correspondence while simultaneously questioning the whereabouts of the physical enclosure explicitly referenced within the primary paragraph of said correspondence.

4.2. The physical package containing the initial request, complete with the enclosed payment in the form of a certified financial instrument, was formally dispatched to the designated mailroom via a duly registered, highly tracked postal mechanism. Specifically, Canada Post Xpresspost was utilized, bearing the incontrovertible tracking number 0105952620936334, to ensure an unassailable, unbroken chain of custody. Furthermore, an objective delivery confirmation—generated by a neutral, state-sanctioned third-party logistics provider—establishes absolutely that the parcel was successfully received, scanned, and signed for by the institution on April 14, 2026, at precisely 10:11 a.m.

4.3. The statutory fee has therefore been duly remitted and placed into the constructive possession of the institution in absolute accordance with the legislative requirements. It is a well-established, foundational principle of administrative law that internal bureaucratic delays pertaining to mail sorting procedures between a central receiving facility and the specific, localized ATIP Branch do not negate an applicant's rigorous compliance with legislative prerequisites. Furthermore, internal mailroom inefficiencies cannot be weaponized by the state to establish valid grounds to arrest the processing of the file, nor can they be utilized to falsely alter the legally operative date of statutory receipt. The institution was in constructive and actual legal possession of the requisition and the associated fee on April 14, 2026. The statutory processing clock commenced upon that objective physical delivery, not upon the subsequent, delayed administrative processing by an ATIP intake clerk days later.

5.0. ESTABLISHMENT OF A SYSTEMIC PATTERN OF STATUTORY DERELICTION AND TEMPORAL OBFUSCATION

5.1. It must be observed with profound concern that the present administrative irregularities are decidedly not isolated, excusable anomalies; rather, they constitute a demonstrated, heavily documented, systemic pattern of statutory dereliction perpetrated by the ATIP Branch. This systemic issue has crystallized within the remarkably truncated temporal period of approximately one month, rendering the pattern of obstruction undeniable.

5.2. In the antecedent matter concerning the concomitant request instituted pursuant to the *Privacy Act* (specifically File P-2025-16999/F339), a time extension was purportedly exacted upon the bald, unparticularized assertion that processing would "unreasonably interfere with operations." This preceding extension was completely devoid of any requisite particulars, operational metrics, or factual grounding necessary to satisfy the strict evidentiary burden of interference mandated by the judiciary. However, it is highly instructive to note that in the previous *Privacy Act* request, an initial institutional response was provided within approximately four days of receipt.

5.3. By stark contrast, operating under the parallel *ATIA* regime for the present requisition, this file languished for nearly ten days before the institution generated a legally defective demand for clarification. This alarming disparity in institutional responsiveness underscores the fact that the RCMP possesses profound issues with the extraction of the specific database artifacts requisitioned herein, owing entirely to the fraudulent inputs injected by the TPS. The near ten-day delay is a palpable attempt to delay the inevitable.

5.4. It is a paramount maxim of equity that *justitia dilata, justitia denegata*—justice delayed is justice denied. This represents a remarkably serious concern that unequivocally engages the public interest. The public interest in securing the cryptographic integrity of the national law enforcement database must remain paramount in this situation. It is for this precise reason, owing to the systemic breakdown of ATIP compliance and the overarching institutional imperatives at stake, that the Commissioner of the RCMP and the Chief Privacy Officer are formally copied herein. They are placed on strict, constructive notice of the ongoing administrative obfuscation occurring within their respective purviews.

*Nota Bene: It is anticipated that the institution may advance the counter-argument that the ATIA and Privacy Act represent distinct legislative regimes, administered via disparate internal silos and processed by different personnel, thereby negating the assertion of a coordinated, systemic pattern of delay. This postulation is legally bankrupt and operationally fictitious. Both statutes operate collaboratively as a "seamless code" governing the dissemination of federal information, and both are administered under the ultimate fiduciary purview of the Head of the Institution and the Chief Privacy Officer. The replication of identical procedural infirmities across concurrent, interwoven files—specifically, the failure to particularize statutory grounds for extensions, the deployment of vague demands for clarification, and the chronic miscalculation of objective postal receipt dates—demonstrates a unified, systemic deficiency within the administrative protocols of the RCMP ATIP apparatus. The institution cannot rely upon its own internal fragmentation or administrative compartmentalization to excuse recurrent, parallel breaches of the *lex terrae*.*

6.0. JURISPRUDENTIAL LIMITS ON STATUTORY TIMEFRAMES AND SECTION 9 EXTENSIONS

6.1. The electronic correspondence dispatched on April 23, 2026, attempts to unilaterally impose a ten-day abeyance upon the file, accompanied by an explicit threat of closure should the applicant fail to comply with an extra-statutory demand. It must be forcefully reiterated that under the *ATIA*, an institution's informal, extra-statutory demand for "clarification" possesses absolutely no statutory mechanism to toll, pause, reset, or otherwise suspend the initial thirty-day statutory processing timeframe. The *ATIA* contains no legal provision empowering an institution to hold a file in administrative abeyance or to arbitrarily "close" it predicated upon an invented, self-imposed deadline. Consequently, such an administrative directive constitutes an absolute nullity, rather than a mere procedural irregularity, as it directly, flagrantly contravenes the strict temporal limitations mandated by the governing statute.

6.2. Furthermore, the correspondence fails entirely to invoke a valid extension of time pursuant to section 9(1) of the *ATIA*. Parliament has strictly, deliberately circumscribed the narrow grounds upon which an institution may extend the initial thirty-day timeframe, and the Federal Courts have rigorously, consistently enforced these parameters to prevent the erosion of democratic access rights through unchecked administrative overreach.

6.3. It is a fundamental, bedrock tenet of statutory interpretation that when legislation prescribes exhaustive, specific grounds for an action—as section 9 explicitly does for extending the thirty-day timeframe—any attempt to rely on extraneous, uncodified, or unspecified reasons is legally invalid and entirely void. By failing to formally cite section 9, or any of its constituent, conditional subsections (a), (b), or (c), the ATIP Branch has effectively provided a tacit legal admission that none of the statutorily permissible circumstances for delay exist.

6.4. The Corollary of Omission (Volume and Consultations): The correspondence under review is entirely devoid of any claim that "the request is for a large number of records or necessitates a search through a large number of records and meeting the original time limit would unreasonably interfere with the operations of the government institution," as is strictly required by section 9(1)(a). It must be deduced as an incontrovertible corollary of this omission that the request is, affirmatively, *not* for voluminous records. Similarly, there is absolutely no assertion that "consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit," as is exclusively mandated by section 9(1)(b). Therefore, it is formally established that no requisite external or inter-departmental consultations are necessary to fulfill this request.

6.5. The Corollary of Omission (Third-Party Notices): Finally, there is no mention whatsoever of any requirement to provide "notice of the request... pursuant to subsection 27(1)" concerning the protection of third-party commercial information, as stipulated by section 9(1)(c). **As no reliance on third-party notification has been formally made or evidenced by the institution, it is substantively confirmed that no third-party implications are at issue herein.** **6.6.** It is highly salient to emphasize that nearly ten full days elapsed from the objective receipt date of April 14, 2026, until the issuance of the defective April 23, 2026 correspondence. The institution possessed ample temporal latitude to determine if voluminous records, inter-departmental consultations, or third-party notices were engaged. The absolute failure to cite these provisions, following a comprehensive ten-day review period, mathematically and legally confirms their absolute inapplicability. The ATIP Branch cannot unilaterally invent administrative pretexts—such as a

manufactured need for "clarification" regarding standard database terminology—to circumvent the rigorous temporal strictures established by the Parliament of Canada.

6.2.1. Fatal Procedural Flaws in Mandatory Notification

6.7. As unequivocally established by the Federal Court of Appeal in *Statham v. CBC*, 2010 FCA 315 (the "*Statham Decision*"), and previously affirmed with equal force in *Hydro-Québec v. Canada (NEB)*, 1997 CanLII 16223 (FC) (the "*Hydro-Québec Decision*"), the failure to formally notify an applicant that an extension is specifically being claimed under section 9 operates as a fatal procedural breach. The jurisprudence dictates, without exception, that an institution must explicitly specify the exact quantum of the delay, the precise statutory justifications for its requirement, and must simultaneously, comprehensively inform the applicant of their corresponding right to register a formal complaint with the Information Commissioner regarding the specific extension. The correspondence received satisfies literally none of these mandatory, foundational notification requirements and, therefore, constitutes a nullity that cannot operate as a legally binding extension under any interpretation of the law.

6.2.2. Phased Releases and Rolling Disclosures

6.8. Furthermore, to the extent that the institution is encountering localized, artificial difficulties in retrieving a specific subset of the requisitioned documentation, the jurisprudence categorically prohibits the utilization of an "all-or-nothing" withholding strategy. While emanating from provincial jurisdictions, the jurisprudential edicts articulated by provincial privacy commissioners—such as *Public Service Commission (Re)*, 2011 CanLII 47545 (NL IPC)—serve as highly persuasive authorities by direct analogy within the federal sphere. These rulings mandate the implementation of "phased releases" or "rolling disclosures." Institutions are explicitly expected and legally required to release records in phases as they become available. Attempting to utilize a manufactured ambiguity regarding one highly technical aspect of a request (such as the DOC-6507 vector analysis) to justify the wholesale, immediate withholding of clearly defined, easily extractable records (such as the immutable PPU 005 audit trails) is a gross, actionable abuse of administrative process.

7.0. THE PARAMOUNTCY OF THE PUBLIC INTEREST AND QUASI-CONSTITUTIONAL IMPERATIVES

7.1. It is further submitted that the procedural maneuvering executed by the ATIP Branch fundamentally fails to account for the paramount public interest underpinning this requisition. The legislative schema governing access to information explicitly contemplates scenarios where the imperative of public disclosure supersedes institutional reticence or residual privacy considerations.

7.2. Specifically, section 19(2) of the *ATIA* delineates exceptions to the general prohibition against disclosing personal information. Crucially, section 19(2)(c) incorporates by reference the disclosure provisions of section 8 of the *Privacy Act*. Thus, the provisions of section 8 of the *Privacy Act* are inextricably intertwined with the present *ATIA* requisition.

7.3. Section 8(2)(m) of the *Privacy Act* vests the Head of the Institution with the explicit discretionary authority—and indeed, the positive statutory obligation—to disclose information where the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure. The institution is reminded that this involves a profound balancing exercise. As established in prevailing jurisprudence, mere curiosity or media sensationalism is insufficient to breach an individual's privacy rights. However, the threshold is uniquely and decisively calibrated when egregious state malfeasance is formally alleged.

7.4. In the context of "Hexadecimal Dumps" and hardware routing metadata—information that is purely administrative, professional, and entirely devoid of intimate personal biographical content—the invasion of privacy is negligible, if not entirely non-existent. Conversely, the public interest in ensuring the cryptographic integrity of the national warrant database is absolute, thereby easily and overwhelmingly satisfying the "clearly outweighs" standard mandated by section 8(2)(m)(i) of the *Privacy Act*.

7.5. The Commissioner of the RCMP is required to exercise this discretion *forthwith*. Improper time extensions—whether formally claimed or informally exacted through administrative threats—as they relate to an individualized *Privacy Act* or *Access to Information Act* request are of absolutely no consequence when weighed against the monumental public interest engaged herein. The exaction of metadata to expose the algorithmic disfigurement of Superior Court instruments by municipal state actors transcends standard administrative processing; it is an absolute imperative of democratic accountability. The institution may not utilize administrative friction to delay the exposure of systemic database fraud.

8.0. CONCLUSION AND THE MECHANICS OF DEEMED REFUSAL

555

The Federal Court of Appeal articulated with absolute, unyielding clarity in *Canada (Information Commissioner) v. Canada (National Defence)*, 2015 FCA 56 (the "*National Defence Decision*"), that while a procedurally valid, legally sound section 9 extension replaces the originating thirty-day deadline, an invalid, procedurally defective, or entirely absent extension ensures that the original statutory clock remains fully active, uninterrupted, and legally binding upon the institution.

8.2. Because the ATIP Branch has failed entirely to secure a procedurally flawless and factually justified extension under section 9, relying instead on non-statutory threats of file closure, the statutory clock has continued to run entirely uninterrupted from the objectively verified physical delivery date of April 14, 2026. This timeline explicitly, categorically rejects the institution's factually defective, administratively delayed assertion of an April 15, 2026 receipt.

8.3. The mandatory statutory deadline for the RCMP to provide a complete, substantive, and unredacted response to the requisition remains irrevocably fixed at **May 14, 2026**.

8.4. It is specifically, profoundly observed that this incontrovertible statutory deadline of May 14, 2026, directly and crucially precedes the imminent departure of Chief Justice Morawetz. The precise temporal alignment of this statutory deadline with the overarching legal matters, potential jurisdictional nullities, and the overarching *Jordan* ceilings renders the timely disclosure of these systemic records to be of paramount, critical, and time-sensitive public interest. It is hereby formally noticed that any failure to disclose the comprehensively requested records by this precise deadline shall be definitively, automatically treated as a deemed refusal (the "**Deemed Refusal**") pursuant to section 10(3) of the *ATIA*.

8.5. Upon the crystallization of such a Deemed Refusal, the institution is entirely stripped of its discretionary latitude, and an escalated, comprehensive complaint shall be immediately filed with the Office of the Information Commissioner. This complaint shall cite bad faith administrative stalling, constructive denial of fundamental access rights, a coordinated attempt to orchestrate spoliation by delay, and a blatant, systemic breach of the statutory duty to assist. Furthermore, the applicant fully reserves the right to seek an immediate writ of *mandamus* before the Federal Court of Canada to compel production and secure punitive cost awards against the institution for flagrant administrative delays.

8.6. It is unequivocally expected that this file shall proceed to the substantive processing phase immediately, entirely devoid of any further administrative obfuscation, and that the specified systemic records shall be extracted and released without further unlawful impedance.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

Enclosures (and previous enclosures by reference)

- Canada Post Retail Receipt (Tracking No. 0105952620936334)
- Canada Post Delivery Confirmation (April 14, 2026)

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

Tab D

[Quoted text hidden]

2 attachments



canada post - scan - rcmp atia .pdf
353K



Canada Post - Track a package by tracking number.pdf
245K

Mr. Kevin McLean <mcleansettlement@gmail.com>

Fri, Apr 24, 2026 at 2:03 PM

To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>, melissa.simpson@rcmp-grc.gc.ca, Michael.Duheme@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca

DELIVERY METHOD: Via Electronic Transmission (ATIP-AIPRP@rcmp-grc.gc.ca)

TO:

Commissioner Michael Duheme, Head of the Institution

Mr. Stéphane Brisson, Chief Privacy Officer and Director General

Melissa Simpson, Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Phone: 647.370.9354

DATE: April 24, 2026

REFERENCE:

ATIA Request A-2026-00761 / F339

OIC Complaint File Number: ACC-2026-04-00379

SUBJECT: FORMAL NOTICE OF INVESTIGATIVE PROCEEDINGS BEFORE THE OFFICE OF THE INFORMATION COMMISSIONER, REJECTION OF

1.0. SCHEDULE OF DOCUMENTS REFERENCED AND THE DOCTRINE OF EVIDENTIARY IMMUTABILITY

1.1. It is formally confirmed that the ensuing documentary instruments are enclosed herewith, establishing the incontrovertible evidentiary matrix upon which this administrative intervention and the subsequent, escalated investigative proceedings are irrevocably predicated. It is respectfully submitted that this schedule constitutes a finalized, unalterable administrative record. The formalization of this documentary history thereby engages the equitable doctrine of estoppel, definitively precluding the institution from subsequently engineering a revised factual timeline or advancing administrative rationales that might obscure the procedural deviations from the strict statutory mandates imposed by the Parliament of Canada:

Item No.	Document Description	Relevance to Current Proceedings and Legal Implications
1.	Formal Access Request	The originating statutory instrument, drafted with exacting forensic precision, explicitly delineating the specific technical parameters, algorithmic structures, and hexadecimal database artifacts requisitioned. This document unequivocally identified enterprise-level software anomalies (e.g., the GrapeCity Documents version 6.0.2.0 platform and the DOC-6507 bounding box mutation) and isolated the personal information bank RCMP PPU 005 (the "PPU 005") audit trails. Furthermore, it necessitated the extraction of originating agency identifiers (the "ORI"), media access control (the "MAC") addresses, and internet protocol (the "IP") assignments. By employing such precise, mathematically immutable nomenclature, this document establishes the highly articulated baseline of the request. Consequently, it pre-empts and renders legally void <i>ab initio</i> any subsequent institutional assertions of technical incomprehension, scope ambiguity, or a purported inability to identify the targeted records.
2.	Aggregated Electronic Correspondence	The institutional communications evincing the extra-statutory demand for clarification and the procedurally irregular attempt to exact a time extension. These records serve as the primary documentary evidence of the institution's <i>ultra vires</i> maneuvering. They explicitly demonstrate the application of

		extra-statutory deadlines and directives implying summary file closure, which appear to have been utilized by the access to information and privacy branch (the " ATIP Branch ") as mechanisms of bureaucratic attrition and administrative exhaustion. The documented delay of nearly ten days prior to issuing a demand for clarification regarding standard database terminology suggests a systematic temporal delay.
3.	Official Confirmation of OIC File Number	The formal acknowledgment generated by the Registry establishing the active, currently monitored investigative file (ACC-2026-04-00379) before the office of the information commissioner (the " OIC "). This instrument legally verifies that the overarching jurisdiction of the federal oversight body has been formally engaged. The crystallization of this docket number operates as an administrative <i>lis pendens</i> , placing the institution under immediate, rigorous investigatory scrutiny and precluding any further unilateral internal actions to terminate the processing of the requisitioned artifacts without independent federal review.
4.	Comprehensive Formal Complaint	The exhaustive, multi-page legal and factual brief submitted directly to the OIC. This document meticulously details the allegations of systemic dereliction, constructive refusal, and the administrative delays attributed to the ATIP Branch. It formally outlines the specific administrative deviations requiring regulatory review, explicitly highlighting the institutional omission of mandatory inter-departmental consultations with database architects of the Canadian police information centre (the " CPIC ") prior to asserting an inability to locate the requested digital ledgers. The complaint establishes a direct evidentiary nexus between the requested hexadecimal dumps and the exposure of irregularly generated judicial instruments.

2.0. FORMAL NOTIFICATION OF JURISDICTIONAL INTERVENTION, INVESTIGATORY OVERSIGHT, AND THE PUBLIC INTEREST OVERRIDE

2.1. Formal notification is hereby provided that a comprehensive, highly particularized complaint has been officially instituted before the OIC. This investigative intervention, officially registered and actively monitored under file number ACC-2026-04-00379, was strictly necessitated by the procedurally defective and inherently *ultra vires* maneuvers repeatedly executed by the ATIP Branch in direct relation to the subject requisition.

The statutory jurisdiction of the OIC has been formally invoked to rigorously scrutinize the institutional attempt to unilaterally toll a binding, quasi-constitutional statutory timeframe. The deployment of an extra-statutory demand for "clarification"—when explicitly confronted with mathematically precise, enterprise-level database terminology recognized by competent systems engineers—coupled with a directive suggesting summary file closure, represents a significant departure from established administrative protocols. Such dilatory actions risk imposing an unacceptable chilling effect upon the fundamental right of access, thereby subverting the democratic transparency explicitly mandated by the legislature.

2.3. The Quasi-Constitutional Imperative and the Public Interest Override: It is further submitted that this jurisdictional intervention compulsorily engages the overriding public interest provisions of the governing legislation. To the extent that artificial delays might be utilized to shield the identities of state actors involved in the algorithmic alteration of Superior Court instruments, such efforts appear to be without foundation in the prevailing jurisprudence. As established by the Supreme Court of Canada in *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403, the foundational objective of access legislation is the rigorous scrutiny of state action. The statutory protection of personal information was ostensibly not envisioned by Parliament to operate as a mechanism to obscure deviations from established judicial and administrative protocols.

2.4. Pursuant to section 19(2)(c) of the access to information act (the "**ATIA**"), read concomitantly with section 8(2)(m)(i) of the privacy act (the "**Privacy Act**"), the Head of the Institution possesses an affirmative, non-delegable statutory obligation to disclose information where the public interest clearly outweighs any residual invasion of privacy. The utilization of federal infrastructure as a digital repository to regularize jurisdictional irregularities—specifically, the manipulation of ORI routing codes to mask the municipal origins of a purportedly federal judicial authorization—engages the foundational legal maxim *fraus omnia corrumpit* (fraud vitiates everything). The public interest in securing the cryptographic integrity of the national law enforcement database is absolute, arguably overriding any expectation of privacy held by the personnel responsible for entering the metadata in question.

2.5. *Nota Bene*: It is anticipated that the institution may advance the counter-argument that the disclosure of PPU 005 audit trails and terminal MAC addresses inherently compromises the protected personal information and operational security of specific law enforcement personnel, thereby justifying a blanket refusal or an indefinite delay for consultation. This postulation fails *in limine*. The jurisprudence indicates that public officials executing their official duties possess a significantly diminished expectation of privacy. Furthermore, the requisitioned artifacts—hexadecimal memory offsets, IP assignments, and binary dumps—constitute highly technical, architectural metadata. They are professional, administrative records largely devoid of intimate biographical substance. The institutional reliance upon hypothetical privacy invasions to obscure the documented algorithmic alterations of a Chief Justice's signature constitutes a misapplication of the statutory balancing test. The institution is legally mandated to sever any genuinely protected information pursuant to section 25 of the *ATIA* and subsequently release the foundational metadata, rather than withholding the entirety of the record *in toto*.

561. It is further submitted that the OIC's investigatory mandate shall encompass an exhaustive examination of the systemic nature of these delays, specifically cross-referencing the identical procedural infirmities previously observed within the concomitant *Privacy Act* file (P-2025-16999 / F339). The institution is placed on strict, constructive notice that internal communications regarding the processing of these specific requests are now subject to external, independent review to ascertain the presence of systemic procedural deficiencies or coordinated administrative obstruction.

3.0. THE NULLITY OF THE UNPARTICULARIZED EXTENSION, STATUTORY CONSTRUCTION, AND THE ABSOLUTE CONTINUITY OF THE STATUTORY CLOCK

3.1. It is a foundational principle of administrative law that an extension of time exacted pursuant to the *ATIA* must explicitly, rigorously, and contemporaneously cite the exact statutory subsection relied upon by the institution. Parliament deliberately and narrowly circumscribed the grounds for an extension to prevent federal institutions from utilizing generalized operational constraints or manufactured ambiguities as administrative barriers against their timely disclosure obligations.

3.2. A forensic review of the institutional correspondence dispatched by Melissa Simpson on April 23, 2026, reveals a substantive absence of any formal invocation of section 9 of the *ATIA*. No legally operative statutory subsection was cited to justify the attempted delay. The correspondence is entirely devoid of claims that an extension is necessitated by a demonstrably large volume of records interfering with operations pursuant to section 9(1)(a); it is bereft of any assertion requiring mandatory inter-departmental consultations pursuant to section 9(1)(b); and it lacks any mandate for third-party notifications pursuant to section 9(1)(c). The sole reliance upon section 6 of the *ATIA*—a provision governing the initial formulation of a request, not the tolling of a statutory deadline—constitutes a profound misapplication of the legislative framework and an *ultra vires* assumption of jurisdiction.

3.3. The Doctrine of Exhaustive Enumeration: It is a paramount canon of statutory interpretation, encapsulated by the maxim *expressio unius est exclusio alterius* (the explicit mention of one thing is the exclusion of another), that where a legislature explicitly enumerates the conditions under which a specific action may be taken, it implicitly prohibits that action under any other unlisted circumstances. Because Parliament exclusively listed volume, consultations, and third-party notices as the sole permissible grounds for an extension under section 9, the introduction of an uncoded rationale—namely, a unilateral abeyance pending clarification of highly specific database terminology—is statutorily prohibited and inherently void.

3.4. Consequently, as authoritatively established and rigorously enforced by the Federal Court of Appeal in *Statham v. Canadian Broadcasting Corporation*, 2010 FCA 315, and subsequently reaffirmed in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56, the failure to particularize the exact statutory grounds for an extension renders the institutional action a procedural nullity *ab initio*. The jurisprudence dictates that an applicant must be provided with the precise statutory subsection utilized to justify the delay, alongside the specific quantum of time exacted, thereby enabling the meaningful exercise of the corresponding right to

register a formal complaint regarding that specific extension. An unparticularized, invalid extension is legally void, inherently defective, and entirely incapable of tolling the statutory clock.

3.5. *Nota Bene*: The institution may raise the highly technical counter-argument that a section 6 request for clarification implicitly tolls the statutory processing clock until the applicant satisfies the administrative inquiry, thereby shifting the burden of delay. This proposition appears entirely unsupported by the *lex terrae*. The *ATIA* operates upon a strict, uninterrupted temporal continuum from the moment of objective physical receipt. The statute contains no abeyance mechanism for clarification. If an institution requires clarification, it must seek it concurrently while the original thirty-day statutory clock continues to run. An institutional failure to comprehend standard CPIC nomenclature within that thirty-day window does not confer the unilateral authority to arrest the legislative timeline.

3.6. Mechanics of Deemed Refusal and the Loss of Institutional Discretion: Therefore, it is formally and unequivocally asserted that the primary thirty-day statutory processing timeframe remains fully active, uninterrupted, and unyielding. The computation commenced upon the objective, third-party verified physical delivery of the requisition on April 14, 2026. The mandatory deadline for the substantive provision of the comprehensively requisitioned digital artifacts—inclusive of the raw hexadecimal dumps, network session logs, and PPU 005 audit trails—remains irrevocably fixed at May 14, 2026.

3.7. It is to be understood that any failure by the institution to effectuate complete, unredacted disclosure by this precise chronological juncture shall be automatically and legally classified as a deemed refusal (the "**Deemed Refusal**") pursuant to section 10(3) of the *ATIA*. The temporal alignment of this May 14, 2026 deadline with the imminent departure of Chief Justice Morawetz is duly noted; the timely extraction of these records is paramount to preventing the loss of jurisdiction and the obscuration of the *status quo ante*. Upon the crystallization of this Deemed Refusal, the institution is entirely stripped of its discretionary processing latitude. The file transcends the standard administrative continuum and ripens immediately for further extraordinary judicial remedies, up to and including the immediate pursuit of a prerogative writ of *mandamus* before the Federal Court of Canada to compel physical production, potentially accompanied by petitions for punitive cost awards.

4.0. MANDATORY PROTOCOLS FOR FUTURE INSTITUTIONAL CORRESPONDENCE, TRANSPARENCY, AND THE PRESERVATION OF EVIDENCE

4.1. Formal Directive for a Litigation Hold and Anti-Spoliation Mandate: Given the formal engagement of the OIC and the highly sensitive nature of the database artifacts requisitioned, the institution is hereby placed under a strict, mandatory legal obligation to preserve all relevant evidence. A formal, comprehensive litigation hold must be immediately implemented across the entire CPIC governance architecture. The routine, algorithmic overwriting, purging, or localized deletion of the specified PPU 005 audit trails, internal IT troubleshooting tickets concerning the

RC-6507 bug, or any system error alerts generated during the September 22 to October 4, 2024 epoch is strictly forbidden.

4.2. This preservation mandate explicitly extends to all mirrored servers, backup tape archives, and individual terminal cache memory banks associated with the inputted ORI codes. Any destruction, alteration, or obfuscation of these digital ledgers following the receipt of this formal notice shall be construed *prima facie* as actionable spoliation of evidence, ostensibly effecting the frustration of a federal investigation and the concealment of a jurisdictional nullity.

4.3. Should the institution attempt to subsequently issue a procedurally compliant extension of time—assuming that any valid, objectively verifiable statutory grounds can be evidenced at this late administrative juncture—it is strictly demanded that such action be executed with the utmost transparency and adhere to the established jurisprudential standards of notification. Generalized assertions of administrative burden or vague allusions to operational interference shall be contested and forwarded immediately to the OIC as compounding evidence of continued administrative deficiencies.

4.4. Any future correspondence pertaining to the tolling of deadlines, the application of discretionary exemptions, or the substantive processing of this highly sensitive requisition must be transmitted directly within this specific, established electronic communication thread. The dissemination of fragmented, disparate communications is administratively unacceptable.

4.5. Furthermore, to ensure absolute administrative synchronization across all oversight bodies and to maintain the pristine integrity of the investigative record, it is a mandatory requirement that any such future correspondence explicitly cite both the RCMP institutional file number (A-2026-00761 / F339) and the corresponding OIC investigative file number (ACC-2026-04-00379) in the subject line. Failure to adhere to these foundational communicative protocols shall be construed as a deliberate attempt to fragment the administrative record, generate jurisdictional ambiguity, and evade the concurrent oversight of the Information Commissioner.

5.0. CONCLUSION AND CONSTITUTIONAL IMPERATIVE

5.1. It is a matter of profound concern that the documented alteration of foundational *Criminal Code* statutory instruments—arguably representing one of the most significant documented deviations from judicial protocol in the post-Patriation era—has not been met with immediate remedial action by the national law enforcement apparatus. Furthermore, the subsequent institutional submission of a time extension, entirely devoid of any explicit statutory citation or requisite analytical precision, constitutes a severe procedural irregularity that undermines foundational democratic principles. It is anticipated that the Head of the Institution will immediately rectify these administrative deficiencies.

Respectfully submitted,

/s/ Kevin A. McLean

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Apr 23, 2026 at 4:17 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DELIVERY METHOD: Via Electronic Transmission (ATIP-AIPRP@rcmp-grc.gc.ca) & Registered Mail

TO:

Commissioner Michael Duheme, Head of the Institution

Mr. Stéphane Brisson, Chief Privacy Officer and Director General

Melissa Simpson, Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Phone: 647.370.9354

DATE: April 23, 2026

REFERENCE: ATIA Request A-2026-00761 / F339 (Concomitant to Privacy Act Request P-2025-16999/F339)

SUBJECT: Rejection of Vague Request for Clarification, Breach of the Duty to Assist, Notice of Systemic Statutory Dereliction, and Formal Notice of Statutory Deadlines

1.0. SCHEDULE OF DOCUMENTS REVIEWED

1.1. It is formally confirmed that the following *acta* and documentary instruments have been meticulously reviewed, catalogued, and are explicitly relied upon in the formulation of the legal, technical, and factual

Documents contained within this exhaustive correspondence:

Document Date	Document Description	Author / Sender	Recipient
February 27, 2026 (Delivered March 9, 2026)	formal request under the <i>Privacy Act</i> (File P-2025-16999)	Mr. Kevin A. McLean	ATIP Branch, RCMP
April 11, 2026	Canada Post Retail Receipt (Tracking No. 0105952620936334)	Canada Post	Mr. Kevin A. McLean
April 13-19, 2026	formal complaints instituted before the office of the privacy commissioner (the "OPCC") regarding unauthorized extensions and systemic delays	Mr. Kevin A. McLean	OPCC
April 14, 2026	Canada Post Delivery Confirmation (Delivered at 10:11 a.m.)	Canada Post	ATIP Branch, RCMP
April 15, 2026	formal access request under the <i>Access to Information Act</i>	Mr. Kevin A. McLean	ATIP Branch, RCMP
April 16, 2026	aggregated electronic correspondence evincing institutional delays	ATIP Branch, RCMP	Mr. Kevin A. McLean
April 23, 2026	electronic correspondence demanding clarification and threatening file closure	Melissa Simpson, RCMP	Mr. Kevin A. McLean

1.2. The aforementioned documentary matrix establishes an incontrovertible chronology of events, rendering any subsequent institutional attempts to alter timelines, feign incomprehension, or assert procedurally defective administrative delays inherently transparent and legally void *ab initio*.

2.0. PRELIMINARY OBSERVATIONS AND LEGISLATIVE FRAMEWORK

2.1. Receipt is hereby acknowledged of the electronic correspondence dated April 23, 2026, dispatched by the access to information and privacy branch (the "ATIP Branch") of the royal canadian mounted police (the "RCMP"). The aforementioned correspondence acknowledges the institutional reception of the underlying requisition pursuant to the *Access to Information Act* (the "ATIA"), albeit erroneously asserting the operative date of receipt as April 15, 2026. As shall be exhaustively proven herein, the objective, third-party delivery metrics confirm the physical reception occurred on April 14, 2026; ergo, the unyielding statutory clock commenced unequivocally on April 14, 2026. This administrative assertion stands in direct, unassailable contradiction to verifiable logistical realities.

2.2. Within the aforementioned communication, the bald, unparticularized assertion is advanced that the institution "fails to understand exactly what you are seeking." Subsequently, section 6 of the *ATIA* is invoked as purported statutory justification for this manufactured administrative incomprehension. Furthermore, an extra-statutory administrative threat is unilaterally issued, suggesting that the formal requisition shall be summarily "closed" if a supplementary response is not furnished within an arbitrarily designated ten-day period. Additionally, a superfluous administrative inquiry is raised regarding the remittance of the statutorily prescribed application fee, a matter already definitively resolved by the physical transmission of the documents.

3. This correspondence must be accepted as the formal, binding clarification, thereby curing any purported ambiguities, whether genuine or strategically manufactured by the ATIP Branch. A profound objection is formally registered *in limine* regarding the characterization of the highly specified requisition as incomprehensible. It is respectfully submitted that the *ATIA* functions as a quasi-constitutional framework designed to ensure the rigorous democratic accountability of state actors, a principle affirmed repeatedly by the Supreme Court of Canada.

2.4. Consequently, the procedurally invalid administrative maneuvers currently being employed by the institution to delay the lawful processing of this file are unequivocally rejected. Such actions are characterized as being inherently *ultra vires* the jurisdiction conferred by the governing legislation. The deployment of arbitrary deadlines to threaten file closure represents a pernicious subjugation of the applicant's fundamental, quasi-constitutional access rights to mere institutional expediency and bureaucratic attrition.

3.0. SATISFACTION OF SECTION 6 OF THE ATIA AND CONCEALMENT OF STATE MALFEASANCE

3.1. The blanket assertion articulated by the ATIP Branch—alleging a systemic inability to comprehend the scope of the requisition—is factually inaccurate, legally untenable, and fundamentally unacceptable in the context of federal law enforcement administration. Section 6 of the *ATIA* imposes a requirement that a requisition provide "sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort." This legislative threshold is designed to mitigate overly broad, ambiguous "fishing expedition" requests; it is decidedly not a mechanism to be weaponized by an institution to feign ignorance when confronted with highly specific, technically precise nomenclature.

3.2. The initial requisition does not rely upon vague generalities, abstract concepts, or broad sweeps of administrative trivia. Rather, it is drafted with surgical, forensic precision, targeting specific federal databases, highly distinct algorithmic file structures, and exact mathematical artifacts. To reiterate and further elucidate, the following specific items were explicitly requisitioned, the nature of which precludes any genuine administrative confusion among competent database architects:

- **Investigative Data Bank Audit Trails:** Specified explicitly for the personal information bank RCMP PPU 005 (the "PPU 005"), strictly limited to the narrow, hyper-focused temporal epoch encompassing September 22 to October 4, 2024. This parameter requires the querying of a designated, centralized database for a predetermined date range to expose the chronological sequence of systemic commands (specifically the ADD, MODIFY, CLEAR, and CANCEL inputs). The precision of this request eliminates the need for discretionary, manual searching; it constitutes a straightforward digital extraction of an immutable systemic ledger. Standard graphical user interface (the "GUI") searches executed by frontline personnel are fundamentally incapable of revealing this historical trajectory, necessitating access to the foundational PPU 005 audit matrices.
- **Hardware and Terminal Metadata:** Specifically targeting the originating agency identifier (the "ORI") mapping, media access control addresses (the "MAC Addresses"), and terminal internet protocol addresses (the "IP Addresses") associated with a specific file entry. This represents standard, automatically generated network infrastructure data necessitated to establish the physical and geographical locus of data entry. The legal maxim *nemo dat quod non habet* is explicitly engaged herein; if an instrument purportedly authorized by a Superior Court was physically inputted from a municipal police division's back-office terminal, the ORI routing codes will incontrovertibly expose the jurisdictional nullity. The national CPIC database cannot be permitted to operate as a "digital laundry" for the sanitization of localized, municipal-level documentary fabrications.
- **Hexadecimal Mainframe Dumps:** The raw, uninterpreted binary and hexadecimal records extracted from the transaction logs for a specifically identified warrant. This request purposefully circumvents the visual homogenization inherent to the presentation layer of the GUI to secure the precise cryptographic memory offsets required to evidence document morphology. A GUI can be manipulated to display a facially valid entry, whereas the hexadecimal dump reveals the foundational mathematical reality of the database entry. This exposes any unauthorized vector alterations, specifically the utilization of enterprise-level applications (such as GrapeCity Documents version 6.0.2.0) to unlawfully flatten documentation and eradicate electronic image signatures.
- **Inter-Agency Communication Logs & System Error Reports:** Specific information technology troubleshooting tickets, automated system alerts, and communications shared between the RCMP

systemic governance authority and external municipal records management branches. This specifically pertains to optical character recognition (the "OCR") interpretation failures, the documented DOC-6507 "whitespace bug," and the catastrophic algorithmic disfigurement of judicial text (e.g., the mutation of the bounding box resulting in the "C L (M)" artifact). Furthermore, inquiries regarding the bypass of the mandatory "Matching Protocol" and the "Judicial Firewall" are demanded. The nomenclature utilized here is absolute standard within the realm of enterprise-level software administration and national database governance.

3.3. It is forcefully submitted that an "experienced employee" tasked with the operation and oversight of the national mainframe architecture—particularly those integrated within the information technology, records management, and systemic governance divisions—possesses definitive, operational knowledge of an ORI code, a hexadecimal dump, and a PPU 005 audit trail. These metrics represent the foundational, inescapable operational architecture of the CPIC database. To assert otherwise is to profess an alarming institutional incompetence regarding the very infrastructure the RCMP is statutorily mandated to govern.

3.4. The Inference of Concealment and Judicial Implication: It is an inescapable extrapolation, derived from advanced syllogisms predicated upon the institutional conduct observed herein, that the present administrative obfuscation is a calculated endeavor. It has become manifestly obvious that the RCMP is attempting to conceal the identity of the purportedly authorizing judicial officer—specifically, whether Chief Justice Morawetz was the presiding Superior Court Justice involved in the issuance of the contested arrest warrant or the "Intake Court Endorsement" dated September 23, 2024. The manipulation of receipt timelines and the attempted arbitrary extension of deadlines to surpass his imminent departure date creates a powerful, incontrovertible circumstantial inference of bad faith. The institution is acutely aware that the exaction of the hexadecimal dumps and ORI metadata will definitively expose the fraudulent inputs injected into the national mainframe by the Toronto Police Service (the "TPS"). Consequently, the demand for "clarification" serves merely as a dilatory tactic—an attempt to orchestrate spoliation by delay and postpone the inevitable revelation of systemic documentary falsifications until the aforementioned judicial officer has officially vacated his office.

3.5. Nota Bene: *It is anticipated that the institution may advance the counter-argument that the advanced technical nomenclature utilized within the requisition renders the request opaque to standard, frontline administrative ATIP intake personnel, thereby justifying the demand for clarification. This anticipated defense is fundamentally flawed, procedurally defective, and legislatively repugnant. An administrative limitation in the technical literacy of an initial intake clerk cannot, ipso facto, nullify the overarching statutory obligations of the institution. Section 4(2.1) of the ATIA imposes a positive, statutory "duty to assist" upon the institution. The jurisprudence necessitates that the institution engage an "experienced employee," which, in this context, inherently mandates internal inter-departmental consultation with systems architects, cybersecurity analysts, or CPIC database administrators who possess the requisite technical acumen to retrieve the specified records. A boilerplate assertion of total incomprehension, issued without attempting rigorous internal consultation, represents a direct, actionable subversion of this statutory duty. The institution may not utilize its own internal partitioning of technical knowledge as a bureaucratic shield against mandatory disclosure.*

4.0. FULFILLMENT OF THE STATUTORY APPLICATION FEE AND INCONTROVERTIBLE CHAIN OF CUSTODY

4.1. In regards to the administrative inquiry concerning the statutorily prescribed application fee, attention must be directed to the primary page of the originating document, which explicitly and unambiguously declared: *"The prescribed statutory application fee of \$5.00 is enclosed with the physical transmission of this document."* It is perplexing that an institution would formally acknowledge receipt of the correspondence while simultaneously questioning the whereabouts of the physical enclosure explicitly referenced within the primary paragraph of said correspondence.

4.2. The physical package containing the initial request, complete with the enclosed payment in the form of a certified financial instrument, was formally dispatched to the designated mailroom via a duly registered, highly tracked postal mechanism. Specifically, Canada Post Xpresspost was utilized, bearing the incontrovertible tracking number 0105952620936334, to ensure an unassailable, unbroken chain of custody. Furthermore, an objective delivery confirmation—generated by a neutral, state-sanctioned third-party logistics provider—establishes absolutely that the parcel was successfully received, scanned, and signed for by the institution on April 14, 2026, at precisely 10:11 a.m.

3. The statutory fee has therefore been duly remitted and placed into the constructive possession of the institution in absolute accordance with the legislative requirements. It is a well-established, foundational principle of administrative law that internal bureaucratic delays pertaining to mail sorting procedures between a central receiving facility and the specific, localized ATIP Branch do not negate an applicant's rigorous compliance with legislative prerequisites. Furthermore, internal mailroom inefficiencies cannot be weaponized by the state to establish valid grounds to arrest the processing of the file, nor can they be utilized to falsely alter the legally operative date of statutory receipt. The institution was in constructive and actual legal possession of the requisition and the associated fee on April 14, 2026. The statutory processing clock commenced upon that objective physical delivery, not upon the subsequent, delayed administrative processing by an ATIP intake clerk days later.

5.0. ESTABLISHMENT OF A SYSTEMIC PATTERN OF STATUTORY DERELICTION AND TEMPORAL OBFUSCATION

5.1. It must be observed with profound concern that the present administrative irregularities are decidedly not isolated, excusable anomalies; rather, they constitute a demonstrated, heavily documented, systemic pattern of statutory dereliction perpetrated by the ATIP Branch. This systemic issue has crystallized within the remarkably truncated temporal period of approximately one month, rendering the pattern of obstruction undeniable.

5.2. In the antecedent matter concerning the concomitant request instituted pursuant to the *Privacy Act* (specifically File P-2025-16999/F339), a time extension was purportedly exacted upon the bald, unparticularized assertion that processing would "unreasonably interfere with operations." This preceding extension was completely devoid of any requisite particulars, operational metrics, or factual grounding necessary to satisfy the strict evidentiary burden of interference mandated by the judiciary. However, it is highly instructive to note that in the previous *Privacy Act* request, an initial institutional response was provided within approximately four days of receipt.

5.3. By stark contrast, operating under the parallel *ATIA* regime for the present requisition, this file languished for nearly ten days before the institution generated a legally defective demand for clarification. This alarming disparity in institutional responsiveness underscores the fact that the RCMP possesses profound issues with the extraction of the specific database artifacts requisitioned herein, owing entirely to the fraudulent inputs injected by the TPS. The near ten-day delay is a palpable attempt to delay the inevitable.

5.4. It is a paramount maxim of equity that *justitia dilata, justitia denegata*—justice delayed is justice denied. This represents a remarkably serious concern that unequivocally engages the public interest. The public interest in securing the cryptographic integrity of the national law enforcement database must remain paramount in this situation. It is for this precise reason, owing to the systemic breakdown of ATIP compliance and the overarching institutional imperatives at stake, that the Commissioner of the RCMP and the Chief Privacy Officer are formally copied herein. They are placed on strict, constructive notice of the ongoing administrative obfuscation occurring within their respective purviews.

5.5. Nota Bene: *It is anticipated that the institution may advance the counter-argument that the ATIA and Privacy Act represent distinct legislative regimes, administered via disparate internal silos and processed by different personnel, thereby negating the assertion of a coordinated, systemic pattern of delay. This postulation is legally bankrupt and operationally fictitious. Both statutes operate collaboratively as a "seamless code" governing the dissemination of federal information, and both are administered under the ultimate fiduciary purview of the Head of the Institution and the Chief Privacy Officer. The replication of identical procedural infirmities across concurrent, interwoven files—specifically, the failure to particularize statutory grounds for extensions, the deployment of vague demands for clarification, and the chronic miscalculation of objective postal receipt dates—demonstrates a unified, systemic deficiency within the administrative protocols of the RCMP ATIP apparatus. The institution cannot rely upon its own internal fragmentation or administrative compartmentalization to excuse recurrent, parallel breaches of the lex terrae.*

6.0. JURISPRUDENTIAL LIMITS ON STATUTORY TIMEFRAMES AND SECTION 9 EXTENSIONS

6.1. The electronic correspondence dispatched on April 23, 2026, attempts to unilaterally impose a ten-day abeyance upon the file, accompanied by an explicit threat of closure should the applicant fail to comply with an extra-statutory demand. It must be forcefully reiterated that under the *ATIA*, an institution's

formal, extra-statutory demand for "clarification" possesses absolutely no statutory mechanism to toll, pause, reset, or otherwise suspend the initial thirty-day statutory processing timeframe. The *ATIA* contains no legal provision empowering an institution to hold a file in administrative abeyance or to arbitrarily "close" it predicated upon an invented, self-imposed deadline. Consequently, such an administrative directive constitutes an absolute nullity, rather than a mere procedural irregularity, as it directly, flagrantly contravenes the strict temporal limitations mandated by the governing statute.

6.2. Furthermore, the correspondence fails entirely to invoke a valid extension of time pursuant to section 9(1) of the *ATIA*. Parliament has strictly, deliberately circumscribed the narrow grounds upon which an institution may extend the initial thirty-day timeframe, and the Federal Courts have rigorously, consistently enforced these parameters to prevent the erosion of democratic access rights through unchecked administrative overreach.

6.3. It is a fundamental, bedrock tenet of statutory interpretation that when legislation prescribes exhaustive, specific grounds for an action—as section 9 explicitly does for extending the thirty-day timeframe—any attempt to rely on extraneous, uncodified, or unspecified reasons is legally invalid and entirely void. By failing to formally cite section 9, or any of its constituent, conditional subsections (a), (b), or (c), the ATIP Branch has effectively provided a tacit legal admission that none of the statutorily permissible circumstances for delay exist.

6.4. The Corollary of Omission (Volume and Consultations): The correspondence under review is entirely devoid of any claim that "the request is for a large number of records or necessitates a search through a large number of records and meeting the original time limit would unreasonably interfere with the operations of the government institution," as is strictly required by section 9(1)(a). It must be deduced as an incontrovertible corollary of this omission that the request is, affirmatively, *not* for voluminous records. Similarly, there is absolutely no assertion that "consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit," as is exclusively mandated by section 9(1)(b). Therefore, it is formally established that no requisite external or inter-departmental consultations are necessary to fulfill this request.

6.5. The Corollary of Omission (Third-Party Notices): Finally, there is no mention whatsoever of any requirement to provide "notice of the request... pursuant to subsection 27(1)" concerning the protection of third-party commercial information, as stipulated by section 9(1)(c). **As no reliance on third-party notification has been formally made or evidenced by the institution, it is substantively confirmed that no third-party implications are at issue herein.** **6.6.** It is highly salient to emphasize that nearly ten full days elapsed from the objective receipt date of April 14, 2026, until the issuance of the defective April 23, 2026 correspondence. The institution possessed ample temporal latitude to determine if voluminous records, inter-departmental consultations, or third-party notices were engaged. The absolute failure to cite these provisions, following a comprehensive ten-day review period, mathematically and legally confirms their absolute inapplicability. The ATIP Branch cannot unilaterally invent administrative pretexts—such as a manufactured need for "clarification" regarding standard database terminology—to circumvent the rigorous temporal strictures established by the Parliament of Canada.

6.2.1. Fatal Procedural Flaws in Mandatory Notification

6.7. As unequivocally established by the Federal Court of Appeal in *Statham v. CBC*, 2010 FCA 315 (the "*Statham Decision*"), and previously affirmed with equal force in *Hydro-Québec v. Canada (NEB)*, 1997 CanLII 16223 (FC) (the "*Hydro-Québec Decision*"), the failure to formally notify an applicant that an extension is specifically being claimed under section 9 operates as a fatal procedural breach. The jurisprudence dictates, without exception, that an institution must explicitly specify the exact quantum of the delay, the precise statutory justifications for its requirement, and must simultaneously, comprehensively inform the applicant of their corresponding right to register a formal complaint with the Information Commissioner regarding the specific extension. The correspondence received satisfies literally none of these mandatory, foundational notification requirements and, therefore, constitutes a nullity that cannot operate as a legally binding extension under any interpretation of the law.

6.2.2. Phased Releases and Rolling Disclosures

6.8. Furthermore, to the extent that the institution is encountering localized, artificial difficulties in retrieving a specific subset of the requisitioned documentation, the jurisprudence categorically prohibits the utilization of an "all-or-nothing" withholding strategy. While emanating from provincial jurisdictions, the jurisprudential edicts articulated by provincial privacy commissioners—such as *Public Service*

570 *Commission (Re)*, 2011 CanLII 47545 (NL IPC)—serve as highly persuasive authorities by direct analogy within the federal sphere. These rulings mandate the implementation of "phased releases" or "rolling disclosures." Institutions are explicitly expected and legally required to release records in phases as they become available. Attempting to utilize a manufactured ambiguity regarding one highly technical aspect of a request (such as the DOC-6507 vector analysis) to justify the wholesale, immediate withholding of clearly defined, easily extractable records (such as the immutable PPU 005 audit trails) is a gross, actionable abuse of administrative process.

7.0. THE PARAMOUNTCY OF THE PUBLIC INTEREST AND QUASI-CONSTITUTIONAL IMPERATIVES

7.1. It is further submitted that the procedural maneuvering executed by the ATIP Branch fundamentally fails to account for the paramount public interest underpinning this requisition. The legislative schema governing access to information explicitly contemplates scenarios where the imperative of public disclosure supersedes institutional reticence or residual privacy considerations.

7.2. Specifically, section 19(2) of the *ATIA* delineates exceptions to the general prohibition against disclosing personal information. Crucially, section 19(2)(c) incorporates by reference the disclosure provisions of section 8 of the *Privacy Act*. Thus, the provisions of section 8 of the *Privacy Act* are inextricably intertwined with the present *ATIA* requisition.

7.3. Section 8(2)(m) of the *Privacy Act* vests the Head of the Institution with the explicit discretionary authority—and indeed, the positive statutory obligation—to disclose information where the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure. The institution is reminded that this involves a profound balancing exercise. As established in prevailing jurisprudence, mere curiosity or media sensationalism is insufficient to breach an individual's privacy rights. However, the threshold is uniquely and decisively calibrated when egregious state malfeasance is formally alleged.

7.4. In the context of "Hexadecimal Dumps" and hardware routing metadata—information that is purely administrative, professional, and entirely devoid of intimate personal biographical content—the invasion of privacy is negligible, if not entirely non-existent. Conversely, the public interest in ensuring the cryptographic integrity of the national warrant database is absolute, thereby easily and overwhelmingly satisfying the "clearly outweighs" standard mandated by section 8(2)(m)(i) of the *Privacy Act*.

7.5. The Commissioner of the RCMP is required to exercise this discretion *forthwith*. Improper time extensions—whether formally claimed or informally exacted through administrative threats—as they relate to an individualized *Privacy Act* or *Access to Information Act* request are of absolutely no consequence when weighed against the monumental public interest engaged herein. The exaction of metadata to expose the algorithmic disfigurement of Superior Court instruments by municipal state actors transcends standard administrative processing; it is an absolute imperative of democratic accountability. The institution may not utilize administrative friction to delay the exposure of systemic database fraud.

8.0. CONCLUSION AND THE MECHANICS OF DEEMED REFUSAL

8.1. The Federal Court of Appeal articulated with absolute, unyielding clarity in *Canada (Information Commissioner) v. Canada (National Defence)*, 2015 FCA 56 (the "*National Defence Decision*"), that while a procedurally valid, legally sound section 9 extension replaces the originating thirty-day deadline, an invalid, procedurally defective, or entirely absent extension ensures that the original statutory clock remains fully active, uninterrupted, and legally binding upon the institution.

8.2. Because the ATIP Branch has failed entirely to secure a procedurally flawless and factually justified extension under section 9, relying instead on non-statutory threats of file closure, the statutory clock has continued to run entirely uninterrupted from the objectively verified physical delivery date of April 14, 2026. This timeline explicitly, categorically rejects the institution's factually defective, administratively delayed assertion of an April 15, 2026 receipt.

8.3. The mandatory statutory deadline for the RCMP to provide a complete, substantive, and unredacted response to the requisition remains irrevocably fixed at **May 14, 2026**.

8.4. It is specifically, profoundly observed that this incontrovertible statutory deadline of May 14, 2026, directly and crucially precedes the imminent departure of Chief Justice Morawetz. The precise temporal alignment of this statutory deadline with the overarching legal matters, potential jurisdictional nullities, and the overarching *Jordan* ceilings renders the timely disclosure of these systemic records to be of paramount, critical, and time-sensitive public interest. It is hereby formally noticed that any failure to

571 disclose the comprehensively requested records by this precise deadline shall be definitively, automatically treated as a deemed refusal (the "**Deemed Refusal**") pursuant to section 10(3) of the *ATIA*.

8.5. Upon the crystallization of such a Deemed Refusal, the institution is entirely stripped of its discretionary latitude, and an escalated, comprehensive complaint shall be immediately filed with the Office of the Information Commissioner. This complaint shall cite bad faith administrative stalling, constructive denial of fundamental access rights, a coordinated attempt to orchestrate spoliation by delay, and a blatant, systemic breach of the statutory duty to assist. Furthermore, the applicant fully reserves the right to seek an immediate writ of *mandamus* before the Federal Court of Canada to compel production and secure punitive cost awards against the institution for flagrant administrative delays.

8.6. It is unequivocally expected that this file shall proceed to the substantive processing phase immediately, entirely devoid of any further administrative obfuscation, and that the specified systemic records shall be extracted and released without further unlawful impedance.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

Enclosures (and previous enclosures by reference)

- Canada Post Retail Receipt (Tracking No. 0105952620936334)
- Canada Post Delivery Confirmation (April 14, 2026)

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Apr 23, 2026 at 2:27 PM ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca> wrote:

Dear Kevin McLean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.

- Hexadecimal Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.

- Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.

- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.

- DF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.

- Offline Historical Search Results: The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.

- System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

In order to process your request we require additional information:

- **Scope:** We have examined your request and fail to understand exactly what you are seeking in terms of records or documentation. As per section 6 of the Access to Information Act, "A request for access to a record under this Part shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort." **Please clarify what records you are seeking.**

- **Application fee:** The Access to Information Act prescribes an application fee of \$5.00. This is payable by cheque or money order to the Receiver General of Canada.

You may send this via regular mail or e-mail to the contact listed below.

Your file will remain open in our office for the next 10 days. If we have not received a response by **May 4, 2026**, this file will be closed.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online: <https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'avisier immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

3 attachments



**Complaint - Office of the Information Commissioner of Canada - RCMP - Improper Time Extension -
Complainant - KAM BA JD CIM - 24-April-2026.pdf**
257K



Summary - RCMP - ATIA - April 24 2026.pdf
125K



Emails with OIC - with file number.pdf
586K

Tab E

575

TO:

The Office of the Information Commissioner of Canada (the "OIC")
30 Victoria Street, 7th Floor

Gatineau, Quebec K1A 1H3

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Phone: 647.370.9354

DATE: April 24, 2026

REFERENCE:

Formal Complaint regarding ATIA Request A-2026-00761/F339

(Concomitant to Privacy Act Request P-2025-16999/F339 and other complaints therein made to the Office of the Privacy Commissioner of Canada)

SUBJECT: FORMAL COMPLAINT PURSUANT TO PART II OF THE ACCESS TO INFORMATION ACT: ALLEGATIONS OF CONSTRUCTIVE REFUSAL, SYSTEMIC DERELICTION, BAD FAITH OBFUSCATION, AND PROCEDURAL NULLITIES BY THE ROYAL CANADIAN MOUNTED POLICE

Table of Contents

TO:	1
FROM:	1
SUBJECT: FORMAL COMPLAINT PURSUANT TO PART II OF THE ACCESS TO INFORMATION ACT: ALLEGATIONS OF CONSTRUCTIVE REFUSAL, SYSTEMIC DERELICTION, BAD FAITH OBFUSCATION, AND PROCEDURAL NULLITIES BY THE ROYAL CANADIAN MOUNTED POLICE.....	1
1.0. SCHEDULE OF DOCUMENTS REVIEWED (CAN BE PROVIDED UPON REQUEST).....	2
2.0. PRELIMINARY OBSERVATIONS AND JURISDICTIONAL INVOCATION	3
3.0. INCONTROVERTIBLE CHAIN OF CUSTODY AND THE FICTION OF ADMINISTRATIVE DELAY	3
4.0. THE SUBSTANTIVE NULLITY OF THE SECTION 6 "CLARIFICATION" DEMAND AND CONCEALMENT OF STATE MALFEASANCE	3
5.0. UNLAWFUL TOLLING OF STATUTORY TIMEFRAMES AND FATAL PROCEDURAL OMISSIONS UNDER SECTION 9	4
6.0. SYSTEMIC PATTERN OF STATUTORY DERELICTION AND THE PARAMOUNTCY OF THE PUBLIC INTEREST	5
7.0. RELIEF SOUGHT AND CONCLUSION	5

1.0. SCHEDULE OF DOCUMENTS REVIEWED (CAN BE PROVIDED UPON REQUEST)

1.1. It is formally confirmed that the following acta and documentary instruments have been meticulously reviewed, catalogued, and are explicitly relied upon in the formulation of the legal, technical, and factual averments contained within this exhaustive formal complaint:

Document Date	Document Description	Author / Sender	Recipient
February 27, 2026 (Delivered March 9, 2026)	formal request under the <i>Privacy Act</i> (File P-2025-16999)	Mr. Kevin A. McLean	ATIP Branch, RCMP
April 11, 2026	Canada Post Retail Receipt (Tracking No. 0105952620936334)	Canada Post	Mr. Kevin A. McLean
April 13-19, 2026	formal complaints instituted before the office of the privacy commissioner (the "OPCC") regarding unauthorized extensions and systemic delays	Mr. Kevin A. McLean	OPCC
April 14, 2026	Canada Post Delivery Confirmation (Delivered at 10:11 a.m.)	Canada Post	ATIP Branch, RCMP
April 15, 2026	formal access request under the <i>Access to Information Act</i>	Mr. Kevin A. McLean	ATIP Branch, RCMP
April 16, 2026	aggregated electronic correspondence evincing institutional delays	ATIP Branch, RCMP	Mr. Kevin A. McLean
April 23, 2026 (2:27 PM)	electronic correspondence demanding clarification and threatening file closure	Melissa Simpson, RCMP	Mr. Kevin A. McLean
April 23, 2026 (4:17 PM)	comprehensive correspondence rejecting the vague request for clarification and providing formal notice of statutory deadlines	Mr. Kevin A. McLean	ATIP Branch, RCMP

1.2. The aforementioned documentary matrix establishes an incontrovertible chronology of events, thereby rendering any subsequent institutional attempts to alter timelines, feign technical incomprehension, or assert procedurally defective administrative delays inherently transparent, ultra vires, and legally void *ab initio*.

2. **577** If a formal complaint is instituted pursuant to the investigative mandate conferred by section 30 of the access to information act (the "**ATIA**"), read concomitantly with the systemic oversight provisions of the privacy act (the "**Privacy Act**") and the mandatory interpretive strictures imposed by the interpretation act (the "**Interpretation Act**"). It is respectfully submitted that the access to information and privacy branch (the "**ATIP Branch**") of the Royal Canadian Mounted Police (the "**RCMP**") has engaged in a coordinated, systemic pattern of statutory dereliction.

2.2. Specifically, the RCMP has unilaterally attempted to suspend binding statutory timeframes through the issuance of an extra-statutory demand for clarification, coupled with an unlawful threat to summarily terminate the processing of the requisition. Such institutional conduct is not merely a procedural irregularity; rather, it constitutes an absolute statutory nullity that strikes at the foundational democratic accountability mechanisms envisioned by the Parliament of Canada.

3.0. INCONTROVERTIBLE CHAIN OF CUSTODY AND THE FICTION OF ADMINISTRATIVE DELAY

3.1. In the electronic correspondence dispatched on April 23, 2026, the RCMP erroneously posited that the subject requisition was received by the institution on April 15, 2026. This administrative assertion is categorically rejected, as it stands in direct, unassailable contradiction to objective, verifiable logistical realities.

3.2. The physical package encompassing the formal requisition, inclusive of the statutorily prescribed application fee in the form of a certified financial instrument, was transmitted via Canada Post Xpresspost. The objective delivery confirmation, generated by a neutral, state-sanctioned logistics provider, unequivocally establishes that the parcel was successfully received, scanned, and signed for by the institutional mailroom on April 14, 2026, at precisely 10:11 a.m.

3.3. It is a foundational tenet of administrative law that an institution assumes constructive and legal possession of a document at the exact moment it is delivered to its designated receiving facility. Internal bureaucratic inefficiencies, or localized delays in routing documentation from a centralized mailroom to the specific ATIP Branch intake personnel, cannot be weaponized by the state to unlawfully abridge an applicant's statutory timelines or retrospectively alter the legally operative date of receipt.

3.4. *Nota Bene*: It is anticipated that the institution may advance the counter-argument that statutory timelines do not commence until the requisition is physically processed and inputted into the internal case management software by an ATIP intake analyst. This postulation is legally bankrupt. To accept such a premise would be to subordinate the strict temporal mandates of the *ATIA* to the arbitrary administrative lethargy of the institution, thereby frustrating the legislative intent. The statutory clock commenced incontrovertibly on April 14, 2026; any institutional computation utilizing April 15, 2026, is a mathematical and procedural nullity.

4.0. THE SUBSTANTIVE NULLITY OF THE SECTION 6 "CLARIFICATION" DEMAND AND CONCEALMENT OF STATE MALFEASANCE

4.1. The blanket assertion articulated by the ATIP Branch on April 23, 2026, alleging a comprehensive inability to comprehend the scope of the requisition, is factually inaccurate, legally untenable, and fundamentally repugnant to the expected competencies of a federal law enforcement administration. The institution invoked section 6 of the *ATIA*, which requires a requisition to provide "sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort."

4.2. It is forcefully submitted that the subject requisition was drafted with unparalleled forensic precision, purposefully eschewing ambiguous generalities in favor of exact mathematical artifacts, specific algorithmic file structures, and identified federal databases. The requisition specifically targeted:

383 Investigative Data Bank Audit Trails: Explicitly isolated to the personal information bank RCMP PPU 005 (the
578 PPU 005") for the highly restricted temporal epoch of September 22 to October 4, 2024.

Hardware and Terminal Metadata: Precisely demanding the originating agency identifier (the "ORI") mapping, media access control addresses (the "MAC Addresses"), and terminal internet protocol addresses (the "IP Addresses").

- Hexadecimal Mainframe Dumps: The raw, uninterpreted binary and hexadecimal records extracted from the transaction logs specifically circumventing graphical user interface homogenization.

4.3. The assertion that an "experienced employee"—specifically, one tasked with the operation, cybersecurity, and systemic governance of the national mainframe architecture—fails to understand standard enterprise-level IT nomenclature (such as MAC Addresses, ORI codes, or Hexadecimal Dumps) strains credulity beyond the breaking point. The deployment of section 6 in this context is a manufactured administrative fiction designed solely to stall processing.

4.4. *Nota Bene*: The institution might hypothetically argue that frontline administrative intake personnel lack the highly specialized technical literacy required to interpret hexadecimal data requests, thereby validating the demand for external clarification. This argument fails *in limine*. Section 4(2.1) of the *ATIA* imposes a positive, overarching statutory duty to assist the requester. This statutory imperative inherently mandates robust inter-departmental consultation. The ATIP Branch is legally obligated to consult its internal database architects and CPIC administrators. A boilerplate declaration of total incomprehension, issued without demonstrating rigorous internal consultation, constitutes an actionable subversion of the duty to assist. The institution may not utilize its internal partitioning of technical acumen as a bureaucratic shield against mandatory public disclosure.

4.5. The Interpretative Mandate and Remedial Imperative: It is further submitted that the institutional weaponization of section 6 of the *ATIA* directly contravenes the paramount interpretative mandate codified within section 12 of the *Interpretation Act*. Section 12 explicitly directs that every federal enactment "is deemed remedial, and shall be given such fair, large and liberal construction and interpretation as best ensures the attainment of its objects." The fundamental object of the *ATIA* is the facilitation of public access to state-controlled records to guarantee democratic accountability. Consequently, the RCMP's utilization of section 6—a provision ostensibly designed to assist institutions in locating records—as an impenetrable administrative shield to obstruct, delay, and obfuscate an exquisitely detailed requisition constitutes a fundamentally impermissible statutory interpretation. It purposefully subverts the remedial legislative intent mandated by the *Interpretation Act* and renders the statutory right of access illusory.

4.6. The Inference of Concealment: It is advanced through logical syllogism and the extrapolation of circumstantial evidence that this procedural obfuscation is a calculated endeavor to orchestrate spoliation by delay. The exaction of the aforementioned hexadecimal dumps and ORI metadata will definitively expose the foundational mathematical reality of fraudulent inputs injected into the national mainframe by municipal state actors. The delay tactics are transparently designed to postpone the inevitable revelation of systemic documentary falsifications until a specific judicial officer (Chief Justice Morawetz) has officially vacated his office.

5.0. UNLAWFUL TOLLING OF STATUTORY TIMEFRAMES AND FATAL PROCEDURAL OMISSIONS UNDER SECTION 9

5.1. The correspondence dispatched by the RCMP unilaterally dictated that the file would be "closed" if a supplementary response was not furnished within an arbitrarily designated ten-day period. It must be unequivocally stated that an extra-statutory demand for "clarification" possesses absolutely no statutory mechanism to toll, pause, reset, or otherwise suspend the primary thirty-day statutory processing timeframe codified within the *ATIA*.

5.2. An administrative directive attempting to hold a formal statutory requisition in abeyance, predicated upon an invented, self-imposed deadline, is not a mere procedural irregularity; it is an absolute jurisdictional nullity. Parliament deliberately circumscribed the narrow grounds upon which an institution may extend the initial thirty-day timeframe via section 9 of the *ATIA*.

5.3. By failing to formally invoke section 9, or any of its constituent conditional subsections—specifically, the necessity of processing voluminous records pursuant to section 9(1)(a), the requirement for inter-departmental consultations pursuant to section 9(1)(b), or the mandate for third-party notifications pursuant to section 9(1)(c)—the ATIP Branch has effectively provided a tacit legal admission that none of the statutorily permissible circumstances for delay are present.

384As authoritatively established by the Federal Court of Appeal in *Statham v. Canadian Broadcasting Corporation*, 2015 FCA 315 (the "*Statham Decision*"), and reinforced in *Hydro-Québec v. Canada (National Energy Board)*, 1997 CanLII 16223 (FC) (the "*Hydro-Québec Decision*"), the failure to formally, explicitly, and contemporaneously notify an applicant of the precise statutory justifications for an extension operates as a fatal procedural breach. The April 23, 2026 correspondence satisfies none of these mandatory notification requirements.

5.5. Consequently, as articulated with absolute clarity in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56 (the "*National Defence Decision*"), an invalid, procedurally defective, or entirely absent extension ensures that the original statutory clock remains fully active and uninterrupted.

5.6. *Nota Bene*: The RCMP might assert that the ten-day "hold" protocol represents a long-standing internal administrative policy utilized across federal departments to manage ambiguous requests. This position offends the foundational doctrine of paramountcy. Internal administrative policies, operational manuals, or customary bureaucratic practices cannot supersede, amend, or dilute explicit, mandatory statutory provisions enacted by the legislature. A practice does not acquire legal validity simply through chronic repetition. The statutory deadline remains irrevocably fixed at May 14, 2026. Any failure to disclose the comprehensively requested records by this precise deadline shall automatically crystallize into a deemed refusal pursuant to section 10(3) of the *ATIA*.

6.0. SYSTEMIC PATTERN OF STATUTORY DERELICTION AND THE PARAMOUNTCY OF THE PUBLIC INTEREST

6.1. It is observed with profound concern that the present procedural malfeasance is not an isolated anomaly but constitutes a demonstrated, heavily documented, systemic pattern of statutory dereliction perpetrated by the RCMP ATIP apparatus. This pattern is incontrovertibly evidenced by the replication of identical procedural infirmities across concurrent, interwoven files, specifically the antecedent matter concerning the concomitant request instituted pursuant to the *Privacy Act* (File P-2025-16999/F339).

6.2. *Nota Bene*: The institution may advance the argument that the *ATIA* and the *Privacy Act* represent distinct, mutually exclusive legislative regimes, administered via disparate internal silos, thereby negating the assertion of a coordinated systemic pattern of delay. This assertion is legally fictitious. Both statutes operate collaboratively as a seamless code governing the dissemination of federal information, and both are administered under the ultimate fiduciary purview of the Head of the Institution and the Chief Privacy Officer. The institutional reliance upon its own internal fragmentation to excuse recurrent, parallel breaches of the *lex terrae* is unconscionable.

6.3. It is a paramount maxim of equity that *justitia dilata, justitia denegata*—justice delayed is justice denied. The public interest in securing the cryptographic integrity of the national law enforcement database is absolute and must supersede institutional reticence.

6.4. Furthermore, the jurisprudence categorical prohibits the utilization of an "all-or-nothing" withholding strategy. As elucidated in *Public Service Commission (Re)*, 2011 CanLII 47545 (NL IPC) (the "*Public Service Commission Decision*"), institutions are legally mandated to implement phased releases or rolling disclosures. Attempting to utilize a manufactured ambiguity regarding one technical aspect (e.g., optical character recognition failures) to justify the wholesale withholding of easily extractable records (e.g., PPU 005 audit trails) constitutes an actionable abuse of administrative process.

7.0. RELIEF SOUGHT AND CONCLUSION

7.1. In light of the egregious, documented circumventions of the governing statutory frameworks, it is respectfully requested that the OIC and the OPCC immediately initiate a comprehensive, systemic investigation into the conduct of the RCMP ATIP Branch pertaining to files A-2026-00761/F339 and P-2025-16999/F339.

7.2. It is further requested that the OIC formally declare the RCMP's "clarification" demand of April 23, 2026, a statutory nullity *ab initio*, confirming that the initial thirty-day processing timeframe remains untolled, uninterrupted, and expires on May 14, 2026.

7.3. The applicant fully reserves the right, upon the imminent crystallization of a deemed refusal, to seek an immediate writ of *mandamus* before the Federal Court of Canada to compel production and to aggressively pursue punitive cost awards against the institution for flagrant, systemic administrative delays.

580

PENDIX A: CPIC RECORDS ASSOCIATED WITH FILE P-2025-16999 / F339 AND ANTICIPATED STATUTORY PRODUCTION FORMATS

8.1. To optimally facilitate the investigative purview of the OIC and the OPCC, and to preemptively forestall any subsequent, disingenuous institutional assertions of technical incomprehension regarding the specific database artifacts requisitioned, the following schedule is submitted. This matrix delineates the exact, immutable morphology of the seven requested categories of CPIC records associated with file P-2025-16999 / F339, strictly mandated pursuant to the strictures of the *ATIA*.

8.2. It is forcefully submitted that any substantive deviation from these rigorous, native data structures—specifically the unauthorized substitution of these exact digital artifacts with homogenized, graphical presentation summaries or heavily redacted portable document format iterations—shall be construed *prima facie* as a deliberate, sanctionable alteration of electronic records. Such actions will automatically engage further, severe investigative scrutiny regarding institutional spoliation of evidence and the destruction of digital provenance.

Item No.	Requisition Category	Contextual Justification and Legal Imperatives	Mandatory Format of Production (Native Architecture)	Exemplar Disclosure Metric (Mock Architecture) – SAMPLE
1.	Investigative Data Bank Audit Trails A full, unredacted disclosure of all audit trails for personal information bank RCMP PPU 005 (the "PPU 005") encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.	It is respectfully submitted that standard CPIC "Persons" file queries, routinely utilized by frontline patrol personnel, are fundamentally insufficient for the present inquiry. The graphical interface accessible to a patrol officer is subjected to algorithmic filtering and reflects exclusively the contemporaneous, operational status of a file. Only the immutable systemic ledgers housed deep within PPU 005—capturing the precise chronological sequence of ADD, MODIFY, CLEAR, and CANCEL commands—can definitively expose	Native tabular database extractions (e.g., CSV, SQL output) derived directly from the mainframe transaction ledger, strictly preserved without redaction of operational syntax or timestamp modification.	[TIMESTAMP] 2024-09-23T14:22:01Z [ACTION] ADD [USER_ID] TPS_8392 [CLEARANCE] L3 [TERMINAL] D-51 [STATUS] SUCCESS

386 581		the temporal trajectory of state-actor malfeasance. The architectural reality of the CPIC database ensures that while a fraudulently altered warrant may be ostensibly excised from the active operational interface to conceal the evidence of an unlawful arrest, the underlying digital artifact and the forensic footprint of the user who executed the deletion are decidedly not eradicated from the federal infrastructural matrix.	467	
2.	Hexadecimal Mainframe Dumps The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.	This mathematical data is strictly required to bypass the visual homogenization inherent to the standard graphical user interface (the "GUI"). The GUI functions merely as a presentation layer; it is highly susceptible to manipulation to display a facially valid warrant even when the underlying data structure is fatally corrupted. Only the uninterpreted binary and hexadecimal records—complete	Raw, continuous hexadecimal and binary outputs (e.g., .HEX files or raw binary dumps), purposely bypassing the visual homogenization inherent to the graphical user interface which routinely masks underlying forgery.	00000000 25 50 44 46 2d 31 2e 34 %PDF-1.4 00000010 2e 2e 2e 5b 47 72 61 70 ...[GrapeCity Documents v6.0.2.0]

387 582		with exact cryptographic memory offsets and ASCII/EBCDIC decoded text translations—can provide the absolute mathematical certitude required to prove vector morphology collapse. These immutable binary ledgers circumvent human interpretation entirely. A raw hexadecimal dump exposes the binary reality of the database entry, demonstrating precisely when the foundational metadata was algorithmically disfigured without lawful judicial authorization, and confirming whether the payload matches the physically forged documentation.	468	
3.	Hardware and Terminal Metadata The internal originating agency identifier (the "ORI") mapping, corresponding media access control (the "MAC") addresses, and associated hardware terminal	This data is critical to irrevocably establishing the physical and geographical locus of the data entry, directly invoking the foundational legal maxim <i>nemo dat quod non habet</i> (no one gives what they do not have). If an instrument purportedly authorized by a	Extracted network session logs explicitly delineating ORI routing codes, MAC addresses, and IP assignments associated with the session token.	[SESSION_ID] 99A4B-772 [ORI] ON59321 [MAC] 00:1A:2B:3C:4D:5E [IP_ASSIGNMENT] 192.168.10.45 [AGENCY] Toronto Police Service

388 583	internet protocol (the "IP") addresses utilized for the specific data-entry sessions that generated the "Frankenstein" information package.	Superior Court Chief Justice operating from the 361 University Avenue courthouse was, in fact, inputted from a municipal police division's back-office terminal (e.g., TPS 52nd Division or 14th Division), the ORI routing codes will incontrovertibly prove the jurisdictional nullity. The institution is precluded from utilizing the "originator control" principle as a shield to avoid disclosing the very records that evidence the commission of a forgery by an originating municipal agency. Once a municipal agency injects data into the federal mainframe, that metadata is instantaneously converted into a federal record, thereby becoming fully subject to federal transparency legislation.	469	
4.	Inter-Agency Communication Logs All internal records of communication	When a catastrophic software failure occurs during the systemic ingestion of a judicial document, automated system	Internal IT troubleshooting ticket exports (e.g., native ServiceNow, Jira data outputs) and raw systemic	[ALERT_ID] 44902 [ERROR_CODE] DOC-6507 BOUNDING_BOX_MUTATION [SYS_MSG] Judicial text string unreadable. Vector flattening detected. Fallback to manual GUI entry mandated.

(including, but not limited to, electronic correspondence, internal memorandums, CPIC system messages, and IT troubleshooting tickets) exchanged between the RCMP CPIC Governance Authority and the toronto police service (the "TPS") records management branch.

alerts and IT troubleshooting tickets are inherently generated. This requisition specifically targets communications regarding the authentication of the corrupted judicial initials "CL (M)", the resolution of vector collapse errors, and any inquiries regarding jurisdictional discrepancies observed between the physical court filings and the electronic mainframe entries during the September to October 2024 epoch. This encompasses any communications with specialized operational units or local registries regarding the absolute failure of the mandatory matching protocol (the "**Matching Protocol**"). A systemic error of this profound magnitude does not exist in a vacuum; a highly documented administrative paper trail of IT professionals attempting to reconcile the corrupted digital

error alerts generated automatically by the CPIC input gateway parsing engine.

390 585		artifacts is inevitably created.	471	
5.	PDF Flattening and Vector Analysis Reports All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, optical character recognition (the "OCR") interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.	This target is particularly directed at system interactions involving the GrapeCity Documents PDF suite (specifically version 6.0.2.0 and the documented DOC-6507 bug). Forensic analysis confirms this enterprise-level developer software was utilized with the specific <i>mens rea</i> to unlawfully flatten the document, forcefully eradicate the transparent electronic image signature of Chief Justice Geoffrey B. Morawetz, and algorithmically disfigure the underlying text to bypass standard criminal intake procedures. Specifically, the software's flattening engine violently clipped the mathematical bounding box of the "J" into an "L" and crushed the initials "G.B." into parentheses "()". Furthermore, records are requisitioned concerning the subsequent, deliberate	Native system alerts, proprietary software ingestion logs, and raw vector diagnostic exports demonstrating morphological collapse.	[VECTOR_ERR] DOC-6507 BOUNDING_BOX_MUTATION [TARGET] Morawetz_Sig_Block [STATUS] Flattened [CERT_OVERLAY] Frugoni-Rojas_Active

391 586		superimposition of a civilian clerk's digital certificate (Court Officer Christyn Frugoni-Rojas) directly over the corrupted artifact to act as a visual obfuscation, alongside the appending of a decoy Justice of the Peace signature line (George Jiri).	472	
6.	Offline Historical Search Results The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the absolute historical chronology of transactions.	The municipal record currently presents a glaring chronological impossibility: an arrest purportedly executed on October 2, 2024, followed by the inexplicable expungement of the purported warrant from provincial systems via the integrated court offences network (the "ICON") on October 3, 2024. A legally valid warrant does not evaporate the day following its execution; it is formally filed as a return to a justice. The RCMP's offline historical data stands as the singular remaining mechanism available to pierce this localized spoliation trap. Furthermore, this data is strictly necessitated to expose the	Offline archival CPIC search printouts generated by centralized data specialists, entirely devoid of redaction.	[OFFLINE_QUERY] 2024-10-04T08:15Z [TARGET_FILE] SCJ_Warrant_992 [RESULT] Warrant_Expunged_ICON_Sync [MODIFIER] TPS_Admin

392 587		retaliatory digital spoliation orchestrated by the justice sector security office (the "JSSO"), which weaponized cybersecurity infrastructure by deploying a 403 Forbidden Error to maliciously block the applicant's IP address from the Ontario Courts Public Portal upon the initial discovery of this jurisdictional nullity.	473	
7.	System Governance Manuals Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (the "MOU") with municipal partners specifically governing the Matching Protocol and the judicial firewall (the "Judicial Firewall").	This encompasses all operational directives establishing the rigorous responsibilities of the CPIC Coordinator to ensure that the electronic data entered perfectly mirrors the physical judicial order. There exists a mandatory air gap (the "Air Gap") between the judiciary and the police; the judiciary possesses no direct terminal access to input data into the CPIC database. Therefore, the structural integrity of the entire system relies unequivocally upon strict police compliance with this Matching Protocol. Manuals detailing	Unredacted PDF manuals, administrative directives, and inter-agency memoranda of understanding delineating operational liabilities.	[MANUAL_EXTRACT] Sec 4.2.1: SCJ vs OCJ Intake Protocols. Mandatory exact match required. GUI bypass strictly prohibited.

393 588		the rigorous, distinct standards required for the intake of Superior Court of Justice (the "SCJ") warrants versus provincial Ontario Court of Justice (the "OCJ") intake endorsements are required to prove exactly how these systemic checks and balances were illicitly bypassed to manufacture a facsimile of judicial authority.	474	

Respectfully submitted,

/s/ Mr. Kevin A. McLean (BA, JD, CIM)

Mr. Kevin A. McLean (B.A., J.D., CIM)

TAB 16

Tab A

591

DELIVERY METHOD: Via Registered Mail (Tracking) (copy to be provided via email)

Classification: Private and Confidential

TO:

Access To Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone: 647.370.9354

SUBJECT: FORMAL REQUEST UNDER THE *ACCESS TO INFORMATION* ACT (*ATIA*) – SOFTWARE PROCUREMENT, LICENSING, NTOP ONBOARDING, EMBEDDED IT ARCHITECTURE, AND AZURE CLOUD UTILIZATION RECORDS (GRAPECITY / MESCIUS SDKS)

Dear ATIP Coordinator,

1. Please accept this correspondence as a formal, highly specific, and multi-tiered statutory request for access to records under the *Access To Information Act (ATIA)*, R.S.C. 1985, c. A-1. The prescribed statutory application fee of \$5.00 is enclosed and/or processed concurrently with this transmission.
2. This request is strictly focused on objective, administrative, and technological procurement data regarding specific enterprise-grade software capabilities deployed within the federal law enforcement Information Technology (IT) ecosystem, specifically intersecting with the RCMP's "Cloud-First" regulatory framework and backend server-side document manipulation infrastructure.

I. STATUTORY RIGHT OF ACCESS, THE DUTY TO ASSIST, AND HEIGHTENED INSTITUTIONAL SCRUTINY

3. I make this request pursuant to Section 4(1) of the *Access To Information Act*:

4 (1) Subject to this Part, but notwithstanding any other Act of Parliament, every person who is
(a) a Canadian citizen, or

(b) a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act,
has a right to and shall, on request, be given access to any record under the control of a government institution.

4. Furthermore, I remind the ATIP Directorate of its absolute, mandatory obligations under Section 4(2.1) of the *ATIA*, which codifies the “Duty to Assist.” The institution is legally required to make every reasonable effort to assist the requester, to respond accurately and completely, and to provide timely access to the records in the format requested.
5. In the context of highly technical IT procurement, this duty strictly precludes the artificial narrowing of the scope of this request. It prohibits the reliance on rigid semantic technicalities to justify a “Nil” response (e.g., claiming no direct vendor contract exists when the software is procured indirectly or embedded).

INSTITUTIONAL CONTEXT & THE OPC 2023-2024 ANNUAL REPORT:

6. The ATIP Directorate is acutely aware that the RCMP is currently operating under intense, heightened external oversight regarding its use of third-party cloud services, embedded software applications, and algorithmic digital tools. This scrutiny has been explicitly codified in the **Office of the Privacy Commissioner of Canada’s (OPC) 2023-2024 Annual Report to Parliament on the Privacy Act, entitled “Trust, innovation, and protecting the fundamental right to privacy in the digital age.”** Following scathing OPC investigations (such as the “Project Wide Awake” report), the RCMP was heavily criticized for prioritizing digital innovation over fundamental rights by failing to conduct sufficient, legally mandated Privacy Impact Assessments (PIAs) prior to utilizing third-party data providers. In direct response to these parliamentary rebukes, the RCMP’s 2024–2025 Annual Report detailed a mandatory five-year modernization plan intended to clear ATIP backlogs and overhaul privacy systems. Given this explicit, publicly documented mandate to ensure that “innovation in the digital age” does not subvert constitutional rights, any attempt to obfuscate or delay this highly specific software inquiry will be viewed as a continuing, systemic breach of the very reforms the RCMP has promised Parliament it would implement.

II. DEFINITIONS, CORPORATE REBRANDING, AND SCOPE OF SEARCH: THE SDK DISTINCTION

7. To assist your Information Technology (IT), Procurement, and Shared Services Canada (SSC) liaison branches in conducting a thorough, legally compliant, and precise search, please be advised of the specific corporate and technological parameters of this request.
8. The software developer previously known globally as “**GrapeCity**” recently underwent a comprehensive corporate rebranding. The developer now operates under the corporate entity “**MESCIUS**” (or MESCIUS, USA). The corporate description for this vendor and its enterprise software suite is formally listed in industry indices as follows:

“We are Now MESCIUS, USA! Same great products. Same commitment to excellence. MESCIUS’ (pronounced mesh-ē-us) product line provides developers, designers, and architects with the ultimate collection of award-winning JavaScript and .NET grids, reporting, spreadsheets, document APIs, viewers, and mobile controls. Our tools help to quickly solve problems so you can focus on creativity, innovation, and optimization.”

9. For the purposes of this search, the software architectures targeted include, but are not strictly limited to, products previously named “**GrapeCity Documents for PDF**” (GcDocs), “**GrapeCity.Document.PDF**” (including specifically version 6.0.2.0, adjacent legacy versions, and subsequent patches), “**SpreadJS**,” “**ActiveReports**,” or any current iterations operating under the “**MESCIUS Document APIs**” nomenclature.

3970. **Crucial Technical Distinction:** This software is highly specialized. It is a **Software Development Kit (SDK)**, not a standard end-user desktop application (like Adobe Acrobat or Microsoft Word). It is an enterprise-grade library utilized exclusively for server-side, programmatic, “headless” generation, modification, algorithmic compression, redaction, and morphological alteration of PDF documents at the hexadecimal and Bezier-curve vector level, entirely bypassing standard Graphical User Interfaces (GUIs). Procurement of an SDK implies the existence of dedicated software developers, custom codebases, and backend server infrastructure.

III. FORENSIC JUSTIFICATION: SDK AUTOMATION, EXIF METADATA, AND THE CPIC “SINGLE SOURCE OF TRUTH”

11. The necessity of querying RCMP and SSC procurement records for GrapeCity/MESCIUS specifically stems from irrefutable, cryptographically sound forensic metadata extracted from a highly suspect, facially void Intake Court Endorsement utilized to detail and detain the Applicant. An independent EXIF data and metadata extraction report performed on the target file—identified as **Information Package 4810 998 24 48129169-00 (4).pdf** (File Size: 336 kB)—yields critical, incontrovertible structural anomalies that point directly to federal, non-provincial server-side software tools and programmatic spoofing.
12. These forensic indicators establish the absolute necessity of this *ATIA* request:
 - a. **The SDK / Automated Back-End Infrastructure Implication:** The identification of “GrapeCity Documents for PDF version 6.0.2.0” as the document producer is the ultimate forensic pivot. Because GrapeCity is an SDK, its presence dictates that the document was not manually scanned or generated via a localized courthouse copier. It was generated through an automated back-end system—likely a specialized integration within a localized federal police records management system or an enterprise-level government portal. This capability allows for the precise, automated “spoofing” of standard Ontario Court pro forma layouts.
 - b. **Intentional Assembly and XMP Toolkit Imprints:** The embedded structural metadata explicitly identifies the xmp_toolkit as **Adobe XMP Core 9.1-c001 79.675d0f7, 2023/06/11-19:21:16**, interacting in tandem with underlying GrapeCity document generation algorithms. This definitively proves the document in question was assembled and manipulated digitally using advanced enterprise code, utilizing developer APIs to overlay, redact, or inject text into existing templates.
 - c. **Linearization and Web Optimization:** The metadata formally confirms the document's structure as **linearized: Yes**. Linearization (also known as “Fast Web View”) is a highly specific file-saving protocol that requires enterprise-level document APIs to reorganize the PDF's internal byte structure, allowing it to be streamed over web servers byte-by-byte. Routine provincial court scanners do not output linearized PDFs. This proves the file was engineered, re-saved, and optimized by an advanced IT system designed for federal-level cloud or CPIC database transmission.
 - d. **Hexadecimal Raw Header Anomaly:** The raw hex dump of the document header reads **25 50 44 46 2D 31 2E 33** (which decodes to the legacy standard %PDF-1.3). Generating a legacy PDF-1.3 structural header while simultaneously utilizing a modern 2023 Adobe XMP core toolkit is a hallmark of enterprise software (like the GrapeCity SDK) operating in a highly restricted, heavily customized backend environment intentionally forcing compatibility with legacy mainframe systems (such as CPIC).
 - e. **Atypical Tooling and the 5-Page Mathematical Impossibility:** Most legitimate Ontario Court documents are generated natively by the Integrated Court Offence Network (ICON) or Criminal Justice Digital Design (CJDD). Finding a GrapeCity enterprise producer tag embedded within these files is highly irregular for a standard provincial court output. Furthermore, the proper provincial pro forma dictates a 6-page layout, yet the exact structural extraction confirms the fabricated file contains exactly **page_number: 5**. This mathematical certainty corroborates the forensic conclusion that a critical page was programmatically, surgically, and intentionally removed during the GrapeCity digital assembly process.
 - f. **The Subversion of Jurisdictional Integrity and the CPIC Repository:** The GrapeCity SDK was utilized to manufacture a front-end document that successfully bypassed standard administrative standards (e.g., misapplying family-law intake standards to a criminal endorsement). Consequently, the physical PDF itself has been irrevocably de-authenticated. This elevates the **Canadian Police Information Centre (CPIC)** transaction logs to the role of

IV. INTAKE COURT ENDORSEMENTS AND ARREST WARRANTS - PROTECTED B CLASSIFICATION

13. To provide necessary operational context for the IT systems being queried, it must be acknowledged that judicial instruments such as Intake Court Endorsements and arrest warrants signed by judges are strictly classified as **Protected B** information. The Treasury Board of Canada Secretariat explicitly defines Protected B as information that, if disclosed without authorization, could cause serious injury to an individual, organization, or the government.
14. Arrest warrants and judicial endorsements inherently meet this “serious injury” threshold for the following reasons:
 - a. **Information about Legal Proceedings:** Government security guidelines specifically classify records of active legal proceedings or criminal investigations within the Protected B category.
 - b. **Sensitive Personal Identifiers:** Warrants contain hyper-sensitive data, including a person's full name, address, date of birth, and highly protected administrative/biometric identifiers. Unauthorized leaks constitute a severe privacy breach.
 - c. **Operational Risk:** The unauthorized disclosure of a warrant prior to its execution carries severe operational risks, potentially subverting the ends of justice, compromising surveillance, or endangering officers.

HANDLING REQUIREMENTS FOR PROTECTED B INSTRUMENTS:

15. Because these judicial instruments are Protected B, the RCMP and all interfacing federal agencies are bound by strict, non-negotiable safeguarding protocols. Consequently, any software SDK—such as MESCIUS or GrapeCity—used to programmatically draft, manipulate, render, or redact these instruments must be utilized within a framework that complies with the following:
 - a. **Digital Storage:** Digital versions must be saved in secure, highly restricted systems like GCdocs or Protected B-compliant cloud environments (e.g., Microsoft Azure's Canadian regions).
 - b. **Physical Security:** When not in active use, physical derivatives must be stored in lockable containers exhibiting signs of attempted entry.
 - c. **Access Protocols:** Only personnel maintaining a valid Reliability Status screening, operating strictly on a “need-to-know” basis, are authorized to access, alter, or interact with these documents via digital software systems.

V. PROTECTED B CLOUD ARCHITECTURE, AZURE INTEGRATION, AND GC CLOUD GUARDRAILS

16. The RCMP currently manages its digital infrastructure and cloud storage through a highly regulated, “Cloud-First” strategy mediated by Shared Services Canada (SSC). For the sensitive **Protected B** information detailed above, the RCMP primarily utilizes **Microsoft Azure** as its enterprise standard.
17. Because MESCIUS (GrapeCity) developer SDK libraries are fundamentally engineered to operate seamlessly within Microsoft .NET and Azure environments, the integration of these server-side PDF-rendering APIs into the RCMP's Azure-based digital evidence and records management systems is highly probable. **Therefore, the ATIP office must extend its search parameters to include the following regulatory and architectural frameworks:**
 - a. **The National Technology Onboarding Program (NTOP):** All new operational technologies—ranging from Axon’s “Draft One” AI-powered report drafting tools to specialized document redaction APIs and SDKs—must be formally onboarded through NTOP. This program is responsible for ensuring cloud-based tools meet strict legal, ethical, and GC Cloud Guardrail standards before deployment. *The ATIP search must query NTOP records for any onboarding evaluations, security clearances, or rejections associated with MESCIUS, GrapeCity, or their underlying SDK components.*

3970. **Crucial Technical Distinction:** This software is highly specialized. It is a **Software Development Kit (SDK)**, not a standard end-user desktop application (like Adobe Acrobat or Microsoft Word). It is an enterprise-grade library utilized exclusively for server-side, programmatic, “headless” generation, modification, algorithmic compression, redaction, and morphological alteration of PDF documents at the hexadecimal and Bezier-curve vector level, entirely bypassing standard Graphical User Interfaces (GUIs). Procurement of an SDK implies the existence of dedicated software developers, custom codebases, and backend server infrastructure.

III. FORENSIC JUSTIFICATION: SDK AUTOMATION, EXIF METADATA, AND THE CPIC “SINGLE SOURCE OF TRUTH”

11. The necessity of querying RCMP and SSC procurement records for GrapeCity/MESCIUS specifically stems from irrefutable, cryptographically sound forensic metadata extracted from a highly suspect, facially void Intake Court Endorsement utilized to detail and detain the Applicant. An independent EXIF data and metadata extraction report performed on the target file—identified as **Information Package 4810 998 24 48129169-00 (4).pdf** (File Size: 336 kB)—yields critical, incontrovertible structural anomalies that point directly to federal, non-provincial server-side software tools and programmatic spoofing.
12. These forensic indicators establish the absolute necessity of this *ATIA* request:
 - a. **The SDK / Automated Back-End Infrastructure Implication:** The identification of “GrapeCity Documents for PDF version 6.0.2.0” as the document producer is the ultimate forensic pivot. Because GrapeCity is an SDK, its presence dictates that the document was not manually scanned or generated via a localized courthouse copier. It was generated through an automated back-end system—likely a specialized integration within a localized federal police records management system or an enterprise-level government portal. This capability allows for the precise, automated “spoofing” of standard Ontario Court pro forma layouts.
 - b. **Intentional Assembly and XMP Toolkit Imprints:** The embedded structural metadata explicitly identifies the xmp_toolkit as **Adobe XMP Core 9.1-c001 79.675d0f7, 2023/06/11-19:21:16**, interacting in tandem with underlying GrapeCity document generation algorithms. This definitively proves the document in question was assembled and manipulated digitally using advanced enterprise code, utilizing developer APIs to overlay, redact, or inject text into existing templates.
 - c. **Linearization and Web Optimization:** The metadata formally confirms the document's structure as **linearized: Yes**. Linearization (also known as “Fast Web View”) is a highly specific file-saving protocol that requires enterprise-level document APIs to reorganize the PDF's internal byte structure, allowing it to be streamed over web servers byte-by-byte. Routine provincial court scanners do not output linearized PDFs. This proves the file was engineered, re-saved, and optimized by an advanced IT system designed for federal-level cloud or CPIC database transmission.
 - d. **Hexadecimal Raw Header Anomaly:** The raw hex dump of the document header reads **25 50 44 46 2D 31 2E 33** (which decodes to the legacy standard %PDF-1.3). Generating a legacy PDF-1.3 structural header while simultaneously utilizing a modern 2023 Adobe XMP core toolkit is a hallmark of enterprise software (like the GrapeCity SDK) operating in a highly restricted, heavily customized backend environment intentionally forcing compatibility with legacy mainframe systems (such as CPIC).
 - e. **Atypical Tooling and the 5-Page Mathematical Impossibility:** Most legitimate Ontario Court documents are generated natively by the Integrated Court Offence Network (ICON) or Criminal Justice Digital Design (CJDD). Finding a GrapeCity enterprise producer tag embedded within these files is highly irregular for a standard provincial court output. Furthermore, the proper provincial pro forma dictates a 6-page layout, yet the exact structural extraction confirms the fabricated file contains exactly **page_number: 5**. This mathematical certainty corroborates the forensic conclusion that a critical page was programmatically, surgically, and intentionally removed during the GrapeCity digital assembly process.
 - f. **The Subversion of Jurisdictional Integrity and the CPIC Repository:** The GrapeCity SDK was utilized to manufacture a front-end document that successfully bypassed standard administrative standards (e.g., misapplying family-law intake standards to a criminal endorsement). Consequently, the physical PDF itself has been irrevocably de-authenticated. This elevates the **Canadian Police Information Centre (CPIC)** transaction logs to the role of

IV. INTAKE COURT ENDORSEMENTS AND ARREST WARRANTS - PROTECTED B CLASSIFICATION

13. To provide necessary operational context for the IT systems being queried, it must be acknowledged that judicial instruments such as Intake Court Endorsements and arrest warrants signed by judges are strictly classified as **Protected B** information. The Treasury Board of Canada Secretariat explicitly defines Protected B as information that, if disclosed without authorization, could cause serious injury to an individual, organization, or the government.
14. Arrest warrants and judicial endorsements inherently meet this “serious injury” threshold for the following reasons:
 - a. **Information about Legal Proceedings:** Government security guidelines specifically classify records of active legal proceedings or criminal investigations within the Protected B category.
 - b. **Sensitive Personal Identifiers:** Warrants contain hyper-sensitive data, including a person's full name, address, date of birth, and highly protected administrative/biometric identifiers. Unauthorized leaks constitute a severe privacy breach.
 - c. **Operational Risk:** The unauthorized disclosure of a warrant prior to its execution carries severe operational risks, potentially subverting the ends of justice, compromising surveillance, or endangering officers.

HANDLING REQUIREMENTS FOR PROTECTED B INSTRUMENTS:

15. Because these judicial instruments are Protected B, the RCMP and all interfacing federal agencies are bound by strict, non-negotiable safeguarding protocols. Consequently, any software SDK—such as MESCIUS or GrapeCity—used to programmatically draft, manipulate, render, or redact these instruments must be utilized within a framework that complies with the following:
 - a. **Digital Storage:** Digital versions must be saved in secure, highly restricted systems like GCdocs or Protected B-compliant cloud environments (e.g., Microsoft Azure's Canadian regions).
 - b. **Physical Security:** When not in active use, physical derivatives must be stored in lockable containers exhibiting signs of attempted entry.
 - c. **Access Protocols:** Only personnel maintaining a valid Reliability Status screening, operating strictly on a “need-to-know” basis, are authorized to access, alter, or interact with these documents via digital software systems.

V. PROTECTED B CLOUD ARCHITECTURE, AZURE INTEGRATION, AND GC CLOUD GUARDRAILS

16. The RCMP currently manages its digital infrastructure and cloud storage through a highly regulated, “Cloud-First” strategy mediated by Shared Services Canada (SSC). For the sensitive **Protected B** information detailed above, the RCMP primarily utilizes **Microsoft Azure** as its enterprise standard.
17. Because MESCIUS (GrapeCity) developer SDK libraries are fundamentally engineered to operate seamlessly within Microsoft .NET and Azure environments, the integration of these server-side PDF-rendering APIs into the RCMP's Azure-based digital evidence and records management systems is highly probable. **Therefore, the ATIP office must extend its search parameters to include the following regulatory and architectural frameworks:**
 - a. **The National Technology Onboarding Program (NTOP):** All new operational technologies—ranging from Axon’s “Draft One” AI-powered report drafting tools to specialized document redaction APIs and SDKs—must be formally onboarded through NTOP. This program is responsible for ensuring cloud-based tools meet strict legal, ethical, and GC Cloud Guardrail standards before deployment. *The ATIP search must query NTOP records for any onboarding evaluations, security clearances, or rejections associated with MESCIUS, GrapeCity, or their underlying SDK components.*

- b. **GC Cloud Guardrails and Data Residency:** To host Protected B data, the RCMP must comply with mandatory security configurations, including Multi-Factor Authentication (MFA) and the “principle of least privilege.” While the Sovereign Cloud Initiative (2025) pushes for Canadian-owned providers to eliminate risks associated with foreign legislation (e.g., the US CLOUD Act), personal information is still routinely hosted on US-based providers (like Microsoft Azure) provided comparable written security agreements are executed. *The search must identify any written security agreements, data residency waivers, or GC Cloud Guardrail compliance matrices associated with the deployment of MESCIUS (a US-based corporate entity) SDKs within the RCMP’s Protected B infrastructure.*
- c. **The “Internal Solution” Silo and Physical Safeguards:** Highly sensitive data (including cybercrime investigative records or restricted terminal logs) is often segregated into specialized analytical triage repositories, such as the “Internal Solution.” *The search must query IT architecture records to determine if GrapeCity/MESCIUS SDK APIs are utilized to automatically generate, redact, or encrypt documents originating from or entering the “Internal Solution” data silo.*

VI. TARGETED ALIGNMENT WITH 2020–2025 RCMP MEGA-PROJECTS

18. Preliminary forensic research into federal IT expenditures via the Open Government Portal and CanadaBuys databases yields no immediate public record of a direct, department-wide, standalone contract awarded by the RCMP directly to MESCIUS or GrapeCity.
19. However, it is a well-established federal IT reality that tools like GrapeCity/MESCIUS function as “invisible” foundational components. They are highly compatible developer libraries that are fundamentally embedded within the custom, large-scale backend applications built by the RCMP’s primary macro-vendors. **Therefore, I am explicitly directing the ATIP office to query the project managers, software architects, and procurement officers associated with the following specific RCMP IT acquisitions (2020-2025) where MESCIUS/GrapeCity libraries are highly likely to be embedded:**
- a. **Microsoft 365 and SharePoint Online Migration (2024–2025):** The RCMP is currently undergoing a massive modernization of its security assessment processes and document management architectures utilizing Microsoft 365. MESCIUS Document Solutions and ActiveReports are industry-standard libraries specifically utilized by enterprise developers to automate the headless generation, manipulation, and rendering of complex PDFs directly from SharePoint data repositories and Azure .NET environments.
- b. **Canadian Firearms Digital Services Solution (CFDSS):** This massive cloud migration and modernization project, actively managed by **Accenture Inc.**, was commissioned to replace outdated, legacy client-facing portals. Large-scale digital portals of this magnitude routinely and inevitably utilize third-party backend SDKs (such as MESCIUS APIs) to handle the high-volume, secure algorithmic generation of complex legal documents without crashing the server infrastructure.
- c. **Axon Digital Evidence Management System (DEMS):** The RCMP’s sprawling **\$136.4 million contract** with Axon encompasses advanced, AI-powered tools for transcribing, managing, and, crucially, *redacting* digital evidence and generating evidentiary reports. While Axon operates as a largely closed ecosystem, the specialized PDF-viewing, redaction, and reporting utilities embedded within their “Productivity Suite” frequently rely on licensed, underlying enterprise architectural components identical or analogous to those offered by MESCIUS/GrapeCity.

VII. PROCUREMENT PATTERNS AND AUTHORIZED RESELLER DIRECTIVES

20. Government departments rarely, if ever, purchase backend developer libraries directly from entities like MESCIUS. Instead, these libraries are sourced through Value-Added Resellers (VARs) who hold active federal Software Licensing Supply Arrangements (SLSAs). **I am formally directing the ATIP office to search procurement logs**

400 482
598 referencing the following specific authorized Canadian resellers and Master Distributors known to bid on general software contracts on behalf of MESCIUS:

- a. **Insight Canada**
- b. **Softchoice**
- c. **SHI Canada (SHI International)**
- d. **ComponentSource** (Operating as a Master Distributor for developer SDK components)
- e. **SoftwareONE** and **Compugen**

21. If the RCMP procured GrapeCity/MESCIUS SDK developer licenses, they were almost certainly routed through the SLSA framework via one of the aforementioned corporate entities.

VIII. THE REQUESTED RECORDS

22. I am formally requesting access to the following specific classes of records under the control of the Royal Canadian Mounted Police (RCMP), encompassing the comprehensive timeframe of **January 1, 2018, to the present date:**

- a. **Indirect and Direct Procurement/Licensing Records:** Any and all records, including purchase orders, end-user licensing agreements (EULAs), vendor contracts, invoices, expenditure approvals, Software Licensing Supply Arrangement (SLSA) call-ups, or budgetary line items demonstrating that the RCMP (or SSC on behalf of the RCMP) has purchased, licensed, or procured GrapeCity/MESCIUS Software Development Kits (SDKs) and/or API access, either directly from the developer or via third-party resellers (e.g., Insight Canada, Softchoice, ComponentSource).
- b. **NTOP Onboarding and Compliance Records:** All records, matrices, and security evaluations generated by the National Technology Onboarding Program (NTOP) regarding the approval, rejection, or conditional use of MESCIUS/GrapeCity developer tools. This must include any GC Cloud Guardrail compliance checks and data residency agreements executed to permit this software to interact with Protected B data on Microsoft Azure servers.
- c. **Embedded IT Architecture, Server-Side Integration, and Mega-Project Logs:** Any internal software architecture diagrams, deployment records, backend integration scripts, vendor technical specifications, or embedded library logs specifically related to the **Microsoft 365/SharePoint Migration, the CFDSS (Accenture), the Axon DEMS projects, or the "Internal Solution" data silo**, indicating that GrapeCity/MESCIUS PDF manipulation tools, SpreadJS, ActiveReports, Document APIs, or .NET/JavaScript grids are embedded within these server-side systems.
- d. **Software Lifecycle and Version Control Logs:** Any IT change-management logs, update tickets, developer requisition forms, or system administration records documenting the installation, upgrading, deprecation, or patching of GrapeCity.Document.PDF (specifically referencing version 6.0.2.0 or subsequent iterations) within the RCMP network, developer workstations, or CPIC-interfacing servers.
- e. **User Manuals, Document Integrity Protocols, and Internal Directives:** Any internal training materials, IT support tickets, developer manuals, Threat Risk Assessments (TRAs), or administrative directives referencing the utilization of GrapeCity or MESCIUS SDKs for the specific operational purposes of automated backend document creation, programmatic PDF generation, headless PDF redaction, algorithmic document alteration, or metadata manipulation by RCMP personnel or contracted developers. Consistent with the OPC's 2023-2024 directives to Parliament, this explicitly includes any **Privacy Impact Assessments (PIAs)** conducted to validate the use of these tools against public privacy rights.

IX. SEVERABILITY AND PRESERVATION OF RECORDS

23. Should any portion of the requested procurement records contain sensitive third-party financial data (e.g., specific negotiated unit pricing with a VAR like Softchoice or Insight Canada) that the institution deems exempt under

401 599 483 Section 20 of the *ATIA*, I remind the coordinator of the strict statutory obligation under Section 25 to sever the exempt financial material and disclose the remainder of the record. **The factual existence of a software license, its NTOP onboarding status, or its presence in a backend IT architecture diagram cannot be withheld merely because its purchase price is protected.**

24. Furthermore, given the extreme technical specificity of this request regarding backend IT infrastructure, SDK deployments, and active mega-projects, I hereby put the RCMP on formal notice to institute an **immediate administrative and IT preservation hold** on all responsive records. This includes directing the IT Directorate, the NTOP governance board, and the project managers for the M365, CFDSS, and Axon deployments to prevent the routine automated purging, overwriting, or deletion of software inventory logs, deployment metadata, and licensing repositories while this *ATIA* request is being processed.

X. FORMAT OF DISCLOSURE

25. I request that all responsive records be provided in an electronic format (searchable PDF).

XI. ENCLOSURES, PDF BOOKMARK DIRECTIVES, AND FEE CONFIRMATION

26. As this physically signed and couriered document serves as the formal *ATIA* request, please consider this section as explicit confirmation that the mandatory statutory application fee of **five dollars (\$5.00)** is enclosed herewith.

27. Furthermore, to assist your technical review and provide operational context for the requested software architectures, the enclosed PDF package contains embedded bookmarks of critical evidentiary importance. The ATIP office and consulting IT directorates are explicitly directed to observe the following bookmark architecture:

- a. **Front Page:** Directs to Page 1.
- b. **Adjournment:** Directs to Page 1.
 - i. *Subheading under Adjournment:* “**MCLEAN, KEVIN**” directs to Page 4 of 5.
- c. **Back Page (sic):** Directs to Page 5 of 5.

28. These navigational markers denote specific structural anomalies and document mutations that underscore the absolute necessity of obtaining the GrapeCity/MESCIUS architectural and SDK utilization records requested herein.

29. The reason for providing this in advance of when the 30 statutory (day) clock commences is to provide the electronic copy of the “False Information Package” so you can utilize the PDF (Adobe) bookmark navigation and clearly review the embedded “Document Properties” and associated EXIF/metadata outputs (as cross-referenced in Section III). Once received, you can respond under this thread.

30. The underlying necessity for these specific architectural and procurement records should be self-evident to your IT infrastructure, federal procurement, and compliance directorates. Should you require any clarification regarding the technical parameters, vendor networks, or search methodology of this request, please contact me immediately via email to avoid unnecessary statutory delays or constructive refusals.

31. Thank you for your prompt attention to this statutory imperative. I will confirm via email when the hard copy document with statutory fee has been delivered so we work together in this access partnership.

Sincerely,

Electronically signed



Mr. Kevin A. McLean

Enclosures:

402. The False Information Package as obtained from the CCJ 10 Armoury Street Courthouse (which was identical to the document obtained by counsel to the TPS in an HRTO Proceeding in March 2025 but for amendments to case history);
2. The standard Lincoln County Law Association (Niagara) Adult Common Form Information Package

Tab B

Track: 0105952086612346

Share

Print

Delivered

May 7 at 9:38 am

Updated: Today at 10:16 am



Received by

Canada Post

May 6



Delivered

May 7

Delivery information

Sender: Unavailable

Service information

Latest updates

View more

Track another item

Support

What's an expected delivery?	+
What's a delivery standard?	+
What's a delivery confirmation?	+
How do I sign up for text notifications?	+
What if my package is missing?	+

See more support (/cpc/en/support/kb/tracking/overview.page)

Service alerts

These events may affect delivery schedules.

See all service alerts (/cpc/en/our-company/news-and-media/service-alerts.page?)

Connect with us

Corporate (https://www.canadapost-sustainabilitypostescanada.ca/cpc/en/our-company/about-us/corporate-sustainability.page)	feedbackQ_lang=EN)
	Provide (https://www.canadapost-accessibilitypostescanada.ca/cpc/en/our-feedback company/accessibility/accessibility-

<https://www.canadapost-na.com/postescanada.ca/cpc/en/home.page?>

[Sending](https://www.canadapost-na.com/postescanada.ca/cpc/en/home.page?)

[Receiving](https://www.canadapost-na.com/postescanada.ca/cpc/en/home.page?)

[Money services](https://www.canadapost-na.com/postescanada.ca/cpc/en/home.page?)

[Stamps and coins](https://www.canadapost-na.com/postescanada.ca/cpc/en/home.page?)

[Tools](https://www.canadapost-na.com/postescanada.ca/cpc/en/home.page?)

[Research participant company/research-panel.page\)](https://www.canadapost-na.com/postescanada.ca/cpc/en/home.page?)

[Media \(https://www.canadapost-centre.postescanada.ca/cpc/en/our-company/news-and-media/media-centre.page\)](https://www.canadapost-centre.postescanada.ca/cpc/en/our-company/news-and-media/media-centre.page)

[Negotiations\(https://www.canadapost-updates.postescanada.ca/cpc/en/our-company/news-and-media/corporate-news/negotiations-list.page\)](https://www.canadapost-updates.postescanada.ca/cpc/en/our-company/news-and-media/corporate-news/negotiations-list.page)

Blogs

[Business Matters \(https://www.canadapost-business-matters.postescanada.ca/blogs/business\)](https://www.canadapost-business-matters.postescanada.ca/blogs/business)

[Canada Post Magazine \(https://www.canadapost-magazine.postescanada.ca/blogs/personal\)](https://www.canadapost-magazine.postescanada.ca/blogs/personal)

Support

[Contact\(https://www.canadapost-us.postescanada.ca/cpc/en/support.page#panel2-1\)](https://www.canadapost-us.postescanada.ca/cpc/en/support.page#panel2-1)

[Service\(https://www.canadapost-alerts.postescanada.ca/cpc/en/our-company/news-and-media/service-alerts.page\)](https://www.canadapost-alerts.postescanada.ca/cpc/en/our-company/news-and-media/service-alerts.page)

[Accessibility\(https://www.canadapost-accessibility.postescanada.ca/cpc/en/our-company/about-us/corporate-responsibility/accessibility.page\)](https://www.canadapost-accessibility.postescanada.ca/cpc/en/our-company/about-us/corporate-responsibility/accessibility.page)

Canada Post

[Our \(https://www.canadapost-company.postescanada.ca/cpc/en/our-company.page\)](https://www.canadapost-company.postescanada.ca/cpc/en/our-company.page)

[Corporate \(https://www.canadapost-sustainability.postescanada.ca/cpc/en/our-company/about-us/corporate-sustainability.page\)](https://www.canadapost-sustainability.postescanada.ca/cpc/en/our-company/about-us/corporate-sustainability.page)

Support

Connect with us

Blogs

[Sending](#)

[Receiving](#)

[Money services](#)

[Stamps and coins](#)

[Tools](#)

[Media \(https://www.canadapost-postescanada.ca/cpc/en/our-company/news-and-media/media-centre.page\)](https://www.canadapost-postescanada.ca/cpc/en/our-company/news-and-media/media-centre.page)

[Negotiations\(https://www.canadapost-postescanada.ca/cpc/en/our-company/news-and-media/corporate-news/negotiations-list.page\)](https://www.canadapost-postescanada.ca/cpc/en/our-company/news-and-media/corporate-news/negotiations-list.page)

[Legal\(https://www.canadapost-postescanada.ca/cpc/en/support/kb/company-policies/terms-conditions/legal-terms\)](https://www.canadapost-postescanada.ca/cpc/en/support/kb/company-policies/terms-conditions/legal-terms)

[Privacy\(https://www.canadapost-postescanada.ca/cpc/en/our-company/about-us/transparency-and-trust/privacy-policy\)](https://www.canadapost-postescanada.ca/cpc/en/our-company/about-us/transparency-and-trust/privacy-policy)

[Access to information\(https://www.canadapost-postescanada.ca/cpc/en/our-company/about-us/transparency-and-trust/access-to-information\)](https://www.canadapost-postescanada.ca/cpc/en/our-company/about-us/transparency-and-trust/access-to-information)

Tab C

**Access to Information Act request A-2026-01933 / F281, Your File N/A,
Acknowledgment**

1 message

ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>
To: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Mon, May 11, 2026 at 10:40 AM

Dear Kevin McLean:

This is to acknowledge receipt of your request under the Access to Information Act, which was received by this office on May 8, 2026, for:

Formal request under the Access to Information Act (ATIA) - software procurement, licensing, NTOP onboarding, embedded it architecture, and azure cloud utilization records (grapecity / mescius sdks)

This request is strictly focused on objective, administrative, and technological procurement data regarding specific enterprise-grade software capabilities deployed within the federal law enforcement Information Technology (IT) ecosystem, specifically intersecting with the RCMP's "Cloud-First" regulatory framework and backend server-side document manipulation infrastructure.

Please be advised that we are currently proceeding with your request. The Royal Canadian Mounted Police is committed to assisting you with your request and we will ensure that every reasonable effort is made to help you receive a complete, accurate and timely response.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online: <https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing in this email.

Regards,

Bryan
Access to Information and Privacy Branch
Mailstop #61
[73 Leikin Drive](#)
Ottawa, Ontario [K1A 0R2](#)

CONFIDENTIALITY NOTICE:

This e-mail message, including attachments, is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

Tab D

610

CLASSIFICATION: Private and Confidential

DATE: May 11, 2026

TO: Office of the Information Commissioner of Canada 30 Victoria Street, 7th Floor Gatineau, Quebec K1A 1H3

FROM: Kevin A. McLean (B.A., J.D., CIM) Email: mcleansettlement@gmail.com

SUBJECT: FORMAL COMPLAINT PURSUANT TO SECTION 30 OF THE ACCESS TO INFORMATION ACT CONCERNING CONSTRUCTIVE REFUSAL, UNLAWFUL EXTENSION, AND INSTITUTIONAL RECALCITRANCE BY THE ROYAL CANADIAN MOUNTED POLICE (FILE: A-2026-01933 / F281)

I. PRELIMINARY ASSERTIONS AND JURISDICTIONAL INVOCATION

1. A formal complaint is hereby promulgated pursuant to the statutory authority vested in the Information Commissioner under section 30 of the *Access to Information Act*, R.S.C. 1985, c. A-1 (the "**Act**").
2. The intervention of the Office of the Information Commissioner is urgently necessitated to rectify the overt statutory non-compliance, *ultra vires* administrative delay tactics, and constructive refusal effectuated by the Royal Canadian Mounted Police (the "**Government Institution**") concerning the targeted access request designated as File No. A-2026-01933 / F281 (the "**Access Request**").
3. It is respectfully submitted that the Government Institution has engaged in a deliberate pattern of administrative obfuscation. This includes the issuance of a facially void processing notification devoid of statutory grounding, followed by a complete cessation of communication upon being served with a formal notice of their statutory defect.

II. CHRONOLOGICAL COMPUTATION OF TIME AND FACTUAL MATRIX

4. To facilitate an expeditious investigatory assessment by the Commissioner, the procedural chronology—corroborated by the annexed evidentiary exhibits—is delineated herein:

Procedural Milestone	Statutorily Recognized Date	Factual Corroboration and Legal Consequence
Transmission of Request	May 5, 2026	Formal Access Request transmitted with prescribed statutory fee, seeking discrete GrapeCity/MESCIUS software procurement and Azure cloud architecture logs.
Effectuated Delivery	May 7, 2026	Delivery confirmed via Canada Post (Tracking: 0105952086612346). <i>Commencement of the non-negotiable thirty-day limitation period.</i>
Defective Acknowledgment	May 11, 2026	Government Institution transmits an email acknowledging receipt but asserts an open-ended processing delay ("currently proceeding") without citing any statutory grounds under section 9(1).
Notice of Non-Compliance	May 11, 2026	Complainant formally serves the Government Institution with a Demand for Strict Computation of Time, explicitly citing the illegality of the generalized extension and inquiring about mandatory section 9(2) notice to the OIC.
Institutional Silence	Post-May 11, 2026	The Government Institution completely fails to respond to the formal Notice of Non-Compliance, operating in flagrant disregard of the transparency framework.
Statutory Deadline	June 6, 2026	Crystallization of the absolute statutory deadline. Failure to produce records constitutes a deemed refusal.

495 110 GROUNDS FOR COMPLAINT: THE DOCTRINE OF NULLITY AND UNLAWFUL EXTENSION

5. **Ground 1: Unlawful Extension of Time Limits.** The administrative correspondence issued by the Government Institution on May 11, 2026, is *prima facie* non-compliant. Section 9(1) of the *Access to Information Act* mandates that any temporal extension must be inextricably tethered to the enumerated statutory preconditions (paragraphs *a*, *b*, or *c*).
6. By relying exclusively upon generalized boilerplate vernacular—failing entirely to articulate a specific statutory exemption or the precise length of the purported extension—the Government Institution's action is elevated beyond a mere procedural irregularity; it is an absolute nullity *ab initio*. As articulated in *Statham v. Canadian Broadcasting Corporation*, 2010 FCA 315, the failure to statutorily notify an applicant of the precise grounds for extension strictly invalidates the attempted delay.
7. **Ground 2: Failure to Provide Notice to the Commissioner.** It is advanced that the Government Institution failed to comply with its mandatory reporting obligations under section 9(2) of the Act, which requires contemporaneous notification to the Information Commissioner when an extension exceeds thirty days. The Government Institution's failure to respond to the Complainant's direct inquiry regarding this matter strongly suggests an *ultra vires* circumvention of statutory oversight.

IV. GROUNDS FOR COMPLAINT: IMPERMISSIBLE NARROWING AND DEEMED REFUSAL

8. **Ground 3: Constructive / Deemed Refusal.** The failure of the Government Institution to validly extend the time limit, coupled with their subsequent recalcitrant silence following the Complainant's May 11, 2026, demand letter, solidifies a state of deemed refusal pursuant to section 10(3) of the Act.
9. **Ground 4: Derogation of the Duty to Assist and Impermissible Narrowing.** The Access Request was surgically drafted to extract objective, administrative, and technological procurement data concerning GrapeCity and MESCIUS software development kits deployed within the federal law enforcement IT ecosystem. This is inextricably linked to the creation of heavily manipulated judicial instruments, as evidenced by the annexed "False Information Package" and the "Chart-FIP and GrapeCity-demonstrating 43 errors."
10. In direct contravention of the jurisprudential mandate established in *Canada (Information Commissioner) v. Minister of National Defence*, 2011 SCC 25, the Government Institution is engaging in an impermissible administrative narrowing. By ignoring the request for underlying application programming interfaces (APIs), Azure cloud utilization logs, and structural metadata validations, the institution is subverting the statutory duty to assist. The legal maxim *quando aliquid mandatur, mandatur et omne per quod pervenitur ad illud* applies directly: the Government Institution must be compelled to deploy the requisite technological means to query and extract these embedded database logs, rather than feigning technological ignorance.

V. RELIEF SOUGHT AND CONCLUDING DIRECTIVES

11. The arbitrary suppression of these architectural procurement logs severely prejudices the Complainant and insulates potentially compromised federal IT infrastructure from requisite public scrutiny.
12. Predicated upon the foregoing matrix of facts and undeniable statutory breaches, it is formally requested that the Office of the Information Commissioner:
 - **A.** Initiate an immediate, expedited investigation into the Government Institution's handling of Request A-2026-01933 / F281;
 - **B.** Render a formal declaration that the Government Institution's May 11, 2026, processing notification is a legal nullity and constitutes an unlawful extension;
 - **C.** Issue a binding order compelling the Government Institution to immediately cease its constructive refusal and remit the complete, unredacted GrapeCity/MESCIUS technological procurement logs and metadata architecture as explicitly detailed in the Access Request.
13. Should this institutional recalcitrance persist, the Complainant remains fully prepared to escalate this matter to the Federal Court for an order of *mandamus*.

Sincerely,



612
ENCLOSURES:

1. Formal Access Request (ATIP) – GrapeCity/MESCIUS SDKs (Signed May 5, 2026)
2. Canada Post Delivery Confirmation (Track: 0105952086612346 - May 7, 2026)
3. Government Institution Defective Acknowledgment Email (May 11, 2026)
4. Complainant's Notice of Statutory Non-Compliance and Demand Letter (May 11, 2026)
5. Chart - FIP and GrapeCity Demonstrating 43 Errors in FIP
6. False Information Package (Information Package 4810 998 24 48129169-00)
7. Lincoln County Law Association Valid CCO Information Standard Form Package

Contact information

Your contact information

First name: Kevin

Last name: McLean

Street address: 68 Abell St

City/Town: Toronto

Province/Territory: Ontario

Country: Canada

Postal code: M6J 0B1

How would you like the Office of the Information Commissioner (OIC) to contact you about this complaint?

Email address: mcleansettlement@gmail.com

How would you like to receive correspondence and reports from the OIC about this complaint?

Email address: As above

In which official language should the OIC communicate with you about this complaint? English

Complaint

Name of the institution that is the subject of your complaint: Royal Canadian Mounted Police

**Access request
number****OIC file number****Complaint type****Additional
information**

A-2026-01933 / F281

Extension of time

DELIVERY METHOD:
Via Electronic
Transmission / OIC
Online Portal
CLASSIFICATION:
Private and
Confidential DATE:
May 11, 2026 TO:
Office of the
Information
Commissioner of
Canada 30 Victoria
Street, 7th Floor
Gatineau, Quebec K1A
1H3FROM: Kevin A.
McLean (B.A., J.D.,
CIM) Email:
mcleansettlement@gm
ail.comSUBJECT:
FORMAL COMPLAINT
PURSUANT TO
SECTION 30 OF THE
ACCESS TO
INFORMATION ACT
CONCERNING
CONSTRUCTIVE
REFUSAL,
UNLAWFUL
EXTENSION, AND
INSTITUTIONAL
RECALCITRANCE BY
THE ROYAL
CANADIAN
MOUNTED POLICE
(FILE: A-2026-01933 /
F281)I. PRELIMINARY
ASSERTIONS AND
JURISDICTIONAL
INVOCATION1.A

formal complaint is hereby promulgated pursuant to the statutory authority vested in the Information Commissioner under section 30 of the Access to Information Act, R.S.C. 1985, c. A-1 (the "Act").² The intervention of the Office of the Information Commissioner is urgently necessitated to rectify the overt statutory non-compliance, ultra vires administrative delay tactics, and constructive refusal effectuated by the Royal Canadian Mounted Police (the "Government Institution") concerning the targeted access request designated as File No. A-2026-01933 / F281 (the "Access Request").³ It is respectfully submitted that the Government Institution has engaged in a deliberate pattern of administrative obfuscation. This includes the issuance of a facially void

processing notification
devoid of statutory
grounding, followed by
a complete cessation
of communication
upon being served with
a formal notice of their
statutory defect.II.

CHRONOLOGICAL
COMPUTATION OF
TIME AND FACTUAL
MATRIX4.To facilitate
an expeditious
investigatory
assessment by the
Commissioner, the
procedural
chronology—corroborated by the annexed
evidentiary exhibits—is
delineated
herein:Procedural
MilestoneStatutorily
Recognized
DateFactual
Corroboration and
Legal
ConsequenceTransmis
sion of RequestMay 5,
2026Formal Access
Request transmitted
with prescribed
statutory fee, seeking
discrete
GrapeCity/MESCIUS

Files uploaded

File name	File size (KB)
Complaint - RCMP - ATIA - GrapeCity Requested Records SIGNED.pdf	198.16

Access Request - ATIP - Grape City Mescius -
Requestor - KAM (BA JD CIM) - 5-May-2026 - 311.59
SIGNED.pdf

Canada Post Delivery - ATIA #2 - delivered
May 7 2026.pdf 294.28

Information Package 4810 998 24 48129169-
00 (4).pdf 328.53

ADULT-COMMON-INFORMATION-FORM-
WITH-HIGHLIGHTED-CHANGES - lcla.pdf 214.98

Gmail - Access to Information Act request A-
2026-01933 _ F281, Your File N_A, 90.12
Acknowledgment.pdf

TAB 17

FEDERAL COURT

B E T W E E N:

KEVIN A. MCLEAN

Applicant

and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, AND
STEPHANE BRISSON

Respondents

**SUPPLEMENTAL WRITTEN REPRESENTATIONS OF THE APPLICANT
FOR NOM #1 – PREDICATED UPON FURTHER FRESH EVIDENCE OF
TODAY’S DATE (JUNE 16, 2026)**

Table of Contents

SUPPLEMENTAL WRITTEN REPRESENTATIONS OF THE APPLICANT FOR NOM #1 –
PREDICATED UPON FURTHER FRESH EVIDENCE OF TODAY’S DATE (JUNE 16, 2026) 1

OVERVIEW AND STATEMENT OF FRESH FACTS 2

2.0 STATUTORY ANALYSIS AND CRYSTALLIZED DEEMED REFUSAL..... 3

2.1 Extinguishment of Administrative Discretion 3

3.0 REJECTION OF ADMINISTRATIVE RETRIEVAL EXCUSES 4

3.1 The Fallacy of the Retrieval Stage..... 4

4.0 THE PARALLEL RULE 305 AND RULE 318 DEFAULTS..... 6

4.1 Institutional Recalcitrance and the Doctrine of Spoliation 6

4.2 Systemic Spoliation by Design and Adverse Inferences..... 7

5.0 BASIS FOR IMMEDIATE EQUITABLE RELIEF 8

5.1 Mandamus and the Prevention of Fraud (further)..... 8

APPENDICES 11

APPENDIX #1	12
Appendix #2: Relief Sought IN THE NOM #1	12

OVERVIEW AND STATEMENT OF FRESH FACTS

1. The present written representations supplement (the “**Written Representations Supplement**”) is respectfully submitted for the immediate adjudication of the presiding motions judge of the Federal Court of Canada. It is advanced to formally introduce an absolute, self-defeating evidentiary admission, promulgated in writing by the respondents (the “**Respondents**”) on June 16, 2026 (see: Tab A, pages 9-10), which materialized a mere twenty-four hour antecedent to the scheduled disposition of this motion in writing (the “**Motion in Writing**”).
2. At precisely 7:58 a.m. on June 16, 2026, electronic correspondence was disseminated to the applicant (the “**Applicant**”) by Ms. Tina Beaudoin, functioning in her capacity as a Federal Team Leader within the access to information and privacy branch (the “**ATIP Branch**”) of the Royal Canadian Mounted Police (the “**RCMP**”). This correspondence pertained to the foundational statutory access file, explicitly designated as *Access to Information Act* Request A-2026-00761 / F339 (the “**ATIA Request**”) (see: Tab A, pages 9-10).
3. Within the aforementioned correspondence, which is forensically integrated into the appended documentary matrix, the Respondents explicitly formulated a profound misrepresentation of both fact and law, articulating: “*Kindly note that no extensions were taken on your file.*” (see: Tab A, page 10). Concurrently, it was confirmed that the

underlying infrastructure metadata, hexadecimal mainframe dumps, and cryptographic audit trails remain strictly unproduced and sequestered within an indefinitely suspended administrative retrieval stage (see: Motion Record, Tab 12, Sub-Tab A, pages 415-429 for the underlying request).

4. It is submitted through advanced syllogistic extrapolation that litigation fundamentally constitutes a truth-searching function, and such proceedings categorically cannot be conducted in the dark. In circumstances wherein the state apparatus actively conceals the foundational *acta* authorizing the deprivation of liberty, the Rule of Law itself is unquestionably on trial and placed directly at issue herein.
5. The legal controversies presented for adjudication significantly transcend the immediate *lis* existing between the respective parties. The issues are inherently of a general nature and of central importance to the legal system as a whole. They involve profound questions of practice and procedure implicating federal institutions governed under the *Access to Information Act* and the *Privacy Act*, while additionally testing the strict jurisdictional boundaries between various administrative tribunals as defined and interpreted under the *Federal Courts Act* and the *Federal Courts Rules*.

2.0 STATUTORY ANALYSIS AND CRYSTALLIZED DEEMED REFUSAL

2.1 EXTINGUISHMENT OF ADMINISTRATIVE DISCRETION

6. Through the formalization of the aforementioned admission, the Respondents have legally decapitated their own administrative positioning, thereby verifying the absolute, incurable crystallization of a statutory default under federal law. Pursuant to section 7 of the *Access to Information Act*, a federal institution is strictly bound by a mandatory, non-discretionary

public legal duty to furnish a final, substantive response within thirty days of the receipt of a valid requisition.

7. The objective factual record dictates that constructive and physical possession of the primary *ATIA Request*, accompanied by the statutorily prescribed financial instrument of five dollars, was crystallized by the Respondents on April 14, 2026 (see: Motion Record, Tab 12, Sub-Tab A, page 415). By strict operation of law, the non-discretionary statutory clock formally expired on May 14, 2026.
8. Under the governing jurisprudential framework established by the Federal Court of Appeal in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56, a government institution is completely stripped of all residual administrative processing latitude at the precise moment a statutory window expires absent the lawful execution of a formalized extension.
9. Insofar as the Respondents have explicitly admitted that no statutory extensions were effectuated pursuant to section 9 of the *Access to Information Act*, the file was automatically plunged into a state of deemed refusal on May 14, 2026, pursuant to subsection 10(3) of the legislation. Any subsequent assertion that the RCMP executed a lawful extension of time is forcefully refuted and categorized not merely as a curable irregularity, but as an absolute jurisdictional nullity.

3.0 REJECTION OF ADMINISTRATIVE RETRIEVAL EXCUSES

3.1 THE FALLACY OF THE RETRIEVAL STAGE

10. The self-serving postulation advanced by the Respondents, claiming that the file remains safely insulated within an ongoing “retrieval stage,” represents a catastrophic misapprehension of the statutory framework. An internal administrative backlog, systemic

lethargy, or mailroom delay possesses absolutely zero legal capacity to toll a crystallized statutory default.

11. Furthermore, the evidentiary record establishes that on April 23, 2026, the Respondents attempted to deploy an *ultra vires* clarification request targeting a personal information bank (the “**PIB**”) designated under code RCMP PPU 005 (see: Motion Record, Tab 12, Sub-Tab B, pages 430-441). As meticulously documented within the initial application, the Applicant's requisition explicitly targeted structural federal IT infrastructure metadata, mainframe transaction logs, and vector-collapse bug analysis reports—artifacts wholly distinct from standard personal data records (see: Motion Record, Tab 12, Sub-Tab A, pages 415-429).
12. The imposition of a clarification demand predicated upon an entirely irrelevant data category, utilized solely to hold a structural IT infrastructure search in abeyance, constitutes a profoundly bad-faith application of section 6 of the *Access to Information Act*. This maneuver is a recognized spoliation tactic, engineered deliberately to orchestrate delay and systematically circumvent judicial oversight. Justice delayed is unequivocally justice denied.
13. The assertion that an extension was necessitated due to an “unreasonable interference with the operations of the RCMP” is rendered entirely bereft of logic when measured against the operational realities of a federal institution commanding an annual budgetary allocation traversing seven billion dollars. The failure to conduct the requisite search is an action that is *ultra vires*, effectively vitiating the ability of the RCMP Commissioner to discharge his mandatory duties under section 8(2)(m) of the *Privacy Act* and the concomitant obligations under section 19 of the *Access to Information Act*.

4.0 THE PARALLEL RULE 305 AND RULE 318 DEFAULTS

4.1 INSTITUTIONAL RECALCITRANCE AND THE DOCTRINE OF SPOILIATION

14. The dynamic timeline of statutory default observed within the ATIP Branch perfectly mirrors the flagrant, institutional disregard for the procedural orders promulgated by this Honourable Court. The Respondents were perfectly served with the originating notice of application (the “**Notice of Application**”) on May 19, 2026 (see: Motion Record, Tab 16, pages 566-615). Pursuant to the strictures of *Rule 305* of the *Federal Courts Rules*, the Respondents were encumbered with an absolute duty to serve and file a notice of appearance (the “**Notice of Appearance**”) utilizing Form 305 within ten days (see: Motion Record, Tab 14, pages 502-525). The complete failure to execute this mandate constitutes a definitive waiver of their right to participate or receive notification of subsequent procedural advancements.

15. Concurrently, the Respondents have completely ignored the mandatory, non-discretionary twenty-day temporal requirement codified under *Rule 318(1)* to transmit the certified tribunal record (the “**CTR**”) to the Registry. No compliance has been filed, no records have been produced, and no formal written objections have been submitted pursuant to *Rule 318(2)*.

16. It is a fundamental tenet of administrative law that while the Federal Court of Canada lacks the jurisdiction to compel a formal appearance by a respondent, it possesses the unassailable, absolute jurisdiction to compel strict compliance with *Rule 318* of the *Federal Courts Rules*. This compulsory power operates entirely irrespective of the filing of a Notice of Appearance by any or all Respondents and applies strictly to the RCMP functioning as

a tribunal. One highly effective mechanism to resolve this institutional delinquency is to legally compel the RCMP Tribunal to transmit the CTR directly to the Registry, thereby ensuring its integration into the open court record pursuant to the initial request executed under *Rule 317* (see: Motion Record, Tab 15, pages 526-565).

17. By refusing to formally attorn to the jurisdiction of this litigation, while simultaneously sequestering the administrative records within the ATIP Branch under the fictitious guise of a “retrieval stage,” the Respondents are executing a highly coordinated procedural blockade. It is submitted that it is not a matter of the RCMP being unable to engage in the mandated searching, but rather that it is resolutely unwilling, driven by an institutional fear of opening a proverbial Pandora's box of systemic liabilities.

4.2 SYSTEMIC SPOILIATION BY DESIGN AND ADVERSE INFERENCES

18. The failure of the RCMP to provide any records across the *Privacy Act* request and both *Access to Information Act* requests supports a compelling legal inference of Systemic Spoliation by Design. The institution is actively attempting to immunize the institutional record from judicial scrutiny ahead of the scheduled proceedings.
19. In the context of active litigation under Court File Number T-2448-26, three critical adverse inferences emerge from this total operational shutdown:
 - **The Inference of Adverse Evidence:** Pursuant to the equitable doctrine of *omnia praesumuntur contra spoliatores* (all things are presumed against the destroyer of evidence), the Court is entitled to infer that the unproduced data contains information demonstrably damaging to the RCMP. By completely withholding native metadata, CPIC transaction logs, and hexadecimal dumps, the institution signals that the digital architecture would verify the Applicant's allegations of vector morphology collapse, commercial PDF manipulation, and the unauthorized alteration of sworn judicial instruments (see: Motion Record, Tab 6, Sub-Tab C, pages 124-130). When a party deliberately suppresses baseline technological

tracking records, the Court is entitled to infer that the unproduced evidence confirms the applicant's case.

- **The Inference of Coordinated Procedural Blockade:** The RCMP is withholding materials across multiple distinct statutory regimes simultaneously while failing to file a Form 305 Notice of Appearance or a Rule 318 Notice of Objection. This dynamic indicates that the ATIP Branch and institutional counsel are operating in tandem to execute a procedural blockade, denying the Applicant the source law artifacts needed to construct the evidentiary record and attempting to force the Federal Court to adjudicate the motion on a hollow record.
- **The Inference of Evisceration of the Statutory Right of Access:** The institution treats the statutory mandates of Subsection 2(1) and 2(2) of the *ATIA* not as binding public duties, but as optional administrative queues. The inescapable inference is that the institution has substituted its own internal administrative preferences for the rule of law, transforming their delay from a routine backlog into a bad-faith jurisdictional nullity.

20. Consequently, the Federal Court is highly entitled, and indeed strongly urged, to invoke these inferences. The overarching principles articulated by the Supreme Court of Canada in *MacDonald Estate v. Martin*, [1990] 3 SCR 1235 dictate that matters of such severe institutional conflict and potential bias are not subject to proof or disproof by mere analogy. Furthermore, as established in *McInerney v. MacDonald*, [1992] 2 SCR 138, the fundamental purpose of ensuring that individuals possess legislative rights to their own Personal Information is specifically designed to avert the opening of the floodgates of litigation, ensuring that aggrieved parties receive their data so they do not inadvertently advance lawsuits devoid of an evidentiary foundation.

5.0 BASIS FOR IMMEDIATE EQUITABLE RELIEF

5.1 MANDAMUS AND THE PREVENTION OF FRAUD (FURTHER)

21. Unilateral administrative silence is not a legally sustainable defense mechanism. Because this Motion in Writing proceeds entirely unopposed, and in light of the fresh written admissions generated on June 16, 2026, the legal standard, evaluated upon a balance of probabilities, weighs overwhelmingly in favor of the immediate issuance of prerogative

relief. A rigid distinction must be drawn between affirmative consent and the complete absence of opposition; no opposition must furnish the presiding motions judge with absolute comfort to grant the Draft Order, and the relief contained therein, in substantially the same form as requested.

22. The extraction of the requisitioned hexadecimal matrices and terminal metadata is a purely mechanical, technological imperative strictly mandated by the governing statutes. It involves absolutely no exercise of discretionary administrative judgment. The institutional conduct documented herein operates in direct contravention of the transparency principles elucidated in *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403, and *Lavigne*.
23. The Federal Court of Canada, in its capacity as a superintending equitable tribunal, can never countenance fraud upon the court, even in circumstances where the fraud was originally perpetrated within the jurisdiction of another provincial or municipal court. The RCMP is not merely inconveniencing the Federal Court; it is operating as if the law itself is entirely inconsequential.
24. It is profoundly unfortunate that the Canadian Rule of Law is being systematically trampled upon. A distinguishing, authoritative judicial decision is absolutely necessary to ensure that individuals who remit fees and formally request documents pursuant to the *Access to Information Act* can obtain access to vital records in a manner that facilitates reasonably informed choices within a functioning democratic society.
25. The Applicant respectfully requests that this Honourable Court execute the submitted Draft Order (see: Motion Record, Tab 3, pages 44-50), compelling absolute compliance with *Rule 318* within twenty-four hours, and granting immediate leave to initiate formal

contempt proceedings against individual and institutional state actors should this default persist.

All of which is respectfully submitted by the Applicant to the Federal Court of Canada (attention: presiding motions judge for the Applicant's NOM #1 to be heard and decided in writing on June 17 2026) on June 16, 2026

A handwritten signature in black ink, appearing to be 'K. McLean', with a stylized flourish at the end.

Mr. Kevin A. McLean (BA, JD, CIM)
Applicant
Moving Party
Pro Se
Email: mclean@searchandseizure.ca

APPENDICES

APPENDIX #1

Statutes and Regulations

1. *Access to Information Act*, RSC 1985, c A-1
2. *Privacy Act*, RSC 1985, c P-21
3. *Federal Courts Act*, RSC 1985, c F-7
4. *Federal Courts Rules*, SOR/98-106

Jurisprudence

5. *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56
6. *MacDonald Estate v. Martin*, [1990] 3 SCR 1235
7. *McInerney v. MacDonald*, [1992] 2 SCR 138
8. *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403
9. *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53

APPENDIX #2: RELIEF SOUGHT IN THE NOM #1

RELIEF SOUGHT**THE MOTION IS FOR the following precise relief sought:****Procedural Relief**

- **Abridgment of Time:** An Order that any timelines required to be abridged are so abridged pursuant to *Rule 8* of the *Federal Courts Rules*, on a nunc pro tunc basis where applicable;
- **Dispensation of Compliance:** An Order varying or dispensing with strict compliance of any rule pursuant to *Rule 55* of the *Federal Courts Rules*, on a nunc pro tunc basis where applicable;
- **Deeming of Filing:** An Order deeming all documents submitted for filing on the day in which they were submitted to the Registry, pursuant to *Rule 72.1* of the *Federal Courts Rules*;
- **Dispensation of Proof of Service:** A Declaration and Order that the Applicant is not required to provide further proof of service upon the Respondents pursuant to *Rule 73*, granted nunc pro tunc, given the Respondents' failure to file a Notice of Appearance (Form 305).

Declaratory and Substantive Relief

- **Declaration of Contravention:** A Declaration that the Royal Canadian Mounted Police (the “RCMP Tribunal”) has contravened its mandatory statutory and procedural duties pursuant to *Rule 318* of the *Federal Courts Rules*;
- **Declaration of Disobedience:** A Declaration that the RCMP Tribunal has disobeyed a lawful process of this Honourable Court, acted in a manner that interferes with the orderly administration of justice, and impaired the authority and dignity of the Court;
- **Mandatory Order for Compliance:** An Order compelling the RCMP Tribunal to fully comply with its duties pursuant to *Rule 318* of the *Federal Courts Rules* by transmitting the complete Certified Tribunal Record to the Registry and the Applicant within twenty-four (24) hours of the issuance of this Order;

- **Imposition of Conditions:** The imposition of such terms, conditions, and directions as this Honourable Court considers just to ensure immediate compliance, pursuant to *Rule 53(1)* of the *Federal Courts Rules*.

Leave Relating to Potential Contempt

- **Leave for Contempt Proceedings:** An Order granting the Applicant leave to bring a motion for contempt against the RCMP Tribunal, and any specific persons facilitating the intentional breach of the orders herein, pursuant to *Rule 50(1)(d)* and *Rules 466* and *467* of the *Federal Courts Rules*.

Cross-Jurisdictional Enforcement Relief

- **Authorization for Enforcement:** An Order declaring that the Applicant is at liberty, authorized, and empowered to apply to any court, tribunal, regulatory, or administrative body, wherever located, for the recognition of this Order, and for assistance in carrying out its terms and the terms of any other order issued in these proceedings.

Costs and Residual Relief

- **Costs:** Costs of this motion in favour of the Applicant on a full indemnity basis, to be assessed after this Honourable Court has rendered judgment herein;
- **Residual Relief:** Such further and other orders of an equitable nature, predicated upon the Federal Court's equitable jurisdiction, that are fair, just, and necessary to restore the status quo ante.

- Nothing past this Line -



Mr. Kevin McLean <mcleansettlement@gmail.com>

Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

Mr. Kevin McLean <mcleansettlement@gmail.com>

Tue, Jun 16, 2026 at 10:17 AM

To: "Beaudoin, Tina (RCMP/GRC)" <tina.beaudoin@rcmp-grc.gc.ca>, Bryan.Larkin@rcmp-grc.gc.ca, "Brisson, Stéphane (RCMP/GRC)" <stephane.brisson@rcmp-grc.gc.ca>, "Ball, Jeff (RCMP/GRC)" <Jeff.ball@rcmp-grc.gc.ca>, "Simpson, Melissa (RCMP/GRC)" <melissa.simpson@rcmp-grc.gc.ca>

Date: June 16, 2026

Creation method: Dictated with voice recognition software (reserve rights to amend any errors involving syntax, spelling, grammar or incorrect double negatives but the substance will remain the same)

TO:

RCMP ATIP Branch

Email: ATIP / AIPRP ATIP-AIPRP@rcmp-grc.gc.ca;

Kind attention:

Beaudoin, Tina (RCMP/GRC) tina.beaudoin@rcmp-grc.gc.caLarkin, Bryan (RCMP/GRC) Bryan.Larkin@rcmp-grc.gc.ca;Brisson, Stéphane (RCMP/GRC) stephane.brisson@rcmp-grc.gc.ca;Simpson, Melissa (RCMP/GRC) melissa.simpson@rcmp-grc.gc.ca

And others

SUBJECT: RE: ACCESS TO INFORMATION ACT REQUEST A-2026-00761 / F339 – RESPONSE TO MS. TINA BEAUDOIN’S EMAIL OF TODAY’S (JUNE 16, 2026) DATE

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

INTRODUCTION AND PRELIMINARY OBSERVATIONS***A. INTEGRATION OF THE FACTUAL RECORD***

1. Receipt is hereby formally acknowledged concerning the electronic correspondence disseminated by the government institution (the “**Government Institution**” or “Institution”) on June 16, 2026. The **Institutional** postulation that the substantive access to information request (the “**Access To**

633

Information Request”) which was delivered to the RCMP on April 14, 2026, bearing file designation A-2026-00761, remains situated within a routine retrieval stage is **categorically repudiated** as being entirely bereft of legal foundation.

2. I adopt the definitions from previous correspondence for ease of reference.

3. I refer to myself in the third person for ease of reference and convenience, and for situational and context purposes.

4. I understand that Ms. Beaudoin is a federal team leader with ATIP since March 2018.

5. The aforementioned correspondence explicitly concedes that no statutory extensions were effectuated upon the operative file. This is a false statement on a de facto and de jure basis. While no legal statutory extensions were taken under the applicable section of *ATIA*, there have been vague references to 60 day time extensions to make a complaint. The time to make a complaint is at the time of the purported or alleged extension.

6. Through the formalization of this specific admission, the absolute crystallization of a statutory default on the part of the Royal Canadian Mounted Police is irrevocably confirmed. The recipients are hereby formally directed to govern subsequent actions in strict adherence to the delineated legal realities.

2.0 CHRONOLOGICAL MATRIX AND STATUTORY DEFAULT

B. TABULAR REPRESENTATION OF THE ACTA

3. The following tabular representation meticulously delineates the objective procedural timeline, fundamentally eviscerating any **Institutional** claim to ongoing administrative processing latitude:

Date	Procedural Event	Statutory Implication
April 14, 2026	Constructive possession of the Access To Information Request and the statutorily prescribed financial instrument of five dollars.	Immediate commencement of the non-discretionary thirty-day statutory processing limitation.
April 23, 2026	Institutional demand for clarification and unlawful threat of file closure.	An <i>ultra vires</i> mechanism engineered to orchestrate spoliation by delay and a nullity <i>ab initio</i> .
May 4, 2026	Arbitrary Institutional deadline demanding clarification regarding the physical location of personal information bank (the “ Personal Information Bank ”) RCMP PPU 005.	A fundamentally impermissible statutory interpretation designed to subvert the paramount right of access.
May 14,	Expiration of the paramount statutory limitation period.	Crystallization of a deemed refusal under <i>Subsection 10(3)</i> of the <i>Access</i>

634

2026

to Information Act.

June 15, 2026	Dissemination of the final legal notice of default.	Integration of the deemed refusal as compounding evidence of bad faith into active litigation.
June 16, 2026	Institutional admission that the file remains in the retrieval stage and no extensions were taken.	Absolute forfeiture of residual administrative discretion.
June 17, 2026	Impending interlocutory proceeding in the Federal Court of Canada.	Adjudication of the failure to adhere to the non-discretionary mandate of <i>Rule 318</i> of the <i>Federal Courts Rules</i> .

3.0 ALLEGATIONS OF FORGERY AND THE DOCTRINE OF SPOILIATION

C. CRYPTOGRAPHIC PROVENANCE AND PUBLIC INTEREST DISCLOSURE

4. The foundational requisition was explicitly formulated to compel the extraction or disclosure of unredacted audit trails, transaction ledgers inherent to the Canadian police information centre (the “**Canadian Police Information Centre**”), and systemic governance manuals. The profound necessity of this overarching public interest disclosure is predicated upon severe, substantiated allegations of warrant forgery perpetrated via portable document format (the “**Portable Document Format**”) manipulation software.

5. The central operational matrix of the Canadian criminal justice paradigm is entirely predicated upon the unbroken chain of custody inherent to sworn judicial instruments. When the cryptographic provenance of a formally sworn document is deliberately severed by state actors deploying commercial manipulation software to falsify jurisdictional realities, the resultant documentation ceases to operate as a lawful authorization. It devolves into a mere instrument of arbitrary coercion.

6. The overarching democratic imperative demands the preservation of the *status quo ante*, compelling rigorous adherence to the supreme governing principles established in *Landreville v. Town of Boucherville*, [1978] 2 SCR 801 (the “*Landreville Decision*”) and *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403 (the “*Dagg Decision*”), which dictate that fraud and synthetic document fabrication systematically unravel everything they touch.

4.0 CRYSTALLIZATION OF DEEMED REFUSAL AND JURISDICTIONAL NULLITY

635**D. THE ABSOLUTE EXTINGUISHMENT OF ADMINISTRATIVE DISCRETION**

7. Insofar as a temporal duration significantly exceeding sixty days has elapsed since the crystallization of constructive possession, and noting the explicit **Institutional** admission that no legally valid statutory abeyance or extension was properly effectuated, the Government Institution has inexorably descended into an automatic state of deemed refusal.

8. Such a transgression of paramount legislative dictates cannot be artificially diminished as a mere procedural irregularity; rather, owing to its direct contravention of the overarching parliamentary statute, it manifests as an absolute jurisdictional nullity *ab initio*. By strict operation of law, the effectuation of a deemed refusal completely eradicates any residual administrative discretion previously vested within the administrative apparatus.

5.0 ACTIVE FEDERAL COURT ENFORCEMENT AND MANDAMUS**E. THE INTERLOCUTORY PROCEEDING AND RULE 318**

9. It must be articulated with unequivocal precision that the present statutory default is not tethered to a passive administrative queue. This profound **Institutional** default has been concurrently integrated as compounding *prima facie* evidentiary proof of bad faith directly into the active, unmitigated litigation presently situated before the Federal Court of Canada, bearing the designation of **Court File Number T-2448-26**.

10. The structural and procedural defaults perpetrated by the respondents—encompassing the total, inexcusable failure to adhere to the non-discretionary imperative codified within *Rule 318* of the *Federal Courts Rules*—shall be forcefully and vigorously prosecuted during the impending interlocutory proceeding on June 17, 2026.

F. THE PREROGATIVE WRIT OF MANDAMUS

11. It is advanced through complex syllogistic reasoning that the balance of convenience weighs overwhelmingly and absolutely in favor of the issuance of a prerogative writ of mandamus. A clear, positive, and non-discretionary public legal duty is affixed to the **Government Institution**; said executory duty is owed explicitly to the applicant; a formal demand has been effectuated *in limine*; and an absolute constructive refusal has materialized *ipso facto* through the expiration of strict temporal parameters.

12. While it is a recognized jurisprudential precept that mandamus cannot dictate a specific, discretionary substantive outcome, it possesses the absolute, unyielding authority to compel the performance of a specific, ministerial, and executory duty. The extraction of the requisitioned hexadecimal and routing metadata ledgers is not an exercise of administrative judgment, but rather a purely mechanical, technological imperative mandated by the statute. Any **Institutional** refusal to execute this technological extraction transcends a mere irregularity and constitutes a jurisdictional nullity.

636

13. The Respondents' failure to serve and file a **Form 305 Notice of Appearance** does not block the operation of Rule 317 and Rule 318 under the Federal Courts Rules. While the Federal Courts Rules and ATIA are distinct in the former being a regulation and the latter being a statute, the analogy, consonance or parallel can be drawn involving the similar fact evidence of failing to comply with "Source Laws" or "Enactments" in an obstructionist manner.
14. Our relations herein are one of an access partnership and the RCMP ATIP Branch is failing not only me but the public.
15. By failing to step into the litigation formally, they are attempting to lock the court record, matching the exact "spoliation by delay" tactics they are executing within the ATIP branch. The Applicant will draw the same to the attention of the FCC with due dispatch.

6.0 STATUTORY PURPOSE AND THE CONTRAVENTION OF LEGISLATIVE INTENT

G. The Paramountcy of Accountability and Transparency

13. The foundational architecture of the *Access to Information Act* is explicitly codified within *Subsection 2(1)*, which unequivocally mandates the enhancement of the accountability and transparency of federal institutions. It is submitted that the deliberate obfuscation of metadata and the persistent suppression of chronological transaction logs fundamentally subvert this paramount statutory objective, a legislative framework enacted specifically to promote an open and democratic society and to enable robust, unimpeded public debate concerning the conduct of state institutions.
14. This democratic imperative is further operationalized by *Subsection 2(2)(a)* of the *Access to Information Act*, which enshrines a positive, quasi-constitutional right of access to records situated under the control of the Government Institution. The supreme governing principle dictates that state-held information must be made intrinsically available to the public sphere. Concomitantly, any requisite exceptions to this overarching right of access are legally compelled to be construed as stringently limited and highly specific. The **Institutional** deployment of manufactured administrative ambiguities and unenumerated extensions to forestall disclosure manifests as a direct contravention of this principle of narrow interpretation, effectively shielding **Institutional** conduct from the independent review mandated by the legislature.

H. Proactive Disclosure and Syllogistic Extrapolation

15. Moreover, in contemplation of *Subsection 2(2)(b)* of the *Access to Information Act*, which establishes stringent requirements for the proactive publication of information, the systemic failure to surrender the requisitioned audit trails elucidates a profound departure from the doctrine of proactive transparency. Through the application of complex syllogistic reasoning, it becomes intrinsically self-evident that the continued obstruction of these cryptographic matrices transcends mere procedural irregularity; it constitutes an absolute jurisdictional nullity and a substantive evisceration of the fundamental democratic oversight expressly envisioned by the Parliament of Canada.

16. It is formally recorded that the *ultra vires* delays engineered by the ATIP Branch necessitated the institution of a formal investigative complaint before the office of the information commissioner (the “**Office of the Information Commissioner**”), distinct from the Office of the Privacy Commission, on April 24, 2026. This complaint meticulously delineated the deliberate **Institutional** subversion of binding statutory timeframes through the issuance of an extra-statutory demand for clarification, coupled with an unlawful threat to summarily terminate the processing of the requisition.
17. The physical package encompassing the formal requisition, inclusive of the statutorily prescribed application fee in the form of a certified financial instrument, was transmitted via Canada Post Xpresspost and objectively delivered on **April 14, 2026**. Internal bureaucratic inefficiencies cannot be weaponized by the state to unlawfully abridge an applicant’s statutory timelines or retrospectively alter the legally operative date of receipt.

J. THE SUBSTANTIVE NULLITY OF THE SECTION 6 “CLARIFICATION” DEMAND

18. The **Institutional** attempt to invoke *Section 6* of the *Access to Information Act*—predicated upon a feigned inability to comprehend a requisition drafted with unparalleled forensic precision—was formally denounced as an absolute statutory nullity. The requisition explicitly targeted specific algorithms, originating agency identifiers, media access control addresses, and hexadecimal mainframe dumps. The assertion that an experienced employee fails to understand standard enterprise-level IT nomenclature is an administrative fiction designed solely to orchestrate spoliation by delay.
19. The initial access request under *ATIA*, which I have defined through as “*ATIA* Request #1” explicitly targeted infrastructure metadata and systemic mainframe transaction logs, which are not personal information bank records. Demanding a clarification based on an irrelevant personal data category to delay a structural IT infrastructure search is a bad-faith application of Section 6 of the Act.

8.0 APPENDIX A: MANDATORY PRODUCTION FORMATS FOR CPIC RECORDS

K. THE STRICT PRESERVATION OF NATIVE DIGITAL ARCHITECTURE

19. To preemptively forestall any subsequent, disingenuous **Institutional** assertions of technical incomprehension regarding the specific database artifacts requisitioned, the following matrix delineates the exact, immutable morphology of the requested categories of CPIC records. Any substantive deviation from these rigorous, native data structures—specifically the unauthorized substitution with homogenized, graphical presentation summaries—shall be construed *prima facie* as a deliberate, sanctionable spoliation of electronic records.

Item No.	Requisition Category	Contextual Justification and Legal Imperatives	Mandatory Format of Production (Native Architecture)

638

1.	Investigative Data Bank Audit Trails	The graphical interface accessible to a patrol officer is subjected to algorithmic filtering. Only the immutable systemic ledgers housed deep within PPU 005—capturing the precise chronological sequence of ADD, MODIFY, CLEAR, and CANCEL commands—can definitively expose the temporal trajectory of state-actor malfeasance.	Native tabular database extractions (e.g., CSV, SQL output) derived directly from the mainframe transaction ledger, strictly preserved without redaction of operational syntax or timestamp modification.
2.	Hexadecimal Mainframe Dumps	This mathematical data is strictly required to bypass the visual homogenization inherent to the standard graphical user interface. Only the uninterpreted binary and hexadecimal records—complete with exact cryptographic memory offsets and decoded text translations—can provide the absolute mathematical certitude required to prove vector morphology collapse.	Raw, continuous hexadecimal and binary outputs (e.g., .HEX files or raw binary dumps), purposely bypassing the visual homogenization inherent to the graphical user interface.
3.	Hardware and Terminal Metadata	This data is critical to irrevocably establishing the physical and geographical locus of the data entry, directly invoking the foundational legal maxim <i>nemo dat quod non habet</i> (no one gives what they do not have).	Extracted network session logs explicitly delineating ORI routing codes, MAC addresses, and IP assignments associated with the session token.
4.	Inter-Agency Communication Logs	A systemic error of this profound magnitude does not exist in a vacuum; a highly documented administrative paper trail of IT professionals attempting to reconcile the corrupted digital artifacts is inevitably created, especially regarding the absolute failure of the mandatory matching protocol.	Internal IT troubleshooting ticket exports (e.g., native ServiceNow, Jira data outputs) and raw systemic error alerts generated automatically by the CPIC input gateway parsing engine.

639

5.	PDF Flattening and Vector Analysis Reports	Forensic analysis confirms enterprise-level developer software was utilized with the specific <i>mens rea</i> to unlawfully flatten the document, forcefully eradicate the transparent electronic image signature, and algorithmically disfigure the underlying text to bypass standard criminal intake procedures.	Native system alerts, proprietary software ingestion logs, and raw vector diagnostic exports demonstrating morphological collapse.

9.0 JURISPRUDENTIAL FRAMEWORK: STATUTORY DEADLINES AND DEEMED REFUSALS

L. THE NON-DISCRETIONARY THIRTY-DAY MANDATE

20. It is a well-established jurisprudential precept that the strict temporal limitations imposed upon government institutions under the *Access to Information Act* are foundational to the operationalization of democratic transparency. Pursuant to *Section 7* of the *Access to Information Act*, a non-discretionary public legal duty is affixed to the Government Institution to render written notice regarding the requested records within thirty days.
21. The jurisprudence articulated in *Rundel v. Canada*, *Coderre v. Canada*, and *Teal Cedar Products Ltd. v. Canada* unequivocally predicates judicial intervention upon the **Institutional** failure to strictly adhere to this baseline statutory deadline. A contravention of this temporal mandate is decidedly not a mere procedural irregularity; owing to its evisceration of the citizen's right to prompt access, it is an absolute jurisdictional nullity.

M. The Doctrine of Deemed Refusal

22. Upon the expiration of the initial thirty-day limitation period, absent a procedurally valid and properly enumerated extension, the institution descends automatically into a state of deemed refusal, codified within *Subsection 10(3)* of the *Access to Information Act*.
23. As authoritatively established by the Federal Court of Appeal in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56, and further elucidated in *Iris Technologies Inc. v. Canada*, the expiration of this deadline without a legally operative extension instantaneously vests the applicant with the absolute right to seek extraordinary **equitable remedies**.
24. It is trite that the relief sought in my FCC Application of May 15, 2026, seeks various equitable remedies including what were known as ancient prerogative writs like mandamus and prohibition.
25. The failure to produce the Records operates as a continuous statutory breach, thereby empowering the reviewing courts to issue a prerogative writ of mandamus to compel executory performance.
26. Under the *Minister of National Defence* FCA framework, once a 30-day timeline expires without a formal *Section 9* extension, the institution is stripped of all processing latitude. A self-serving

640

administrative claim that a file is in a “retrieval stage” cannot legally toll a crystallized statutory default. Again, the reference to another 60 days for a complaint to be exercised is not founded in any “Source Law” or jurisprudence. If you feel that the Applicant is incorrect, kindly cite some authority in this regard.

27. As such, this document will be relied upon for lawful purposes with notice.

N. Judicial Scrutiny of Unenumerated Extensions

24. Furthermore, as codified in *Biogénie Canada Inc. v. Canada*, the reviewing courts apply exacting scrutiny to determine whether an **Institutional** attempt to artificially toll the foundational thirty-day window is genuinely supported by objective evidentiary realities. Extra-statutory delays, manufactured administrative ambiguities, or unenumerated extensions are invariably classified as *ultra vires* actions, thereby rendering the subsequent withholding of information a fundamentally impermissible exercise of state authority.

10.0 FINAL CONCLUSION AND RESERVATION OF RIGHTS

O. Comprehensive Preservation of Equitable Entitlements

25. The Government Institution is strictly prohibited from preemptively conflating the anticipated application of an exemption with the primary duty to conduct the mandated digital extraction. All rights, privileges, and remedies, whether existing in fact, at common law, or in equity, are hereby comprehensively and irrevocably reserved.

26. Govern yourselves accordingly.

Respectfully submitted,

/s/Mr. Kevin A. McLean (BA, JD, CIM)

Mr. Kevin A. McLean (BA, JD, CIM)
Chartered Investment Manager

On Tue, Jun 16, 2026 at 7:47 AM Beaudoin, Tina (RCMP/GRC) <tina.beaudoin@rcmp-grc.gc.ca> wrote:

Good morning,

641

I am writing to provide a status update further to your recent inquiry.

Your request is currently in the retrieval stage, and efforts are ongoing to identify and collect all records responsive to your request. Kindly note that no extensions were taken on your file. Rest assured that your request continues to be actively processed, and a response will be issued once all required steps have been completed.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada

30 Victoria Street, 7th Floor

Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:

<https://www.oicci.gc.ca/en/submitting-complaint>

We appreciate your patience and understanding in this matter.

Tina Beaudoin

From: Mr. Kevin McLean <mcleansettlement@gmail.com>

Sent: June 15, 2026 1:54 AM

To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>; Simpson, Melissa (RCMP/GRC) <Melissa.Simpson@rcmp-grc.gc.ca>; Brisson, Stéphane (RCMP/GRC) <Stephane.Brisson@rcmp-grc.gc.ca>; Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>; Mirsky, Tanya (RCMP/GRC) <Tanya.Mirsky@rcmp-grc.gc.ca>; Larkin, Bryan (RCMP/GRC) <Bryan.Larkin@rcmp-grc.gc.ca>

Subject: Re: Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

Date: June 15, 2026

**SUBJECT: IMMEDIATE LEGAL NOTICE: ATIA REQUEST A-2026-00761 / F339 —
DEEMED REFUSAL UNDER LAW AND URGENT STRATEGIC NOTICE OF
PENDING FEDERAL COURT ENFORCEMENT (COURT FILE NO. T-2448-26)**

642***DELIVERY METHOD:***

Via Electronic Transmission & Immediate Record Logging into Federal Court File T-2448-26

TO:

- **Mr. Bryan Larkin**, Acting Commissioner, Royal Canadian Mounted Police (Bryan.Larkin@rcmp-grc.gc.ca)
- **Mr. Stéphane Brisson**, Chief Privacy Officer and Director General, ATIP Branch (stephane.brisson@rcmp-grc.gc.ca)
- **Ms. Melissa Simpson**, Access to Information and Privacy Branch (melissa.simpson@rcmp-grc.gc.ca)
- Ms. Tanya Mirsky;
- Mr. Jeff Ball
- **Central ATIP Intake Branch**, Royal Canadian Mounted Police (ATIP-AIPRP@rcmp-grc.gc.ca)

REFERENCE: Formal Requisition under the Access to Information Act (*ATIA*) — File A-2026-00761 / F339 (unlike the botching on the Privacy Act request referencing "2025" (sic))

CONCOMITANT JUDICIAL PROCEEDING: Federal Court of Canada, Court File Number: T-2448-26

UPCOMING MOTION HEARING: June 17, 2026 (Motion Number One)

UPCOMING HEARING ON THE MERITS: June 29 OR 30, 2026 (Hearing for Requisition) (nota bene: prior to the summer recess when general sittings of the FCC are less abundant)

Dear Acting Commissioner Ms. Larkin, Chief Privacy Officer Monsieur Brisson, Ms. Mirsky, Mr. Ball and Ms. Simpson,

643

1. This correspondence serves as an unyielding, final legal notice identifying the total statutory default and crystallization of a Deemed Refusal by the Royal Canadian Mounted Police (RCMP) as of today, **June 15, 2026**. This notice links the ongoing administrative evasions of the RCMP ATIP Branch directly into the active, unmitigated litigation currently pending before the Federal Court of Canada in **Court File Number: T-2448-26** (Motion Rec... p. 1).
2. As you know, this *ATIA* request has been outstanding since April 14, 2026, but to assist Acting Commissioner Mr. Larkin, and the response by Ms. Simpson on April 28, 2026, was not compliant with *ATIA* in terms of what appears to be an arbitrary, unlawful and unknown to the Parliamentary statute in *ATIA* purported extension of time
3. To ensure that any reviewing body fully grasps the structural gravity of the records being withheld, the depth of the seven targeted technical classifications is detailed below. These items represent the inescapable operational footprint of the CPIC database (p. 22):

INVESTIGATIVE DATA BANK AUDIT TRAILS (RCMP PPU 005):

- a. Restricted to the critical temporal epoch of **September 22 to October 4, 2024** (p. 3). Frontline Graphical User Interfaces (GUIs) show only contemporaneous operational filtering (pp. 3, 21). Only the deep, immutable ledger captures the exact chronological sequence of ADD, MODIFY, CLEAR, and CANCEL commands, exposing when a state actor sought to excise data to mask an unlawful arrest (p. 3).

HEXADECIMAL MAINFRAME DUMPS:

- b. The raw binary logs associated with the target warrant (p. 3). The presentation layer of a standard user terminal can be disfigured to display a facially valid warrant (p. 4). Only uninterpreted hexadecimal dumps reveal cryptographic memory offsets and EBCDIC decoded translations, proving the exact moment a document's morphology collapsed (p. 4).

HARDWARE AND TERMINAL METADATA:

- c. The internal ORI mappings, Media Access Control (MAC) addresses, and hardware IP pathways used during the target sessions (p. 4). Invoking *nemo dat quod*

644

non habet, if a document supposedly authorized by a Superior Court Chief Justice was actually inputted from a municipal police division's back-office terminal, the ORI codes will incontrovertibly expose the jurisdictional nullity (p. 4).

INTER-AGENCY COMMUNICATION LOGS:

d. All internal emails, system alerts, and IT troubleshooting tickets shared between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch (p. 4). This explicitly isolates the communications regarding the catastrophic failure of the mandatory "Matching Protocol" during the ingestion of corrupted judicial initials (p. 4).

PDF FLATTENING AND VECTOR ANALYSIS REPORTS:

e. All system logs concerning OCR interpretation failures or "whitespace bugs" caused by the deployment of the GrapeCity Documents PDF suite (version 6.0.2.0, bug DOC-6507) (p. 5). This software was weaponized with explicit *mens rea* to violently flatten a document, erase the transparent electronic signature of Chief Justice Geoffrey B. Morawetz, and superimpose a civilian clerk's digital certificate as a visual smokescreen (p. 5).

OFFLINE HISTORICAL SEARCH RESULTS:

f. The unredacted results of the specialist search into the Investigative Data Bank archives (p. 5). This is required to pierce the chronological impossibility of an arrest executed on October 2, 2024, followed by an immediate provincial system expungement on October 3, 2024, alongside retaliatory cybersecurity blocking via a 403 Forbidden Error (p. 5).

SYSTEM GOVERNANCE MANUALS:

g. Unredacted copies of the CPIC Reference Manual and Memorandums of Understanding governing the "Judicial Firewall" (p. 5). This evidence is vital to demonstrating exactly how the mandatory "Air Gap" separating the independent judiciary from law enforcement entry teams was compromised (p. 5).

645

4. I draw your attention to section 9 of the *ATIA* which states:

“Extension of time limits

9 (1) The head of a government institution may extend the time limit set out in section 7 or subsection 8(1) in respect of a request under this Part for a reasonable period of time, having regard to the circumstances, if

(a) the request is for a large number of records or necessitates a search through a large number of records and meeting the original time limit would unreasonably interfere with the operations of the government institution,

(b) consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit, or

(c) notice of the request is given pursuant to subsection 27(1)

by giving notice of the extension and, in the circumstances set out in paragraph (a) or (b), the length of the extension, to the person who made the request within thirty days after the request is received, which notice shall contain a statement that the person has a right to make a complaint to the Information Commissioner about the extension.

Notice of extension to Information Commissioner

(2) Where the head of a government institution extends a time limit under subsection (1) for more than thirty days, the head of the institution shall give notice of the extension to the Information Commissioner at the same time as notice is given under subsection (1).”

5. While section 9 of the *ATIA* is distinct in some respects from section 15 of the *Privacy Act*, the question arises based upon the Ms. Simpson email if you do not comply with providing access by tomorrow because it would exceed more than 30 days as to whether you have notified the Commissioner. If you do not do so and do not provide full, complete and lawful disclosure of the requested Records, I will notify if the Commissioner unless you represent to me that you have done so with a copy of said letter on a forthwith basis.

6. For Ms. Simpson’s edification, the time limit of extension commences when the access request is received, which was April 14, 2026 so the 60 days would have commenced, if valid which it was not on April 14, 2026, and with 31 days in May 2026,

646

it would have been on **June 13, 2026**, but that was a Saturday so one must expect forthwith production, access and disclosure tomorrow morning.

7. Moreover, since the notice required to the Commissioner under ss. 9(2) of the *ATIA* would have been required at the time given and not at the time of receipt of the notice as Ms. Simpson would have it (see: Appendix).

**FINAL EXPIRATION OF THE STATUTORY CONTINUUM AND NOTICE OF
DEEMED REFUSAL**

8. The final, non-negotiable statutory window for the RCMP to deliver complete, unredacted access to the architectural metadata governing the Canadian Police Information Centre (CPIC) database has officially closed today, June 15, 2026. While I have continuously rejected your branch's procedurally defective attempts to use Section 6 of the *ATIA* to feign a systemic inability to comprehend basic database arrays, your administrative processing latitude is now entirely exhausted.

9. Because no responsive records, phased disclosures, or rolling extractions have been delivered by the close of business on this date, the RCMP is in a state of absolute statutory default. Pursuant to Section 10(3) of the *ATIA*, this default operationalizes an absolute **Deemed Refusal**. By operation of law, this text completely strips the head of the institution of any remaining administrative discretion or processing flexibility over this file.

**IMMEDIATE INTEGRATION INTO ACTIVE FEDERAL COURT PROCEEDING T-
2448-26**

10. Let there be no ambiguity: this default will not be deferred to external regulatory complaint structures. It is being injected directly into the active litigation before the Federal Court of Canada (Motion Rec... p. 1). As documented in the attached **Motion Record filed on June 10, 2026**, the Respondents are already in profound procedural default for failing to serve and file Form 305 Notices of Appearance within the mandatory 10-day window (Motion Rec... pp. 1, 26). You are explicitly reminded that under the strict terms of Form 301, your failure to oppose this application means judgment may be rendered in your absence and without further notice (Motion Rec... p. 1).

11. The ongoing refusal to search for and extract the raw hexadecimal mainframe logs and Personal Information Bank (PIB) RCMP PPU 005 audit trails is a continuation of

647

the exact institutional recalcitrance detailed in my pending motion (Motion Rec... pp. 1, 14). This statutory default will serve as immediate, compounding evidence of bad faith and a total failure to perform public legal duties (Motion Rec... pp. 31-32).

**THE NON-DISCRETIONARY MANDATE OF RULE 318 AND THE UPCOMING
JUNE 17, 2026 MOTION**

12. Your attention is directed to **Notice of Motion Number One**, which is formally scheduled to be heard and decided by the Federal Court on **Wednesday, June 17, 2026, at 9:30 a.m.** (Motion Rec... p. 24). This motion proceeds entirely unopposed due to your structural default (Motion Rec... pp. 2, 20).

13. The relief sought on June 17, 2026, focuses on the RCMP's flagrant contravention of its mandatory duties under **Rule 318 of the Federal Courts Rules** (Motion Rec... pp. 1, 25). Under Rule 318(1), the tribunal has no discretion: it *shall* transmit a certified copy of the requested material to the Registry within 20 days (Motion Rec... p. 2). You have failed to comply, failed to file a formal objection, and instead elected to remain silent (Motion Rec... pp. 40-41). This Court will be forcefully asked to:

- a. Issue a **Mandatory Order** compelling the RCMP Tribunal to fully comply with Rule 318 by transmitting the complete Certified Tribunal Record within twenty-four (24) hours of the order (Motion Rec... p. 25);
- b. Grant the Applicant explicit leave to bring immediate **Contempt Proceedings** against the specific institutional and individual actors facilitating this intentional breach (Motion Rec... p. 25).

14. Any such failure to comply with the *ATIA*, having failed to even have conducted a search in the *Privacy Act* request of myself from early March 2026, along with having failed to have complied with my second *ATIA* request of May 7, 2026, will be further evidence in support of some or all of the above and contained in the Motion Record #1.

15. I can also confirm that I have paid the "Requisition for Hearing – Application" as of Friday, June 12, 2026, which is to be set for June 29 or 30, 2026.

**JUDICIAL ENFORCEMENT OF SECTION 8(2)(M) AND SECTION 19 AT THE
JUNE 29/30, 2026 HEARING**

648

16. The crystallization of today's Deemed Refusal provides the final evidentiary bridge required for the upcoming **Hearing for Requisition scheduled for June 29 and 30, 2026**. At this upcoming hearing, the Federal Court will exercise its full superintending and equitable jurisdiction to adjudicate the core failures that your branch has desperately sought to conceal (Motion Rec... pp. 25, 32). Specifically, the court will directly enforce:

- a. **The Mandatory Discretion Under Section 8(2)(m) of the *Privacy Act*:** The total failure of the RCMP Commissioner to turn his mind to or exercise his statutory duty to consider the public interest override (Motion Rec... pp. 26, 31).
- b. **The Application of Section 19 of the *ATIA*:** Piercing the institutional stonewalling regarding purely professional metadata—such as Originating Agency Identifier (ORI) mapping, MAC addresses, and EBCDIC decoded text translations (Motion Rec... pp. 3, 14).

17. The depth of the evidence now filed in Court File No. T-2448-26 proves that the underlying documents—including the disfigured Ontario “Information Package” bearing commercial GrapeCity Software version 6.0.2.0 metadata—are absolute jurisdictional nullities *ab initio* (Motion Rec... pp. 5, 33, 38). Under the supreme governing principles established in *Landreville v. Town of Boucherville*, fraud, bad faith, and synthetic document fabrication unravel everything they touch (Motion Rec... pp. 8, 32).

5. FINAL WARNING, STRICT LITIGATION HOLD, AND STATUTORY HOLD MANDATE

18. The RCMP through its ATIP Branch cannot leverage the technical complexity of decentralized databases or internal mailroom delays to insulate ultra vires state action from the superintending purview of the Federal Court (Motion Rec... pp. 36, 41, 43).

19. The formal litigation hold and anti-spoliation mandate remains fully active. Any routine or algorithmic overwriting of the raw PPU 005 audit trails, network terminal cache memory banks, or system error alerts generated during the September-October 2024 epoch will be treated *prima facie* as a **criminal obstruction of justice** and intentional spoliation of evidence (Motion Rec... p. 14).

20. While the Respondents have failed to appear in the FCC and defaulted on their obligations under Rule 318 of the Federal Courts Rules, the pending motions is up in the Federal Court of Canada on June 17, 2026, and at the final argument on June 29 or 30, 2026.

I trust whomever was behind this sort of misconduct is on leave and will be terminated. To be engaged in that sort of fraudulent manipulation of documents in any proceeding let alone a criminal

649

proceeding and to allow that kind of charade and fraud on the court is unforgivable. It nearly killed me but I am still standing through some sort of divine intervention.

21. I reserve all of my rights in fact and at law.

22. Govern yourselves accordingly.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

Enclosures

APPENDICES

<i>APPENDIX #1:</i>

650

ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>

Apr 28, 2026, 2:03 PM

to me

Dear Kevin Mclean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.
- Hexadecimal Mainframe Dumps: The raw, unadulterated “Hexadecimal Dumps” from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.
- Hardware and Terminal Metadata: The internal “Originating Agency Identifier” (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the “Frankenstein” Information Package.
- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.
- DF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or “whitespace bugs” during the processing of judicial PDF instruments.

651 Offline Historical Search Results: The complete, unredacted results of the mandatory “Offline Search” conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.

- System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the “Matching Protocol” and the “Judicial Firewall.”

In order to process your request we require additional information:

- Location: Regarding the first point in your request, “Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.”- Please be advised that PIB PPU 005 is not a singular database, PIBs themselves are not a singular database but rather a way the government collects and stores personal information. Please specify which data base/location you would like to have searched.

You may reply to this email.

Please respond by May 4, 2026.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada

30 Victoria Street, 7th Floor

Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:
<https://www.oic-ci.gc.ca/en/you-submit-complaint>

652

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

On Thu, May 14, 2026 at 9:25 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Date: May 14, 2026

Classification: Private and Confidential

Subject I: Expiration of Statutory Mandate, Crystallization of Deemed Refusal, and Procedural Nullity of Unenumerated Time Extension – File A-2026-00761 / F339

Subject II: Formal Requisition for Mandatory Consideration of Public Interest Disclosure pursuant to Section 19(2)(c) of the Access to Information Act

Sending method: Via Email

Your file number: A-2026-00761 / F339

To:

Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

653

(nota bene: inclusion of Mr. Ball (a director of ATIA and Privacy Branch and included due to crossover between section 8(2)(m) and section 19 of ATIA) and Ms. Tanya Mirsky whom was included by Mr. Ball and I understand to be a chief of staff)

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

1.0. Introduction, Provision of Foundational Acta, and the Doctrine of Constructive Possession

1.1. Correspondence is hereby formally directed regarding the aforementioned matters and the concurrent, interwoven statutory obligations affixed to the institution. It is submitted that the present matter transcends standard administrative inquiries and strikes directly at the foundational cryptographic integrity of the national law enforcement apparatus.

1.2. Appended hereto are the foundational documentary instruments and acta necessary for the adjudication of the principles articulated herein. These records irrevocably establish the chronological matrix and the consequent, unmitigated expiration of the statutory processing period. The incontrovertible evidence of delivery acts as the catalyst for the crystallization of the institution's strict statutory obligations.

1.3. It is categorically advanced that the chronological matrix is governed absolutely by the doctrine of constructive possession. The physical package encompassing the primary requisition, inclusive of the statutorily prescribed financial instrument, was transmitted via independent, state-sanctioned logistical frameworks. The objective delivery confirmation undeniably establishes receipt by the centralized institutional facility on April 14, 2026. At the precise moment the official representative of the state-sanctioned carrier executed the transfer of possession to the institutional receiving facility, the document entered the constructive and legal control of the government institution.

1.4. Internal bureaucratic inefficiencies, deliberate sorting bottlenecks, or localized lethargy in routing documentation from a centralized mail receiving facility to the specific intake analysts operating within the access to information and privacy branch (the "ATIP Branch") possess precisely zero legal capacity to artificially alter the statutorily operative date of receipt. The institutional obligations crystallized instantaneously upon physical delivery; any subsequent internal computation utilizing a delayed processing date is a mathematical and administrative fiction entirely unsupported by the *lex terrae*.

1.5. To permit an institution to unilaterally dictate the commencement of the statutory clock based entirely upon internal administrative convenience would be to completely subvert the quasi-constitutional nature of access legislation. The Supreme Court of Canada has consistently affirmed that the right of access is foundational to democratic accountability; therefore, the statutory timelines designed to facilitate that access must be strictly construed against the state and generously construed in favor of the applicant. The commencement date is irrevocably fixed, rendering the expiration date equally immutable.

2.0. The Absolute Procedural Nullity of the Unenumerated Time Extension and the Prohibition of Extra-Statutory Abeyance

2.1. It is formally recorded that the strict statutory limitation period for the provision of the requisitioned records has irrevocably expired as of May 14, 2026. The institution is presently

654

devoid of any lawful authorization to withhold the demanded metadata.

2.2. It is acknowledged that the institution previously disseminated correspondence purporting to rely upon a time extension (the "**Time Extension**"). However, it is forcefully advanced that the aforementioned correspondence completely neglected the mandatory statutory imperative to meticulously cite the operative subsections or clauses under section 9 of the *Access to Information Act* (the "**ATIA**").

2.3. By neglecting to formally invoke any of the constituent conditional subsections—specifically, the necessity of processing voluminous records pursuant to section 9(1)(a), the requirement for mandatory inter-departmental consultations pursuant to section 9(1)(b), or the explicit mandate for third-party notifications pursuant to section 9(1)(c)—the institution has effectively provided a tacit legal admission that none of the statutorily permissible circumstances for delay are actually present. An extension cannot exist in a jurisdictional vacuum; it must be tethered to a specific, enumerated legislative allowance.

2.4. Consequently, the purported extension constitutes a fundamental, explicit contravention of the statutorily prescribed schema. It is decidedly not a mere administrative irregularity or a curable defect of form; rather, owing to its direct contravention of a federal statute governing quasi-constitutional rights, it manifests as an absolute jurisdictional nullity *ab initio*. A nullity cannot be subsequently ratified or breathed into life by administrative fiat.

2.5. This principle is unequivocally ratified within federal jurisprudence. As authoritatively established by the Federal Court of Appeal in *Statham v. Canadian Broadcasting Corporation*, 2010 FCA 315 (the "*Statham Decision*"), and reinforced consequentially in *Hydro-Québec v. Canada (National Energy Board)*, 1997 CanLII 16223 (FC) (the "*Hydro-Québec Decision*"), an institutional failure to formally, explicitly, and contemporaneously notify an applicant of the precise statutory justifications for a delay operates as a fatal procedural breach. The reviewing courts have definitively concluded that Parliament did not intend to grant institutions a blanket, unreviewable power to delay access; the requirement to specify the subsection is the foundational accountability mechanism ensuring the delay is genuinely warranted.

2.6. Furthermore, as articulated with absolute clarity in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56 (the "*National Defence Decision*"), an invalid, procedurally defective, or entirely absent extension ensures that the original statutory clock remains completely uninterrupted. The legal fiction of the unenumerated extension simply evaporates, leaving the original thirty-day mandate fully operative.

2.7. **Nota Bene:** It is anticipated that the institution might subsequently attempt to retroactively cure this procedural defect by asserting an implied reliance upon administrative burdens, sheer volume, or external consultation requirements in future correspondence. Such an *ex post facto* rationalization is legally barren and must be summarily rejected. The doctrine of *expressio unius est exclusio alterius* mandates that statutory exceptions must be expressly invoked at the time they are relied upon. A failure to explicitly articulate the foundational clause *in limine* ensures that the original statutory clock remains uninterrupted and fully active. The institution is presently operating in a state of constructive refusal.

2.8. **Nota Bene:** Furthermore, any institutional reliance upon a manufactured demand for clarification under section 6 of the *ATIA* as a mechanism to unilaterally hold the statutory timeframe in abeyance is an *ultra vires* maneuver. The governing legislation contains no

655

statutory "pause" mechanism. The deployment of staggered, piecemeal clarification requests formulated weeks after the receipt of an exquisitely detailed, forensically precise requisition constitutes a recognized bad faith tactic designed solely to orchestrate spoliation by delay. The doctrine of paramountcy dictates that internal administrative policies cannot supersede explicit, mandatory statutory provisions enacted by the Parliament of Canada.

3.0. The Substantive Requisition, the Doctrine of Institutional Control, and the Paramount Duty to Search and Seize

3.1. To rigorously forestall any further administrative obfuscation, it is imperative to definitively reiterate the exact parameters of the foundational requisition. The extraction of specific digital artifacts was formally demanded, namely: raw hexadecimal mainframe dumps, immutable investigative data bank audit trails associated with personal information bank RCMP PPU 005, precise hardware and terminal routing metadata (encompassing originating agency identifiers, media access control metrics, and internet protocol assignments), comprehensive inter-agency communication logs, vector analysis reports, offline historical data archives, and system governance manuals.

3.2. It is categorically advanced that these digital artifacts and systemic ledgers reside absolutely within the statutory control of the institution. As the supreme governance authority and physical custodian of the Canadian Police Information Centre (the "CPIC") infrastructure, the institution exercises complete dominion over the mainframe architecture. The postulation that localized data was initially inputted by a municipal police force—frequently mischaracterized as the "originator control" principle—is wholly inapplicable to the systemic metadata, audit logs, and transaction ledgers generated automatically by the federal mainframe itself.

3.3. When a municipal actor engages the federal database, the interaction generates discrete, secondary data points (such as timestamps, network node routing paths, and system error codes) that are inherently authored and owned by the federal apparatus. Once data is injected into the federal apparatus, the corresponding digital footprint is *ipso facto* under federal control and fully subject to the strictures of the *ATIA*. The institution cannot artificially sever its ownership of the systemic architecture simply because a municipal actor utilized the interface.

3.4. Consequently, an absolute, positive statutory duty to execute a comprehensive search is immediately crystallized at the first instance. It is a fundamental tenet of administrative law that the obligation to locate and extract records is a distinct, preliminary operational mandate, entirely divorced from the subsequent, discretionary application of statutory exemptions. The institution is strictly prohibited from preemptively conflating the anticipated application of an exemption with the primary duty to conduct the search. A refusal to even interrogate the database on the speculative presumption that the resulting records might be exempt constitutes a catastrophic failure of the statutory duty to assist and a profound misunderstanding of the two-step processing paradigm.

3.5. Furthermore, should the extracted ledgers contain the personal information or personally identifiable information (the "PII") of third-party individuals other than the applicant (Mr. Kevin A. McLean), the institution is legally precluded from utilizing an "all-or-nothing"

656

withholding strategy. Section 25 of the *ATIA* mandates the rigorous application of the doctrine of severability. The institution must parse the record line-by-line, byte-by-byte.

3.6. Applying the foundational legal maxim *utile per inutile non vitiatur* (the useful is not vitiated by the useless), the institution is statutorily compelled to surgically sever any legitimate third-party personal information and disclose the remaining substantive metadata. For instance, if a network routing log contains the name of a civilian third party alongside the critical internet protocol address exposing a forged entry, the name must be redacted, but the metadata proving the structural collapse of the judicial instrument must be segregated and produced. The mere presence of third-party biographical data cannot be weaponized as a blanket justification to suppress the algorithmic reality of the underlying digital forgery.

3.7. **Nota Bene:** The institution may attempt to argue that the intermingling of municipal operational data with federal metadata renders the extraction technologically burdensome or legally ambiguous, thereby ostensibly excusing the failure to search. This postulation is a technical fiction and a legal nullity. The institution possesses enterprise-level database querying capabilities specifically designed to segregate audit trails based on precise temporal epochs and user identifiers. Any refusal to execute the search based on feigned technological paralysis or the misapplication of third-party privacy exemptions at the search phase constitutes an actionable subversion of the right of access.

4.0. Escalation to the Investigative Authority and the Crystallization of Extraordinary Judicial Remedies

4.1. In light of the aforementioned procedural nullity and the expiration of the operative timelines, formal notification is hereby provided that the issue of the fundamentally improper and *ultra vires* time extension shall be contemporaneously re-raised and prosecuted before the office of the information commissioner (the "**Office of the Information Commissioner**" or "**OIC**").

4.2. The crystallization of this deemed refusal empowers the investigative apparatus to bypass administrative friction and immediately compel the production of the foundational mainframe metadata.

4.3. It must be rigorously observed that pursuant to recent legislative amendments incorporated into section 36.1(1) of the *ATIA*, the Office of the Information Commissioner has undergone a profound jurisdictional transformation. No longer functioning merely as an advisory ombudsman restricted to issuing unenforceable recommendations, the OIC is now vested with explicit, binding order-making authority. Upon the substantiation of this constructive refusal, the investigatory body possesses the unmitigated statutory power to issue a formal, legally binding mandate compelling the immediate extraction and unredacted disclosure of the targeted hexadecimal dumps and systemic routing ledgers. The institution will be subjected to formal compliance orders.

4.4. Moreover, the crystallization of this deemed refusal on May 14, 2026, strips the institution of all discretionary latitude. The matter immediately ripens for extraordinary judicial remedies. The absolute right is fully preserved to seek an immediate prerogative writ of *mandamus* before the Federal Court of Canada.

4.5. The rigorous, multi-pronged legal test for the issuance of *mandamus* is conspicuously satisfied in the present circumstances: firstly, there exists a clear, non-discretionary public legal duty to act (the mandatory processing of the requisition under the *ATIA*); secondly, this

657

duty is owed directly to the applicant; thirdly, there is a clear right to the performance of that duty without extraneous administrative preconditions; fourthly, a formal demand has been explicitly articulated; and finally, a constructive refusal by the state apparatus to execute said duty has materialized through the expiration of the statutory deadline and the reliance on a void extension. An application for *mandamus* will inexorably expose the coordinated orchestration of spoliation by delay.

5.0. The Positive Statutory Obligation of the Head of the Government Institution and the Jurisprudential Imperative

5.1. Notwithstanding the systemic delays orchestrated by the administrative apparatus, an inescapable and non-delegable fiduciary obligation remains affixed to the head of the government institution (the "**Head of the Institution**"). Specifically, the Head of the Institution is statutorily compelled to meticulously evaluate whether a public interest disclosure is warranted regarding the profound institutional malfeasance previously delineated within the primary requisitions.

5.2. The underlying malfeasance involves profound documentary metamorphosis and an orchestrated vector morphology collapse. It has been extensively documented that enterprise-level developer software—specifically the GrapeCity Documents PDF suite, exploiting the documented DOC-6507 bounding-box anomaly—was utilized with precise *mens rea* to unlawfully flatten judicial instruments, forcefully eradicate transparent electronic image signatures, and algorithmically mutate underlying text strings to bypass standard criminal intake procedures.

5.3. This overriding obligation is inextricably rooted within the concomitant legislative frameworks governing the dissemination of federal records. The protections afforded to personal information must invariably be measured against the prevailing democratic imperative. Section 19(1) of the *ATIA* establishes the foundational prohibition against the disclosure of personal information; however, section 19(2)(c) of the *ATIA* immediately incorporates the explicit threshold for the overriding of localized privacy interests as codified within section 8 of the *Privacy Act* (the "**Privacy Act**"), specifically engaging the public interest override mechanism of section 8(2)(m).

5.4. It is a foundational precept of administrative law, as articulated by the Supreme Court of Canada in *Canada (Information Commissioner) v. RCMP*, 2003 1 SCR 66 (*the "RCMP Decision"*), that the Head of the Institution is strictly prohibited from issuing a boilerplate denial upon the mere detection of personal information. The statutory architecture mandates an active, non-delegable duty to exercise discretion and formally document the weighing of the public interest against the privacy invasion. A failure to conduct and document this rigorous balancing exercise constitutes a fundamental abdication of statutory jurisdiction and is universally recognized by the reviewing courts as a reversible error of law. The reviewing courts heavily scrutinize whether that discretion was exercised logically, transparently, and entirely free from improper motives or political interference.

5.5. The threshold for the public interest override, while exactingly high, is unequivocally met in the present circumstances. As delineated in *Mackenzie v. Canada (Minister of Health)*, 2006 FC 871 (*the "Mackenzie Decision"*) and *Fraser v. Canada (Attorney General)*, 2009 FC 272 (*the "Fraser Decision"*), a sharp, uncompromising distinction is drawn between matters of mere public curiosity or sensationalism and matters of genuine democratic public interest. The algorithmic disfigurement of Superior Court instruments, and the subsequent

658

subversion of the coercive apparatus of the state, strikes at the very heart of the democratic order. It represents a systemic corruption of the judicial supply chain, thereby easily vaulting the "clearly outweighs" standard demanded by the legislature.

5.6. Furthermore, the open court principle, robustly defended in *Ritchie v. Canada, 2016 FC 259 (the "Ritchie Decision")*, dictates that when information is inextricably linked to the formal compulsion of the judicial system, the expectation of privacy is severely diminished, if not entirely extinguished. The utilization of the federal mainframe to manufacture a shadow justice system, shielded from public scrutiny by an impermissible invocation of the *Privacy Act*, is fundamentally anathema to this foundational constitutional principle. A justice system that operates on altered PDFs and falsified metadata is a system that has utterly lost the consent of the governed.

5.7. It is advanced through complex syllogistic reasoning that the alleged systemic algorithmic manipulation of the national law enforcement database—specifically the CPIC mainframe—fundamentally eclipses any residual privacy interests of the state actors involved in the initial transcription of the compromised data. As definitively expounded by the Supreme Court of Canada in *Dagg v. Canada (Minister of Finance), 19972 SCR 403 (the "Dagg Decision")*, the fundamental legislative objective of access legislation is the rigorous, unyielding scrutiny of state action. Consequently, public officials engaged in the execution of official duties inherently possess a severely diminished expectation of privacy.

5.8. However, this diminished expectation is entirely obliterated when malfeasance is introduced. When these public officials abdicate their lawful mandates and actively deploy digital architecture to forge authorizations, they cease operating under the lawful execution of their duties. They operate merely under the "colour of authority." Any remaining vestiges of professional immunity are instantly evaporated.

5.9. Applying the foundational legal maxims curated by Herbert Broom, specifically *fraus omnia corrumpit* (fraud vitiates everything), *actus curiae neminem gravabit* (an act of the court shall prejudice no man), and *nemo dat quod non habet* (no one gives what they do not have), it becomes inherently self-evident that a judicial process infected by deliberate digital manipulation is irreparably compromised. A municipal agency possesses absolutely zero inherent jurisdiction to manufacture or disseminate a Superior Court warrant.

5.10. Therefore, the public interest in guaranteeing the cryptographic provenance and algorithmic integrity of the CPIC database is absolute. This overarching democratic imperative *ipso facto* and *prima facie* satisfies the rigorous standard codified within section 8(2)(m)(i) of the *Privacy Act*, as the preservation of the *status quo ante* undeniably outweighs any negligible invasion of the perpetrators' professional privacy. The names, terminal IDs, and ORI routing codes of state actors operating a federal database are professional metrics, not intimate biographical details.

5.11. Consequently, should the institution proceed with an application of the public interest override, the mandatory procedural safeguard codified within section 8(5) of the *Privacy Act* is immediately engaged, requiring proactive, written notification to the federal Privacy Commissioner to ensure rigorous ombudsman oversight over the state's calibration of transparency and privacy harms.

5.12. **Nota Bene:** It is ultimately cautioned that while the reviewing courts apply a deferential "reasonableness" standard to the ultimate opinion formulated by the Head of the Institution, an irrational determination—such as concluding that the professional anonymity

659

of state actors engaged in digital forgery supersedes the algorithmic integrity of the national warrant database—will unequivocally fail to survive even the most deferential judicial scrutiny. The Head of the Institution is bound by a positive obligation to explicitly document the balancing of these factors; a blanket refusal to engage in this statutory balancing exercise would constitute an actionable dereliction of duty, bereft of all reasonableness.

5.13. **Nota Bene:** The institution may attempt to posit the counter-argument that the disclosure of identifying metadata could precipitate the re-identification of specific law enforcement personnel via the mosaic effect. This postulation must be summarily discarded as a profound misapplication of the legislation. The identifying metadata sought—namely, originating agency identifier codes, terminal internet protocol addresses, and media access control metrics—constitutes purely professional, administrative metrics, entirely devoid of intimate biographical substance. The veil of statutory privacy must never be weaponized as an impenetrable sanctuary for the concealment of systemic jurisdictional nullities. In cases of alleged state malfeasance and the arbitrary deprivation of liberty, the public's absolute right to reconstruct the "mosaic of forgery" constitutes the paramount democratic interest.

5.14. **Nota Bene:** Furthermore, any institutional attempt to assert that the requisitioned metadata is overly complex, thereby necessitating sweeping redactions or non-disclosure based on internal technical illiteracy, is a legally fatal maneuver. Section 4(2.1) of the *ATIA* imposes a positive, overarching statutory duty to assist the requester. This duty mandatorily encompasses comprehensive inter-departmental consultations with specialized database architects and cybersecurity personnel. The institution is expressly prohibited from utilizing its own compartmentalized administrative ignorance as a bureaucratic shield.

6.0. Concluding Imperatives and the Crystallization of the *Mandamus* Remedy

6.1. The institution's prompt compliance with its non-delegable statutory obligations and the immediate discharge of its public duties *forthwith* are formally anticipated and demanded.

6.2. The requisite legal demands have been meticulously articulated, and irrefutable receipt thereof has been established via the doctrine of constructive possession. The institutional duty to act is unequivocal, absolute, and non-discretionary. Through the expiration of statutory timelines and the *ultra vires* reliance upon void administrative instruments, the state apparatus has fundamentally failed to discharge this executory duty in the face of a clear, corresponding right of performance.

6.3. It is formally submitted that no alternative, adequate administrative remedy remains extant. The relief sought before the Federal Court of Canada possesses immense, overarching practical value, as it serves to unilaterally restore the cryptographic provenance of the national law enforcement database and expose jurisdictional nullities.

6.4. Consequently, the balance of convenience does not merely tip in favor of granting a prerogative writ of *mandamus* to compel the execution of the foundational search; rather, it weighs overwhelmingly and absolutely in favor of issuing the judicial mandate. While it is a recognized jurisprudential precept that *mandamus* cannot dictate a specific, discretionary substantive outcome, it possesses the absolute, unyielding authority to compel the performance of a specific, ministerial, and executory duty—namely, the mandatory systemic search and the consequent extraction of the requisitioned hexadecimal and routing metadata ledgers.

660

I confirm for good faith purposes, the now comprehensively drafted, signed, and to be paid for and filed NOA (Form 301) will be provided in short order. Short leave to have the primary issues involving writs of mandamus will be sought prior to the commencement of a "long weekend" for some and a statutory holiday for others. I will provide notice to the lead and managerial legal counsel for the RCMP and seek whether they will accept service for the RCMP. If that is the case, all obligations herein and generally will remain.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

On Mon, May 4, 2026 at 9:31 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear RCMP (Access To Information Act Branch):

For ease of reference and continuity, I have copied and pasted your previous email herein. I repeat and rely upon the previous herein and cordially remind you of the deadline of May 14 2026. Thank you.

Mr. Kevin A. McLean (BA, JD, CIM)

Appendix

ATIP / AIPRP

Tue, Apr 28, 2:03 PM (6 days ago)
to me

661

Dear Kevin Mclean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.
- Hexadecimal Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.
- Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.
- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.
- DF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.
- Offline Historical Search Results: The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.
- System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

In order to process your request we require additional information:

- Location: Regarding the first point in your request, "Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction." - Please be advised that PIB PPU 005 is not a singular database, PIBs themselves are not a singular database but rather a way the government collects and stores personal information. Please specify which data base/location you would like to have searched.

You may reply to this email.

Please respond by May 4, 2026.

Please be advised that you are entitled to lodge a complaint with the Information

Commissioner concerning the processing of your request within 60 days of receipt of this

662

notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:

<https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive

Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message, including attachments, is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Fri, May 1, 2026 at 11:29 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DELIVERY METHOD: Via Electronic Transmission (ATIP-AIPRP@rcmp-grc.gc.ca)

TO:

663

Commissioner Michael Duheme, Head of the Institution

Mr. Stéphane Brisson, Chief Privacy Officer and Director General

Melissa Simpson, Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

DATE: May 1, 2026

REFERENCE:

ATIA Request A-2026-00761 / F339

OIC Complaint File Number: ACC-2026-04-00379

SUBJECT: FORMAL REJECTION OF OBSTRUCTIVE CLARIFICATION TACTICS, EXPLICIT IDENTIFICATION OF DATABASE LOCATIONS, REBUKE OF WILLFUL BLINDNESS, AND REAFFIRMATION OF THE MAY 14, 2026 STATUTORY DEADLINE

1.0. PRELIMINARY OBSERVATIONS AND THE DOCTRINE OF BAD FAITH

1.1. Receipt is hereby acknowledged of the electronic correspondence dispatched by your office on April 28, 2026. In this correspondence, the Access to Information and Privacy (ATIP) Branch asserts a purported inability to locate the requisitioned records on the grounds that Personal Information Bank (PIB) RCMP PPU 005 is "not a singular database" but merely a classification method, and subsequently demands that I "specify which data base/location you would like to have searched."

1.2. This communication is formally and categorically rejected as a deliberately obtuse administrative maneuver, entirely devoid of substantive merit. It constitutes a secondary, transparent attempt to artificially pause the statutory clock under the guise of Section 6

664

of the Access to Information Act (ATIA). The institution is acutely aware that an active investigative file (ACC-2026-04-00379) has already been crystallized before the Office of the Information Commissioner (OIC) regarding this exact, documented pattern of manufactured ambiguity, arbitrary extensions, and statutory dereliction. In administrative law, the deployment of piecemeal, staggered requests for clarification—especially when deployed weeks after the initial receipt of a highly specified requisition—is routinely recognized by the Federal Courts as a bad faith tactic designed to orchestrate spoliation by delay. It is a systematic subversion of the legislative intent of the ATIA, which is predicated on timely, unencumbered public access.

1.3. The institutional attempt to weaponize Treasury Board Secretariat (TBS) definitions against an applicant is a profound misapplication of administrative procedure. It is a matter of foundational federal record-keeping that a Personal Information Bank describes the *nature* of the records, the class of individuals to whom the data pertains, and the statutory authority for their collection. It inherently does not, and was never intended to, dictate the physical topology of the server farm or the specific network pathways. The RCMP, as the sovereign custodian of these records, inherently possesses the internal architectural mapping that links the TBS classification (PPU 005) to the specific physical servers, virtual environments, and digital repositories where this data is housed. The master indices bridging policy classifications with IT infrastructure are entirely within your institutional control.

1.4. To demand that a civilian applicant provide the proprietary, internal server rack designations, exact software file-paths, or secure network node identifiers utilized by the RCMP Information Technology Directorate is an absurdity that borders on administrative malfeasance. The foundational premise of access to information legislation is that the government holds both the records and the corresponding indices required to locate them. You hold the master key; you are legally, statutorily, and ethically obligated to turn it. Attempting to shift the internal administrative burden of locating a federal server onto a private citizen represents a catastrophic failure of the ATIP Branch's statutory mandate and a glaring breach of the public trust. It operates on the legally bankrupt premise that an applicant must be a certified systems architect of the very institution they are seeking to hold accountable in order to exercise their quasi-constitutional rights.

2.0. EXHAUSTIVE SPECIFICATION OF DATABASE ARCHITECTURE AND LOCATION

2.1. The institution's assertion that it requires me to name the specific "database/location" is procedurally fatal and factually bankrupt. The original requisition, drafted with exacting, enterprise-level forensic precision, explicitly identified the target architectures. To feign ignorance of the targeted location when the "CPIC mainframe" and "Investigative Data Bank" were explicitly named in the very first bullet point of the primary request is an egregious exhibition of willful institutional blindness.

2.2. However, to permanently cure any residual, manufactured ambiguity, to completely exhaust the ATIP Branch's ability to rely upon feigned technical incomprehension or artificial ignorance, and to meticulously prepare the evidentiary record for the Federal

665

Court of Canada, you are hereby formally directed to execute the required digital extractions within the following specific, explicitly defined federal architectures:

A. The Canadian Police Information Centre (CPIC) Mainframe: Specifically, the foundational transaction logs and immutable audit ledgers housed deep within the core CPIC system architecture. This explicitly includes the uninterpreted hexadecimal and binary matrices—complete with EBCDIC/ASCII decoded text translations. It is an incontrovertible fact of database architecture that standard graphical user interfaces (GUIs) utilized by frontline officers are merely a presentation layer; they are entirely inadequate for this inquiry. The GUI acts as an operational smokescreen that visually homogenizes corrupted data to present a facially valid warrant to the end-user. Only the raw hexadecimal memory offsets can bypass this presentation layer to expose the algorithmic disfigurement and vector morphology collapse of the specified judicial instruments. These binary dumps are mathematically immune to human misinterpretation and will irrefutably demonstrate exactly when, and by whom, the enterprise-level GrapeCity Documents PDF suite (specifically version 6.0.2.0, utilizing the documented DOC-6507 bounding-box bug) was utilized to unlawfully flatten the document, algorithmically mutate the text, and forcefully delete the transparent electronic image signature of Chief Justice Geoffrey B. Morawetz.

B. The Investigative Data Bank (IDB): As explicitly referenced in my primary request ("Investigative Data Bank Audit Trails" and "Offline Historical Search Results"), this is the precise operational database wherein the historical chronology of transactions is preserved. The municipal record currently presents a glaring chronological impossibility: an arrest executed on October 2, followed by the inexplicable expungement of the purported warrant via the Integrated Court Offences Network (ICON) on October 3. In the realm of lawful judicial processes, a warrant does not magically evaporate the day after its execution; it is formally filed as a return to a justice. While a fraudulently altered warrant may be ostensibly excised from the active frontline interface to conceal an unlawful arrest and orchestrate localized spoliation, the underlying chronological footprint of the ADD, MODIFY, CLEAR, and CANCEL commands remains permanently and immutably inscribed within the IDB archives. Every keystroke generates a timestamped digital artifact; this request demands the extraction of those exact artifacts.

C. The National Police Information Services (NPIS) Infrastructure: This encompasses any centralized transaction ledgers, active mirror servers, localized terminal caches, or disaster recovery backup tape archives operating under the overarching NPIS umbrella. In a modern, enterprise-level federal law enforcement framework, true digital deletion is an absolute myth. Highly sophisticated asynchronous data replication redundancies ensure that when a corrupted file is purged from a local municipal terminal in a panic to hide evidence of forgery, it is immediately preserved in the federal disaster recovery backups. This request specifically targets the preservation of data that captures network session activity for the critical temporal epoch encompassing September 22 to October 4, 2024. The RCMP is strictly prohibited from allowing the routine overwriting of these specific backup tapes.

666

D. The CPIC Audit Log (CAL) / Systemic Routing Ledgers: The specific digital repository and network gateway logs where Originating Agency Identifiers (ORI), Media Access Control (MAC) addresses, and Internet Protocol (IP) terminal metadata are permanently recorded during data-entry sessions. This is specifically targeted at data originating from municipal partner agencies (namely, the Toronto Police Service). These routing metrics are fundamentally necessary to invoke the foundational legal maxim *nemo dat quod non habet* (no one gives what they do not have). If an instrument purportedly authorized by a Superior Court Chief Justice operating out of the 361 University Avenue courthouse was, in digital reality, inputted from a municipal police division's back-office terminal, the ORI routing codes and MAC addresses will incontrovertibly prove the jurisdictional nullity. A municipal agency possesses absolutely zero inherent jurisdiction to manufacture, authorize, or disseminate a Superior Court warrant. The metadata will expose the federal database being utilized as a secure digital vault for municipal-level documentary forgery.

3.0. BREACH OF THE DUTY TO ASSIST AND MANDATORY INTERNAL CONSULTATIONS

3.1. The burden of navigating the RCMP's proprietary internal server nomenclature does not rest upon the applicant, nor can the ATIP Branch utilize its own internal compartmentalization of technical knowledge as a bureaucratic shield against mandatory disclosure. Section 4(2.1) of the ATIA imposes a positive, overarching "duty to assist" upon the institution. This is not a passive suggestion, a mere administrative courtesy, or a set of guidelines to be followed when convenient; it is a rigorous, legally enforceable statutory mandate designed to facilitate transparency and dismantle institutional obstruction.

3.2. The Supreme Court of Canada has consistently and forcefully held that access legislation is not a game of blind man's bluff. An institution cannot hide behind administrative semantics or feigned technical illiteracy to deny access to clearly described records. As previously stated, the jurisprudence mandates that you process the request utilizing an "experienced employee." A standard administrative intake clerk in the ATIP mailroom may not immediately understand the physical network topology of where PPU 005 data resides, but a CPIC Database Administrator, a senior cybersecurity systems architect, or the Director of Information Management fundamentally does.

3.3. Your absolute failure to conduct this mandatory inter-departmental consultation prior to dispatching an obstructive, ten-day demand for clarification constitutes a highly actionable breach of process. The correct, legally mandated procedure upon receiving a highly technical request is to forward the parameters to the specialized operational unit (in this case, CPIC Systems Governance, IT Security, and the NPIS database architects) for extraction. If the ATIP analyst does not know where the PPU 005 audit trails are located, their strict legal duty is to ask the RCMP's internal systems administrators—not to bounce the requisition back to the applicant in a transparent attempt to exhaust civilian resources, create artificial administrative friction, and arrest the statutory timeline. Internal friction between the RCMP's ATIP division and its IT division is an

667

internal operational failure; it is not a valid statutory excuse for denying a Canadian citizen their quasi-constitutional rights.

4.0. ABSOLUTE CONTINUITY OF THE STATUTORY CLOCK AND REJECTION OF EXTRA-STATUTORY DEADLINES

4.1. The institution's attempt to unilaterally impose a new, arbitrary deadline of "May 4, 2026" to respond to this feigned incomprehension, coupled with the highly irregular implicit threat of summary file closure, is *ultra vires* the jurisdiction conferred by the governing legislation and legally void *ab initio*. The Access to Information Act does not contain an "abeyance mechanism," nor does it feature a "pause button" for administrative clarification once a request containing sufficient detail has been formally received.

4.2. To rigorously reiterate the doctrine of exhaustive enumeration (*expressio unius est exclusio alterius*), Parliament deliberately and specifically outlined the *only* valid reasons for delaying a request under Section 9 of the ATIA (specifically: massive volume of records, mandatory external consultations, or mandatory third-party notice). If Parliament had intended for federal institutions to possess the sweeping authority to arbitrarily pause the thirty-day clock simply because they wished to ask the applicant a clarifying question under Section 6, they would have explicitly legislated that extraordinary power. They decidedly did not. Therefore, this unilateral deadline is an invention of institutional convenience, a pure procedural phantom entirely unsupported by the *lex terrae*.

4.3. As previously and exhaustively detailed in my correspondence of April 24, 2026, the statutory clock commenced upon the objectively verified, third-party delivery of the original requisition via Canada Post on April 14, 2026. The Supreme Court of Canada and the Federal Courts recognize the doctrine of constructive possession. Internal mailroom inefficiencies, internal routing delays, sorting bottlenecks, and subsequent administrative tardiness by the ATIP Branch in physically opening the file on April 15, 2026, do not artificially alter the legally operative date of receipt. The institution was in constructive possession of the request on April 14; the legal obligations crystallized at that precise moment.

4.4. Furthermore, the institution failed entirely to secure a procedurally valid extension of time pursuant to Section 9 of the ATIA within the necessary timeframe. The jurisprudence is absolute on this matter: you cannot retrospectively repair a failure to invoke a formal Section 9 extension by generating an informal, extra-statutory Section 6 clarification delay as a stopgap measure. Therefore, the mandatory, legally binding deadline for the complete, substantive, and unredacted provision of these systemic records remains irrevocably, mathematically fixed at May 14, 2026.

4.5. I hereby confirm that the deadline to provide these records, as an absolute and unyielding statutory deadline, remains that of May 14, 2026. There will be no further extensions, no permitted abeyances, and no tolerance for further bureaucratic attrition.

5.0. IN LAYMAN'S TERMS

668

5.1. Breakdown of Institutional Misunderstanding

In layman's terms, Ms. Simpson is confusing a conceptual filing category with a physical storage location, and she is asking me to do her IT department's job for her. The request operates on the transparently bad-faith assumption that if the ATIP branch plays dumb long enough, the statutory deadline will quietly pass, and the applicant will simply abandon the pursuit of these critical records out of sheer administrative exhaustion.

Here is a breakdown of exactly what she is misunderstanding (or deliberately pretending to misunderstand to orchestrate delay):

5.1.1. The "Filing Cabinet" Analogy

A Personal Information Bank (PIB), like "PPU 005," is just a government classification code. It describes the *type* of information collected (e.g., investigative records, as opposed to employee payroll records, human resources data, or procurement contracts). Imagine going to a large, complex metropolitan hospital and asking the administration for a copy of your "Medical Records." Ms. Simpson's response is the exact equivalent of the hospital receptionist looking at you blankly and stating, *"Medical Records isn't a physical drawer; it's just a conceptual framework of how we group health data according to Ministry guidelines. Therefore, I cannot help you. Please tell me the exact floor, the specific room number, the specific filing cabinet serial number, and the exact manila folder where your papers are kept before I will even begin to look for them."* She is arguing that because PPU 005 is a category label, she doesn't know where to physically look. However, the RCMP's own database administrators absolutely know which specific servers, which specific mainframes, and which software systems hold "PPU 005" data. They built the systems. She simply hasn't asked them, preferring instead to feign paralysis.

5.1.2. The Bank Statement Analogy

To provide a secondary, equally damning analogy, this institutional response is akin to an individual requesting a transaction history from a major commercial bank for a specific date range, only for the bank teller to respond: *"A transaction history is just a classification of financial data. Please provide us with the exact IP address of the server rack in our underground data center where your specific digital ledger is hosted, otherwise we will close your inquiry."* It is an absurd, structurally illogical proposition designed solely to frustrate access and protect the institution from scrutiny.

5.1.3. The Library Analogy (Dewey Decimal System)

If the RCMP were a public library, PPU 005 is simply the Dewey Decimal code for "History." I have asked for a specific history book. Ms. Simpson is claiming she cannot fulfill the request because "History" is a category, not a physical shelf, and is demanding that I provide her with the exact GPS coordinates of the shelf in her own building. The librarian knows where the history section is; the ATIP branch knows where the PPU 005 records are stored.

5.1.4. Ignoring What I Already Told Her

669

She is pretending that I didn't give her a location. However, in the very first bullet point of my original request, I explicitly named the Canadian Police Information Centre (CPIC) mainframe and the Investigative Data Bank. I *did* give her the locations; she is simply ignoring those highly specific, globally recognized federal system names to falsely claim my request is too vague to process.

5.1.5. Shifting the Burden (Breach of Duty to Assist)

Under the law, she is strictly required to consult with an "experienced employee" (like an RCMP systems architect, a database engineer, or a network security officer) to figure out where to pull this data. Instead of doing her job and asking her own internal IT department, "*Hey, which internal database holds the PPU 005 transaction logs for CPIC?*", she is illegally bouncing the question back to me. She is effectively demanding that I, a civilian, provide the RCMP's proprietary, internal server names or highly specific classified network file paths—which is an impossible, unreasonable, and statutorily prohibited request.

Ultimately, her "misunderstanding" serves as nothing more than a convenient, highly manufactured bureaucratic excuse to illegally pause the 30-day statutory clock, frustrate the federal oversight process, and delay handing over the CPIC transaction logs I requested.

6.0. CONCLUSION, DEEMED REFUSAL, AND ESCALATION TO THE FEDERAL COURT

6.1. The continued utilization of these dilatory tactics creates a profound, inescapable circumstantial inference of bad faith. It is becoming manifestly obvious that these administrative delays are a coordinated attempt to conceal the algorithmic disfigurement of Superior Court instruments by state actors. By intentionally pushing the disclosure timeline past the imminent departure of Chief Justice Morawetz, the institution is seemingly attempting to obscure the *status quo ante*, run out the clock on the immediate jurisdictional issues, and evade contemporaneous judicial scrutiny regarding the integrity of the warrants issued under his purported authority.

6.2. Be formally advised that any failure to effectuate the complete, unredacted disclosure of the specified hexadecimal dumps, IDB audit trails, and ORI routing codes from the CPIC mainframes by the exact deadline of May 14, 2026, shall be automatically and decisively classified as a Deemed Refusal pursuant to Section 10(3) of the ATIA.

6.3. Statutory Order-Making Powers of the Information Commissioner: The institution is formally reminded that the Office of the Information Commissioner (OIC), in stark, profound contrast to the Office of the Privacy Commissioner, is vested with explicit, binding order-making authority under recent legislative amendments to the ATIA. Pursuant to Section 36.1(1) of the ATIA, should the Commissioner find this complaint of administrative stalling and constructive refusal to be well-founded, she possesses the statutory power to issue a formal, legally binding order compelling the Head of the Institution to disclose the requested records. The Information Commissioner does not

670

merely issue polite recommendations or operate as a toothless ombudsman; she wields the sword of compliance. The ATIP Branch's continued reliance on obstructive tactics will not merely result in adverse administrative findings; it will culminate in a binding legal mandate to disclose, accompanied by a highly damaging public report detailing the institution's obstruction.

6.4. Upon the crystallization of this Deemed Refusal on May 14, 2026, the institution is stripped of all discretionary latitude. This matter will ripen immediately for extraordinary judicial remedies. I fully reserve the right to seek an immediate prerogative writ of *mandamus* before the Federal Court of Canada to compel the physical production of these digital ledgers. The legal test for *mandamus* is clearly met here: there is a public legal duty to act, the duty is owed to the applicant, there is a clear right to the performance of that duty, and there has been a demand and a constructive refusal. A *mandamus* application will explicitly cite the institution's bad faith, the flagrant breach of the statutory duty to assist, deliberate administrative stalling, and the coordinated orchestration of spoliation by delay.

6.5. Furthermore, should it become necessary to engage the Federal Court to bypass this administrative blockade and pierce the veil of institutional secrecy, such an application will be accompanied by petitions for severe, punitive cost awards against the institution. It may also necessitate naming specific institutional heads, Directors General, and ATIP officers in their official capacities to answer directly to a Federal Court Justice for the systemic dereliction of their statutory duties.

6.6. Public Disclosure Notice and Statutory Balancing: I cordially remind the Commissioner of the RCMP, along with the Chief Privacy Officer, that the Head of the Institution is required by law to consider the requirement to issue a public disclosure notice. In my view, the systemic algorithmic manipulation of the national warrant database does not fall under standard complaint grounds; it is a matter of profound national security and constitutional integrity that would necessitate immediate judicial review. I note definitively that the Access to Information Act (specifically Section 19 regarding public interest overrides) and the Privacy Act (specifically Section 8 regarding the disclosure of personal information in the public interest) work in tandem as a seamless code. The overarching public interest in ensuring the Canadian law enforcement apparatus is not operating on algorithmically forged judicial instruments absolutely obliterates any residual privacy interests of the state actors who inputted the fraudulent data.

This document serves as full, final, and exhaustive clarification. There is no further ambiguity. The locations are identified. The databases are named. The analogies have been provided. Proceed with the substantive extraction of the records from the explicitly named databases immediately.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

671

Chartered Investment Manager

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Apr 23, 2026 at 2:27 PM ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca> wrote:

Dear Kevin McLean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.***
- Hexadecimal Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.***
- Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.***
- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.***

672

- DF Flattening and Vector Analysis Reports: *All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.*

- Offline Historical Search Results: *The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.*

- System Governance Manuals: *Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."*

In order to process your request we require additional information:

- **Scope:** We have examined your request and fail to understand exactly what you are seeking in terms of records or documentation. As per section 6 of the Access to Information Act, "A request for access to a record under this Part shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort." **Please clarify what records you are seeking.**
- **Application fee:** The Access to Information Act prescribes an application fee of \$5.00. This is payable by cheque or money order to the Receiver General of Canada.

You may send this via regular mail or e-mail to the contact listed below.

Your file will remain open in our office for the next 10 days. If we have not received a response by **May 4, 2026**, this file will be closed.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:
<https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

673

Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'aviser immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

TAB 18



 Print page

Your documents have been submitted to the Federal Court using the Electronic Filing System (E-Filing System).

Your document(s) have been submitted to the Federal Court.

- You have submitted **1 document(s)** to the **Toronto Registry Office**.
- Your unique confirmation number for this submission is: **2026-06-16-9672326776129**.
- Date submitted: **06/16/2026 at 4:39:13 P.M. Eastern Time (ET)**.

Note that your document(s) will be **considered successfully filed after the Registry reviews, accepts and processes your submission**.

You will then receive an email that includes the Court File Number and a hyperlink to the stamped documents.

- [What's next](#)
- [Urgent matter](#)
- [Online access to documents](#)
- [Your submission](#)

What's next

You will receive an email from **noreply-nepasrepondre@cas-satj.gc.ca** with the unique confirmation number above.

Federal Court Registry personnel will review your submission and determine whether it can be accepted.

✓ Accepted document(s)

If your document(s) comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will accept and process your submission.
 - Your document(s) will be deemed as filed on the date and time of your submission to the E-Filing System, Eastern time (ET); unless you submitted on a Saturday, Sunday, or [holiday](#). If you submitted on a weekend or holiday, they will be deemed as filed on the next business day.
2. You will receive an email confirming that your document(s) have been accepted and filed. The email will include the Court File Number and a hyperlink to the stamped document(s).

✗ Non-accepted document(s)

If your document(s) do not comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will send you an email to inform you of the filing status and provide instructions for corrections.
2. Use the E-filing System and your unique confirmation number to submit the corrected document(s). The submission of a corrected document will not result in additional charges.
3. After you submit the corrected document(s), they will be reviewed. The Registry will send you an email indicating whether or not the corrected documents have been accepted.

676

 Issues related to document type

If you selected the wrong document type(s) in the E-Filing System this may affect the applicable filing fee. The Federal Court Registry may contact you by phone or email for additional payment or a refund.

Urgent matter

If you have flagged your submission as urgent, please [contact the Registry](#). Submitting documents electronically does not guarantee that they will be reviewed immediately.

Online access to documents

If you have requested your submission be exempt from public online access, the documents mentioned will not be made available online until the Court makes a decision about your request and informs you.

► Your submission

Share your feedback

Take 5 minutes to help us improve our service.

Start survey

Start a new submission

About the Court

[Jurisdiction](#)

[Careers](#)

[Liaison Committees](#)

[Reports and Statistics](#)

Law and Practice

[Acts and Rules](#)

[Practice Guides](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Court Costs](#)

[Deadlines Calculator](#)

[Checklists](#)

Online Access

[Forms](#)

[E-Filing](#)

[E-Motion](#)

Representing Yourself

- [Finding Legal Help](#)
- [Practice Guides](#)
- [Procedural Charts](#)
- [Procedural Roadmaps](#)
- [Checklists](#)
- [Court Costs](#)
- [Deadlines Calculator](#)
- [Resolving Your Case](#)
- [Registry](#)

Court Files and Decisions

- [Court Files](#)
- [Decisions](#)
- [Hearing Lists](#)
- [Generalittings](#)
- [Summer Recess](#)
- [Calendar of Hearings](#)

Media

- [Administration of the Court](#)
- [Court Files](#)
- [Decisions](#)
- [Calendar of Hearings](#)

Resources

- [Registry](#)
- [Court Costs](#)
- [Procedural Charts](#)
- [Procedural Roadmaps](#)
- [Resolving Your Case](#)
- [Finding Legal Help](#)
- [Checklists](#)

TAB 19

Requisition for Hearing — Application

Court File Number: T-2448-26

FEDERAL COURT

B E T W E N:

KEVIN A. MCLEAN

Applicant

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL,
AND STEPHANE BRISSON

Respondents

Requisition for Hearing

TO:

Manager of Court Operations/Judicial Administrator/Registrar of the Federal Court of Canada (City of Toronto)

180 Queen Street West,
Suite 200
Toronto, Ontario
M5V 3L6**THE APPLICANT REQUESTS** that a date be set for the **Hearing** of this **Application**.**THE APPLICANT CONFIRMS THAT:**

1. The requirements of subsection 309(1) of the Federal Courts Rules have been complied with.
2. There is no requirement to serve a notice of constitutional question under section 57 of the Federal Courts Act in this application.
3. The hearing should be held at Toronto, Ontario.
4. The Applicant respectfully submits that the hearing of this unopposed Judicial Review Application should be scheduled for no more than two (2) hours, and that the Application should be determined entirely in writing pursuant to Rule 369, for the following reasons:

- a. The Respondents have not participated in this Proceeding, have not opposed the relief sought in the Judicial Review Application (served May 15, 2026), and have not objected to the Applicant’s Rule 317 Request for materials in the possession of the RCMP, an “other tribunal” within the meaning of the *Federal Courts Act* and *Federal Courts Rules*. The issues raised are of **general public importance**, including:
- (i) the proper scope of access rights under the *Privacy Act* and *Access to Information Act*;
 - (ii) the jurisdictional boundaries between federal administrative bodies;
 - (iii) the constitutional relationship between Parliament, provincial legislatures, and administrative decision-makers; and
 - (iv) core Rule of Law principles, including equality before the law, accountability, and access to justice.

The Rule of Law requires judicial intervention where administrative bodies adopt conflicting interpretations of their authority, as the legal system cannot tolerate operational conflicts or inconsistent orders. Uniformity, consistency, and the judiciary’s “final word” on such matters are essential.

- b. Although the Federal Court is not subject to the statutory timelines imposed on provincial superior courts (e.g., *Courts of Justice Act*, s. 123), the Canadian Judicial Council’s standards contemplate that decisions should be released within six months of being taken under reserve. It would be contrary to the public interest for such a timeline to apply where:

- (i) the Respondents have not opposed the Application;
- (ii) the Rule 317 Request is unopposed and unobjected to; and
- (iii) the issues are novel, unprecedented, and of significant public importance.

A hearing date before the end of June 2026 ensures that the decision-making timeline is engaged and that these issues receive timely adjudication.

- c. The Applicant has requested that the motions judge assigned to Notice of Motion #1 (June 17, 2026) issue **Bottom-Line Orders** (Federal Courts Rules, s. 2) with reasons to follow, consistent with *Teskey*; *Cunningham*; *Children’s Aid Society of Toronto v. K.(A.)*; *Law Society of Ontario v. Harrison*; and *Little Start Child Care Inc.* The Supreme Court of Canada has affirmed that justice may be best served by releasing the disposition promptly, with written reasons to follow. This principle applies with even greater force where a federal institution has not opposed the relief sought and where the underlying statutes (*Privacy Act* and *ATIA*) are quasi-constitutional in nature.
- d. The Ontario Court of Appeal in *R. v. Cunningham*, 2011 ONCA, held that reasons—even if released long after the disposition—are presumed to reflect the reasoning that led to the decision, and that there is **no legal time limit** on the delivery of reasons. This reinforces the propriety of Bottom-Line Orders in matters of public importance.
- e. To ensure a binding, public, and authoritative decision that provides necessary jurisdictional boundaries and guidance, a hearing date must be set by the Judicial Administrator **before the end of June 2026**, prior to the Court’s summer recess.
- f. Although judicial review requires the Court to apply the appropriate standard of review to each question, the Applicant—consistent with the principle of **dominus litis**—has structured the Application Record and

Motion Record to facilitate an efficient written determination. The Applicant has filed a comprehensive, fully bookmarked and hyperlinked record addressing all relevant standards of review and legal issues.

- g. Judicial review is intended by Parliament and the Governor in Council to be a **summary procedure**, reinforced by Rule 3 of the *Federal Courts Rules*. Where Respondents do not oppose the relief sought, the Rules impose mandatory obligations:

(i) under Rule 305, a Respondent must file a Notice of Appearance within 10 days if it intends to oppose;

(ii) under Rule 318(2), a Respondent must object in writing, with reasons, if it opposes the production of materials requested under Rule 317.

None of these mandatory steps have been taken.

- h. As conferences are not applicable to this Judicial Review Application as the Applicant has now filed a Requisition for Hearing in Form 314 before the expiry of the 180 day period (see: section 380(2) of the Federal Courts Rules) the Applicant submits that the Judicial Review Application should be scheduled for hearing on **June 29 or June 30, 2026**, together with the unopposed Rule 317 motion, to secure the **just, most expeditious, and least expensive** determination of this Proceeding, consistent with Rule 3 and the overarching interests of justice.
- i. The Applicant undertakes to be available on both days in full on a remote basis to appear via remote video technology should any oral submissions or clarifications to the written submitted and filed documents be required.

5. The representatives of all parties to the application are as follows:

a. on behalf of the Applicant:

- i. Mr. Kevin A. McLean (BA, JD, CIM), appearing Pro Se and Pro Bono Publico, 68 Abell Street, Toronto, ON M6J 0B1; Email: mclean@searchandseizure.ca

b. on behalf of the Respondents:

- i. Nil.
- ii. The Respondents failed to serve, file with proof of service, a Notice of Appearance pursuant to Rule 305 and are disentitled to the following:

1. Notice of steps;
2. Service of documents;

6. The parties are available at any time except:

- a. The Applicant is fully available on the below dates to appear remotely should any oral submissions or clarification regarding written submissions.

- i. The Applicant respectfully requests a hearing date of Tuesday, June 29 or Wednesday, June 30, 2026, to ensure the public interest issues are heard and decided, in writing (allowing

7. The hearing will be in English.
8. An interpreter will not be required.
9. The materials in the requisition for hearing file are in English.

The Applicant, with gratitude to the FCC (Toronto), and with great respect submits the following and certifies that it is true, accurate and complete:

DATED at Toronto, Ontario, this 12th day of June, 2026.



Mr. Kevin A. McLean (BA, JD, CIM)

68 Abell Street

Toronto, ON

M6J 0B1

email: mclean@searchandseizure.ca

Applicant (Self-Represented)

TO:

Nil (as per the above and the evidence contained in the Applicant's most recent Motion Record for NOM #1 of June 11, 2026)

[SOR/2021-151, s. 23](#)



 Print page

Your documents have been submitted to the Federal Court using the Electronic Filing System (E-Filing System).

Your document(s) and payment have been submitted to the Federal Court.

- You have submitted **1 document(s)** to the **Toronto Registry Office**.
- Your unique confirmation number for this submission is: **2026-06-12-5485328130686**.
- Date submitted: **06/12/2026 at 4:32:40 P.M. Eastern Time (ET)**.

Note that your submission will **only be considered filed** in Federal Court **after it has been examined, accepted and processed by the Registry**.

- [What's next](#)
- [Urgent matter](#)
- [Online access to documents](#)
- [Your submission](#)

What's next

You will receive an email from **noreply-nepasrepondre@cas-satj.gc.ca** with the unique confirmation number above.

Federal Court Registry personnel will review your submission and determine whether it can be accepted.

✓ Accepted document(s)

If your document(s) comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will accept and process your submission.
 - Your document(s) will be deemed as filed on the date and time of your submission to the E-Filing System, Eastern time (ET); unless you submitted on a Saturday, Sunday, or [holiday](#). If you submitted on a weekend or holiday, they will be deemed as filed on the next business day.
2. You will receive an email confirming that your document(s) have been accepted and filed. The email will include the Court File Number and a hyperlink to the stamped document(s).

✗ Non-accepted document(s)

If your document(s) do not comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will send you an email to inform you of the filing status and provide instructions for corrections.
2. Use the E-filing System and your unique confirmation number to submit the corrected document(s). The submission of a corrected document will not result in additional charges.
3. After you submit the corrected document(s) by email, they will be reviewed. The Registry will send you an email indicating whether or not the corrected documents have been accepted.
 - If you paid filing fees for document(s) that the Court did not accept for filing, you will receive a refund.

684

 Issues related to document type

If you selected the wrong document type(s) in the E-Filing System this may affect the applicable filing fee. The Federal Court Registry may contact you by phone or email for additional payment or a refund.

Urgent matter

If you have flagged your submission as urgent, please [contact the Registry](#). Submitting documents electronically does not guarantee that they will be reviewed immediately.

Online access to documents

If you have requested your submission be exempt from public online access, the documents mentioned will not be made available online until the Court makes a decision about your request and informs you.

► Your submission

Share your feedback

Take 5 minutes to help us improve our service.

Start survey

Start a new submission

About the Court

[Jurisdiction](#)

[Careers](#)

[Liaison Committees](#)

[Reports and Statistics](#)

Law and Practice

[Acts and Rules](#)

[Practice Guides](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Court Costs](#)

[Deadlines Calculator](#)

[Checklists](#)

Online Access

[Forms](#)

[E-Filing](#)

[E-Motion](#)

Representing Yourself

[Finding Legal Help](#)

[Practice Guides](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Checklists](#)

[Court Costs](#)

[Deadlines Calculator](#)

[Resolving Your Case](#)

[Registry](#)

Court Files and Decisions

[Court Files](#)

[Decisions](#)

[Hearing Lists](#)

[Generalittings](#)

[Summer Recess](#)

[Calendar of Hearings](#)

Media

[Administration of the Court](#)

[Court Files](#)

[Decisions](#)

[Calendar of Hearings](#)

Resources

[Registry](#)

[Court Costs](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Resolving Your Case](#)

[Finding Legal Help](#)

[Checklists](#)



Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Payment received – Submission Confirmation (Federal Court). Unique Confirmation number 2026-06-12-5485328130686 (T-2448-26)

1 message

noreply-nepasrepondre@cas-satj.gc.ca <noreply-nepasrepondre@cas-satj.gc.ca>
To: mclean@searchandseizure.ca
Cc: mclean@searchandseizure.ca

Fri, Jun 12, 2026 at 4:35 PM

This email confirms you have paid a filing fee associated with a proceeding in the Federal Court.

We value your feedback! If you have not already done so, [share your experience with Pay Now](#) in our quick survey.

Contact Information

First Name: Kevin
Last Name: McLean
Telephone Number: 6473709354
Email Address: mclean@searchandseizure.ca

Proceeding Information

Payment Reference Number: 4126493
Unique Confirmation Number: 2026-06-12-5485328130686
Court File Number: T-2448-26
Style of Cause: Kevin Alexander McLean v. Royal Canadian Mounted Police

Filing Party: KEVIN A MCLEAN
Document Type: Requisition for Hearing - Application (\$50.00)
Document File Name: Form 314 - Requisition For Hearing - McLean v. RCMP et al - Applicant - KAM (BA JD CIM) - 12-June-2026 - SIGNED - FILED.pdf
Online Access: Not Applicable

Payment Information

Transaction Date: June 12, 2026 at 04:32 PM ET
Authorization number: 665402670017340840
Amount Paid: \$50.00

Please do not respond to this email. This email address is automated and unattended, and cannot help with questions or requests.

Please contact the [Registry of the Federal Court](#).

TAB 20

Date: June 19, 2026

Classification: Private and Confidential

Sending and filing method: E-Filing Portal

TO:

The Registry of the Federal Court of Canada

Attention: The Registrar/Manager of the Federal Court of Canada, Local Registrar of the Toronto Federal Court of Canada Court Office and Mr. Tristan Mercieca, Registry Officer

SUBJECTS

Subject I: Resubmission of Form 314 Requisition for Hearing – Court File No. T-2448-26

Subject II: Clarification of Procedural Nullities and Response to Registry Correspondence Dated June 16, 2026

Subject III: Formal Request for the Provision and Processing of Accepted Filings that Remain Outstanding (Including Filings Outstanding Since June 3, 2026), Encompassing, but Not Limited to, the Following:

1. Application Record (Unique Confirmation Number: 2026-06-03-1192357147322);
2. Memorandum of Fact and Law for the Judicial Review Application (Unique Confirmation Number: 2026-06-03-0007422788029);
3. June 3, 2026, Cover Letter (Unique Confirmation Number: 2026-06-03-8359215481736);
4. Notice of Motion in Writing (June 10, 2026) Documents (Unique Confirmation Number: 2026-06-10-0635652712965), comprising:
 - a. Final NOM #1 - McLean v. RCMP et al - Applicant - Moving Party - 10-June-2026 - DIG SIGNED - FILED.pdf;
 - b. Memo of Fact and Law - NOM 1 - McLean v. RCMP et al - Applicant - MP - KAM (BA JD CIM) - 10-June-2026 - FILED - DS.pdf;
 - c. Draft Order - NOM #1 - Applicant - McLean v. RCMP et al - 10-June-2026 - Final.pdf;
 - d. Cover Letter - McLean v. RCMP et al - NOM #1 - June 10 2026 - returnable June 17 2026 - Applicant.pdf;

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns

PART 1: INTRODUCTION

1. This correspondence is provided to the Registry of the Federal Court of Canada to facilitate the resubmission of a requisition for hearing (the "**Requisition for Hearing**"), and to systematically address the administrative assertions articulated in the correspondence transmitted by Mr. Tristan Mercieca on Tuesday, June 16, 2026.
2. It is confirmed that an initial requisition for hearing (the "**Initial Requisition for Hearing**") was formally submitted to the Federal Court of Canada on Friday, June 12, 2026. Concurrently, the prescribed statutory fee in the quantum of fifty dollars (\$50.00) was remitted, culminating in the generation of the unique confirmation number (the "**Confirmation Number**") 2026-06-12-5485328130686.
3. Following the aforementioned submission, correspondence was received from the Registry on Tuesday, June 16, 2026, wherein it was erroneously averred that the requisition for hearing (the "**Requisition for Hearing**") could not be accepted for filing. The justifications proffered for this refusal relied predominantly upon an administrative procedural chart, a purportedly omitted affidavit of service (the "**Affidavit of Service**"), and a mischaracterization of the proceeding as an application for leave (the "**Application for Leave**").
4. It is strictly maintained that the aforementioned administrative chart is inherently non-binding and cannot operate *ultra vires* the promulgated *Federal Courts Rules*. The trajectory of this proceeding is governed *strictissimi juris* by the statutory framework and the *Federal Courts Rules*, not by generalized administrative guidelines which fail to contemplate the absolute procedural default of respondents.

PART 2: THE NULLITY OF THE SERVICE REQUIREMENT IN THE CONTEXT OF ABSOLUTE DEFAULT

5. A fundamental error of law is evident in the Registry's directive mandating the provision of a proof of service (the "**Proof of Service**") prior to the acceptance of the requisition for hearing (the "**Requisition for Hearing**"). It is submitted that the imposition of a service requirement in direct contravention of *Rule 305* of the *Federal Courts Rules* constitutes a nullity rather than a mere procedural irregularity.
6. Specifically, the notice of application (the "**Notice of Application**") was formally issued on May 19, 2026, and subsequently served. Pursuant to *Rule 305*, the Respondents were strictly compelled to serve and file a notice of appearance (the "**Notice of Appearance**") within ten (10) days. The Respondents failed to execute this mandatory procedural step.
7. Consequently, by operation of law and pursuant to the explicit parameters of *Rule 305*, a respondent who has failed to file a notice of appearance (the "**Notice of Appearance**") is explicitly disentitled to

subsequent notice of any steps, is entirely deprived of the right to be served with further documentation, and is subject to the issuance of judgment in their absence. Thus, the Registry's demand for an affidavit of service (the "**Affidavit of Service**") upon parties who are unequivocally in default is a legal nullity *ab initio*. (*Nota bene*: It is anticipated that a counter-argument might be advanced suggesting that *Rule 314* necessitates the exhaustion of the temporal period allotted for the filing of a responding record prior to the submission of a requisition. This proposition is fundamentally flawed. Pursuant to the doctrine of *lex non cogit ad impossibilia*—the law does not compel the impossible—a timeline designated for a party in absolute default is vitiated *ab initio*. To mandate adherence to a lapsed procedural window belonging to a forfeited party constitutes a legal absurdity and offends the maxim *lex dilationes semper exhorret*, dictating that the law always abhors delays.)

PART 3: RECTIFICATION OF ADMINISTRATIVE MISCHARACTERIZATIONS

8. The assertion promulgated by the Registry that the documentation was submitted prematurely in the context of an application for leave (the "**Application for Leave**") is substantively and procedurally unfounded. The underlying proceeding is decidedly not an application for leave (the "**Application for Leave**"); rather, it is a substantive notice of application (the "**Notice of Application**") initiated under Part 5 of the *Federal Courts Rules*.
9. The notice of application (the "**Notice of Application**") was submitted on May 15, 2026, and formally issued on May 19, 2026. Concurrently, a rule 317 request (the "**Rule 317 Request**") was filed on May 19, 2026, and served upon the necessary parties. Both filings were comprehensively supported by an accepted certificate of service, encapsulated within the properly stamped and filed application record (the "**Application Record**") and motion record (the "**Motion Record**").
10. In parenthesis, it must be emphasized that the RCMP tribunal (the "**RCMP Tribunal**") has conspicuously failed to transmit any notice of objection or furnish the certified tribunal record (the "**Certified Tribunal Record**"). As a direct consequence of this delinquency, a notice of motion #1 (the "**NOM #1**") was scheduled to be adjudicated in writing on Wednesday, June 17, 2026. (*Nota bene*: Should it be posited that federal tribunals or Crown respondents are implicitly insulated from the strictures of *Rule 305*, such an assertion is definitively rebuffed by the doctrine of *expressio unius est exclusio alterius*—the expression of one is the exclusion of the other. The *Federal Courts Rules* delineate no jurisdictional carve-outs or sovereign immunities regarding the mandatory filing of appearances. The absolute default of the tribunal must, therefore, be treated with the identical procedural severity as that of a private litigant.)

PART 4: DECONSTRUCTION OF THE ADMINISTRATIVE CHART VIS-À-VIS THE FEDERAL COURTS RULES

- 691 11. Out of an abundance of caution, the administrative procedural chart repeatedly referenced by the Registry is hereby deconstructed and exhaustively correlated against the paramount statutory authority of the *Federal Courts Rules*. It is a bedrock principle of administrative law that informal policy directives, guidelines, or operational flowcharts cannot supersede, abrogate, or amend promulgated statutory instruments. To apply an administrative chart in a manner that contradicts the explicit text of the *Federal Courts Rules* is an exercise of authority that is plainly *ultra vires*. Consequently, this comparative analysis is provided to definitively demonstrate the unquestionable procedural propriety and *prima facie* validity of the present filing:
12. **Steps 1, 2, 3, and 5:** These preliminary jurisdictional thresholds were fully and unequivocally extinguished upon the formal filing, Registry acceptance, official issuance (perfected on May 19, 2026), and certified service of both the notice of application (the "**Notice of Application**") and the rule 317 request (the "**Rule 317 Request**"). By executing these foundational procedural maneuvers, the jurisdiction of the Federal Court was conclusively crystallized, thereby shifting the procedural onus onto the Respondents to engage with the judicial process in strict accordance with the prescribed statutory timelines.
13. **Step 4:** The mandatory requirement for the Respondents to serve and file a notice of appearance (the "**Notice of Appearance**") pursuant to the strictures of *Rule 305* and *Form 305* was fundamentally and irreversibly breached. This glaring omission renders this particular procedural step entirely moot and places the Respondents in a state of absolute legal default *ipso facto*. By voluntarily abstaining from this mandatory participatory prerequisite, the Respondents have effectively waived their entitlement to the protections afforded by the doctrine of *audi alteram partem*, extinguishing any subsequent rights to procedural fairness regarding ongoing notice or service of documentation.
14. **Step 6:** The RCMP tribunal (the "**RCMP Tribunal**") flagrantly violated the mandatory obligations stipulated within *Rule 318* by failing to transmit the required evidentiary materials and the certified tribunal record (the "**Certified Tribunal Record**") to both the Registry and the Applicant. This statutory contravention is not merely an administrative oversight but a substantive derogation of public duty that actively frustrates the supervisory jurisdiction of the Court. The presumption of regular administrative conduct (*omnia praesumuntur rite esse acta*) is thoroughly rebutted by this deliberate non-compliance, necessitating compelled judicial intervention.
15. **Step 7:** The procedural obligation to serve supporting affidavits is deemed exhaustively complete. The evidentiary foundation having been laid, a notice of motion #1 (the "**NOM #1**") was subsequently instituted and formally heard in writing on June 17, 2026. As delineated *supra*, the absolute and uncured default of the Respondents entirely negates any ongoing service obligations on the part of the Applicant. The evidentiary record submitted by the Applicant must therefore stand uncontroverted,

establishing a *prima facie* evidentiary basis upon which the Court is empowered to adjudicate the substantive matters.

16. **Steps 8 through 12:** The subsequent procedural machinations contemplated within these intermediate steps—encompassing adversarial cross-examinations, the reciprocal service of responding records, and interconnected evidentiary filings—are rendered utterly inapplicable, procedurally impossible, and legally irrelevant. It is a recognized tenet of judicial economy that the law does not compel the performance of futile acts. The Respondents' total failure to engage, synthesized with the Royal Canadian mounted police tribunal (the "**RCMP Tribunal**") default requiring direct judicial intervention, renders these sequential steps inert and functionally obsolete. The procedural landscape has, therefore, bypassed these adversarial mechanisms and advanced directly to the ultimate adjudicative stage.
17. **Step 13:** Predicated upon the exhaustive satisfaction of the Applicant's obligations and the default-induced nullification of all antecedent steps by the Respondents, the Applicant is unequivocally and statutorily entitled to file the requisition for hearing (the "**Requisition for Hearing**") utilizing *Form 314*. This entitlement crystallizes without any concomitant or vestigial obligation to effectuate service upon Respondents who are, *prima facie* and *de jure*, disentitled to receive it. To demand compliance with a service requirement against defaulting parties is an administrative overreach that fundamentally offends the principle of *dominus litis*. (*Nota bene*: It is further preemptively addressed that any reliance upon the technical parameters or mandatory data fields of the electronic filing portal—specifically, an unyielding software requirement for an uploaded proof of service—cannot supersede substantive legal rights. The doctrine of substance over form strictly dictates that an administrative or technological limitation cannot be weaponized as an *ultra vires* fetter on access to justice or operate in derogation of the statutory framework.)

PART 5: CONCLUSION AND RESUBMISSION

18. As a direct consequence of the preceding analysis, and in strict relation to both the *Federal Courts Rules* and the administrative chart provided by the Registry, it is unequivocally submitted that all mandatory procedural prerequisites incumbent upon the Applicant have been exhaustively fulfilled prior to the filing—without the necessity of service—of the requisition for hearing (the "**Requisition for Hearing**").
19. Notwithstanding the aforementioned jurisdictional and procedural legalities, it is conceded that a solitary, remediable defect existed within the initial requisition for hearing (the "**Initial Requisition for Hearing**"): the inadvertent omission of unavailable dates pursuant to *Rule 314*.
20. This minor procedural oversight has been meticulously rectified. That being said, it has been expressly denoted within the amended filing that the Applicant remains fully available on all prospective dates

693

within the ensuing ninety (90) day period (notwithstanding that the requested hearing is to be adjudicated in writing). The requisition for hearing (the "**Amended Requisition for Hearing**") is hereby resubmitted for immediate filing with this slight amendment properly effectuated.

21. Concurrently, an updated application record (the "**Application Record**") shall be transmitted subsequently to ensure the *status quo ante* is preserved. Furthermore, it is respectfully demanded that the outstanding filings delineated under Subject III, some of which have remained in abeyance since June 3, 2026, be immediately processed and accepted to formalize the Court's repository.
22. It is respectfully anticipated that this correspondence unequivocally clarifies the legal posture of the proceeding and that the enclosed requisition for hearing (the "**Amended Requisition for Hearing**") will be processed with the utmost expediency, restoring the administrative equilibrium and allowing the judiciary to function as *dominus litis*.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)

Enclosures

1. Resubmitted Requisition for Hearing of the Applicant (initial paid for and submitted for filing on June 12, 2026); and
2. Evidentiary Record in support of the same that addresses each and every issues contained in the email from Mr. Mercieca and the email generated response from the FCC (nota bene: there is no Application for Leave contained herein)

Requisition for Hearing — Application

Court File Number: T-2448-26

FEDERAL COURT

B E T W E N:

KEVIN A. MCLEAN

Applicant

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL,
AND STEPHANE BRISSON

Respondents

Requisition for Hearing

TO:

Manager of Court Operations/Judicial Administrator/Registrar of the Federal Court of Canada (City of Toronto)

180 Queen Street West,
Suite 200
Toronto, Ontario
M5V 3L6THE APPLICANT REQUESTS that a date be set for the **Hearing** of this **Application**.

THE APPLICANT CONFIRMS THAT:

1. The requirements of subsection 309(1) of the *Federal Courts Rules* have been complied with.
2. There is no requirement to serve a notice of constitutional question under section 57 of the *Federal Courts Act* in this application.
3. The hearing should be held at **Toronto, Ontario**.
4. The Applicant respectfully submits that the hearing of this unopposed (on account of none of the Respondents having served, filed, with proof of service, Notices of Appearances within ten days or at all (and not having

transmitted the requisite Certified Tribunal Record within 20 days of having been served (May 19, 2026) or having filed a notice of objection pursuant to Rule 318 of the Federal Courts Rules) Judicial Review Application (Form 301) (accepted as filed on May 15, 2026, and issued on May 19, 2026) should be scheduled for no more than two (2) hours (even notionally) but that the Application should be determined entirely in writing pursuant to *Rule 369* (without need for a duration of hearing), for the following reasons:

- a. The Respondents have not participated in this Proceeding, have not opposed the relief sought in the Judicial Review Application (served May 15, 2026), and have not objected to the Applicant's Rule 317 Request for materials in the possession of the RCMP, an "other tribunal" within the meaning of the *Federal Courts Act* and *Federal Courts Rules*. The issues raised are of **general public importance**, including:
 - (i) the proper scope of access rights under the *Privacy Act* and *Access to Information Act*;
 - (ii) the jurisdictional boundaries between federal administrative bodies;
 - (iii) the constitutional relationship between Parliament, provincial legislatures, and administrative decision-makers; and
 - (iv) core Rule of Law principles, including equality before the law, accountability, and access to justice.

The Rule of Law requires judicial intervention where administrative bodies adopt conflicting interpretations of their authority, as the legal system cannot tolerate operational conflicts or inconsistent orders. Uniformity, consistency, and the judiciary's "final word" on such matters are essential.

- b. Although the Federal Court is not subject to the statutory timelines imposed on provincial superior courts (e.g., *Courts of Justice Act*, s. 123), the Canadian Judicial Council's standards contemplate that decisions should be released within six months of being taken under reserve. It would be contrary to the public interest for such a timeline to apply where:
 - (i) the Respondents have not opposed the Application;
 - (ii) the Rule 317 Request is unopposed and unobjected to; and
 - (iii) the issues are novel, unprecedented, and of significant public importance.

A hearing date before the end of June 2026 ensures that the decision-making timeline is engaged and that these issues receive timely adjudication.

- c. The Applicant has requested that the motions judge assigned to Notice of Motion #1 (June 17, 2026) issue **Bottom-Line Orders** (Federal Courts Rules, s. 2) with reasons to follow, consistent with *Teskey*; *Cunningham*; *Children's Aid Society of Toronto v. K.(A.)*; *Law Society of Ontario v. Harrison*; and *Little Start Child Care Inc.* The Supreme Court of Canada has affirmed that justice may be best served by releasing the disposition promptly, with written reasons to follow. This principle applies with even greater force where a federal institution has not opposed the relief sought and where the underlying statutes (*Privacy Act* and *ATIA*) are quasi-constitutional in nature.
- d. The Ontario Court of Appeal in *R. v. Cunningham*, 2011 ONCA, held that reasons—even if released long after the disposition—are presumed to reflect the reasoning that led to the decision, and that there is **no**

legal time limit on the delivery of reasons. This reinforces the propriety of Bottom-Line Orders in matters of public importance.

- e. To ensure a binding, public, and authoritative decision that provides necessary jurisdictional boundaries and guidance, a hearing date must be set by the Judicial Administrator **before the end of June 2026**, prior to the Court's summer recess.
- f. Although judicial review requires the Court to apply the appropriate standard of review to each question, the Applicant—consistent with the principle of **dominus litis**—has structured the Application Record and Motion Record to facilitate an efficient written determination. The Applicant has filed a comprehensive, fully bookmarked and hyperlinked record addressing all relevant standards of review and legal issues.
- g. Judicial review is intended by Parliament and the Governor in Council to be a **summary procedure**, reinforced by Rule 3 of the *Federal Courts Rules*. Where Respondents do not oppose the relief sought, the Rules impose mandatory obligations:
 - (i) under Rule 305, a Respondent must file a Notice of Appearance within 10 days if it intends to oppose;
 - (ii) under Rule 318(2), a Respondent must object in writing, with reasons, if it opposes the production of materials requested under Rule 317.
 None of these mandatory steps have been taken.
- h. As conferences are not applicable to this Judicial Review Application as the Applicant has now filed a Requisition for Hearing in Form 314 before the expiry of the 180 day period (see: section 380(2) of the Federal Courts Rules) the Applicant submits that the Judicial Review Application should be scheduled for hearing on **June 29 or June 30, 2026**, together with the unopposed Rule 317 motion, to secure the **just, most expeditious, and least expensive** determination of this Proceeding, consistent with Rule 3 and the overarching interests of justice.
- i. The Applicant undertakes to be available on both days in full on a remote basis to appear via remote video technology should any oral submissions or clarifications to the written submitted and filed documents be required.

5. The representatives of all parties to the application are as follows:

- a. on behalf of the Applicant:
 - i. Mr. Kevin A. McLean (BA, JD, CIM)
 - ii. Pro Se (Self-Represented);
 - iii. 68 Abell Street, Toronto, ON M6J 0B1;
 - iv. Email: mclean@searchandseizure.ca
- b. on behalf of the Respondents:
 - i. Nil.

1. The Respondents failed to serve, file with proof of service, a Notice of Appearance pursuant to Rule 305 and are disentitled to the following:

- a. Notice of steps;
- b. Service of documents; and
- c. With knowledge that Judgment could be pronounced against them without their attendance (and such non-appearances by the Respondents have been bolstered and reaffirmed by the failure of the RCMP to have transmitted a Certified Tribunal Record within 20 days or at all, or a notice of objection within 20 days).

6. The party(ies) are available at any time except:

- a. The Applicant is fully available on the below dates to appear remotely should any oral submissions or clarification regarding written submissions along with any days within the 90 days (i.e. available on all days should any type of clarification or oral submissions be required).

- i. The Applicant respectfully requests a hearing date of **Tuesday, June 29, 2026** or **Wednesday, June 30, 2026**, to ensure the public interest issues are heard and decided, in writing, for the above noted reasons and those contained in the submitted documents for filing albeit which remains not confirmed as filed:

1. June 3, 2026:

- a. Application Record (Unique Confirmation Number: 2026-06-03-1192357147322);
- b. Memorandum of Fact and Law for the Judicial Review Application (Unique Confirmation Number: 2026-06-03-0007422788029);
- c. Cover Letter (Unique Confirmation Number: 2026-06-03-8359215481736);

2. June 10, 2026:

- a. Notice of Motion in Writing (June 10, 2026) Documents (Unique Confirmation Number: 2026-06-10-0635652712965), comprising:
 - i. Final NOM #1 - McLean v. RCMP et al - Applicant - Moving Party - 10-June-2026 - DIG SIGNED - FILED.pdf;

- ii. Memo of Fact and Law - NOM 1 - McLean v. RCMP et al - Applicant - MP
- KAM (BA JD CIM) - 10-June-2026 - FILED - DS.pdf;
- iii. Draft Order - NOM #1 - Applicant - McLean v. RCMP et al - 10-June-2026
- Final.pdf;
- iv. Cover Letter - McLean v. RCMP et al - NOM #1 - June 10 2026 - returnable
June 17 2026 - Applicant.pdf;

3. June 11, 2026:

- a. Motion Record (June 11, 2026) (Unique Confirmation Number: 2026-06-11-0960124814350).

b. Respondents:

- i. Not applicable due to failure to serve, file, with proof of service, Notices of Appearances within ten days of being served or at all

- 7. The hearing will be in **English**.
- 8. An interpreter will **not be required**.
- 9. The materials in the requisition for hearing file are in **English**.

The Applicant, with gratitude to the FCC (Toronto), and with great respect submits the following and certifies that it is true, accurate and complete:

DATED at Toronto, Ontario, this 19th day of June, 2026.



Mr. Kevin A. McLean (BA, JD, CIM)
68 Abell Street
Toronto, ON
M6J 0B1
email: mclean@searchandseizure.ca
Applicant (Self-Represented)

TO:

Nil (as per the above and the evidence contained in the Applicant's most recent Motion Record for NOM #1 of June 11, 2026)

[SOR/2021-151, s. 23](#)



 Print page

Your documents have been submitted to the Federal Court using the Electronic Filing System (E-Filing System).

Your document(s) and payment have been submitted to the Federal Court.

- You have submitted **1 document(s)** to the **Toronto Registry Office**.
- Your unique confirmation number for this submission is: **2026-06-12-5485328130686**.
- Date submitted: **06/12/2026 at 4:32:40 P.M. Eastern Time (ET)**.

Note that your submission will **only be considered filed** in Federal Court **after it has been examined, accepted and processed by the Registry**.

- [What's next](#)
- [Urgent matter](#)
- [Online access to documents](#)
- [Your submission](#)

What's next

You will receive an email from **noreply-nepasrepondre@cas-satj.gc.ca** with the unique confirmation number above.

Federal Court Registry personnel will review your submission and determine whether it can be accepted.

✓ Accepted document(s)

If your document(s) comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will accept and process your submission.
 - Your document(s) will be deemed as filed on the date and time of your submission to the E-Filing System, Eastern time (ET); unless you submitted on a Saturday, Sunday, or [holiday](#). If you submitted on a weekend or holiday, they will be deemed as filed on the next business day.
2. You will receive an email confirming that your document(s) have been accepted and filed. The email will include the Court File Number and a hyperlink to the stamped document(s).

✗ Non-accepted document(s)

If your document(s) do not comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will send you an email to inform you of the filing status and provide instructions for corrections.
2. Use the E-filing System and your unique confirmation number to submit the corrected document(s). The submission of a corrected document will not result in additional charges.
3. After you submit the corrected document(s) by email, they will be reviewed. The Registry will send you an email indicating whether or not the corrected documents have been accepted.
 - If you paid filing fees for document(s) that the Court did not accept for filing, you will receive a refund.

701

 Issues related to document type

If you selected the wrong document type(s) in the E-Filing System this may affect the applicable filing fee. The Federal Court Registry may contact you by phone or email for additional payment or a refund.

Urgent matter

If you have flagged your submission as urgent, please [contact the Registry](#). Submitting documents electronically does not guarantee that they will be reviewed immediately.

Online access to documents

If you have requested your submission be exempt from public online access, the documents mentioned will not be made available online until the Court makes a decision about your request and informs you.

► Your submission

Share your feedback

Take 5 minutes to help us improve our service.

Start survey

Start a new submission

About the Court

[Jurisdiction](#)

[Careers](#)

[Liaison Committees](#)

[Reports and Statistics](#)

Law and Practice

[Acts and Rules](#)

[Practice Guides](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Court Costs](#)

[Deadlines Calculator](#)

[Checklists](#)

Online Access

[Forms](#)

[E-Filing](#)

[E-Motion](#)

Representing Yourself

- [Finding Legal Help](#)
- [Practice Guides](#)
- [Procedural Charts](#)
- [Procedural Roadmaps](#)
- [Checklists](#)
- [Court Costs](#)
- [Deadlines Calculator](#)
- [Resolving Your Case](#)
- [Registry](#)

Court Files and Decisions

- [Court Files](#)
- [Decisions](#)
- [Hearing Lists](#)
- [General Sittings](#)
- [Summer Recess](#)
- [Calendar of Hearings](#)

Media

- [Administration of the Court](#)
- [Court Files](#)
- [Decisions](#)
- [Calendar of Hearings](#)

Resources

- [Registry](#)
- [Court Costs](#)
- [Procedural Charts](#)
- [Procedural Roadmaps](#)
- [Resolving Your Case](#)
- [Finding Legal Help](#)
- [Checklists](#)



Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Payment received – Submission Confirmation (Federal Court). Unique Confirmation number 2026-06-19-9957964156529 (T-2448-26)

1 message

noreply-nepasrepondre@cas-satj.gc.ca <noreply-nepasrepondre@cas-satj.gc.ca>

Fri, Jun 19, 2026 at 4:28 PM

To: mclean@searchandseizure.ca

Cc: mclean@searchandseizure.ca

This email confirms you have paid a filing fee associated with a proceeding in the Federal Court.

We value your feedback! If you have not already done so, [share your experience with Pay Now](#) in our quick survey.

Contact Information

First Name: Kevin

Last Name: McLean

Telephone Number: 6473709354

Email Address: mclean@searchandseizure.ca

Proceeding Information

Payment Reference Number: 4134494

Unique Confirmation Number: 2026-06-19-9957964156529

Court File Number: T-2448-26

Style of Cause: Kevin Alexander McLean v. Royal Canadian Mounted Police

Filing Party: KEVIN A MCLEAN

Document Type: Letter

Document File Name: Cover Letter - Outstanding Issues - RFHA - June 19-26.pdf

Online Access: Not Applicable

Filing Party: KEVIN A MCLEAN

Document Type: Requisition for Hearing - Application (\$50.00)

Document File Name: Form 314 - RFHA Applicant - 19-June-2026 - E-Sig.pdf

Online Access: Not Applicable

Payment Information

Transaction Date: June 19, 2026 at 04:23 PM ET

Authorization number: 665402670017411170

Amount Paid: \$50.00

Please do not respond to this email. This email address is automated and unattended, and cannot help with questions or requests.

Please contact the [Registry of the Federal Court](#).

TAB 21

Requisition of Hearing

4 messages

Mercieca, Tristan <Tristan.Mercieca@cas-satj.gc.ca>
To: "Mr. Kevin Alexander McLean" <mclean@searchandseizure.ca>

Tue, Jun 16, 2026 at 1:49 PM

Hello Applicant,

The Requisition for Hearing document you submitted to the Federal Court can not be accepted for filing at this moment. I am going to outline all of the reasons and next steps for you to follow.

First, I direct you to this chart →

[Application for Judicial Review - Federal Court](#)

This chart sets forth the order in which documents are to be filed and processed. This document comes last, you are jumping steps here.

Second, please amend the requisition of hearing form to comply with the rule 314. See here →

Contents of requisition

(2) A requisition referred to in subsection (1) shall

- (a) include a statement that the requirements of subsection 309(1) have been satisfied and that any notice required under section 57 of the Act has been given;
- (b) set out the place at which the hearing should be held;
- (c) set out the maximum number of hours or days required for the hearing;
- (d) list any dates within the following 90 days on which the parties are not available for a hearing;
- (e) set out the name, address, telephone number and fax number of the solicitor for every party to the application or, where a party is not represented by a solicitor, the person's name, address, telephone number and any fax number; and
- (f) indicate whether the hearing will be in English or French, or partly in English and partly in French, and whether the materials in the requisition for hearing file will be in English or French, or partly in English and partly in French.

Third

When submitting documents to the registry, you need to provide proof of service in the form of an affidavit of service that the Respondent has received a copy of the document being given.

Moving forward, as you have already paid for the requisition of hearing, you no longer need to do so in the future. When you eventually reach this step in the application process please reference this number 2026-06-12-5485328130686

Please review the chart I noted above and contact the registry regarding any questions or concerns regarding these procedures.

Regards,

Tristan Mercieca

Registry Officer | Agent du greffe

Courts Administration Service | Service administratif des tribunaux judiciaires

Federal Court: 416-973-3356 | Federal Court of Appeal: 416-952-8006

✉ Tristan.Mercieca@cas-satj.gc.ca



Courts Administration
Service

Service administratif des
tribunaux judiciaires

Canada

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>
To: "Mercieca, Tristan" <Tristan.Mercieca@cas-satj.gc.ca>

Tue, Jun 16, 2026 at 4:55 PM

Subject: RE: Requisition of Hearing — Court File No. T-2448-26 — McLean v. RCMP et al.

Dear Mr. Mercieca:

I confirm receipt of your email and thank you for your review. I respectfully disagree on an urgent basis and before five pm. Nonetheless I confirm my NOM #1 is to be heard in writing tomorrow regarding the Rule 317 Request. I will amplify my position, grounded in law and with the binding jurisprudence in support, but in the spirit of urgency, this is a quick summary.

While I appreciate the general operational flowchart provided, I must respectfully clarify that the *Federal Courts Rules* dictate a different procedural reality when a respondent is in absolute default. The Requisition for Hearing is procedurally ripe and compliant based on the following specific rules:

1. **Total Default of Appearance (Rule 305):** The Respondents were served with the Notice of Application on May 19, 2026. The 10-day statutory timeline under Rule 305 has long since expired. The Respondents have failed to file a Notice of Appearance.
2. **Absolute Exemption from Service (Rule 305):** Under Rule 305, a respondent who has not entered an appearance is *not entitled to notice of any subsequent steps or service of any subsequent documents* prior to final judgment. Frontline requirements for an Affidavit of Service are legally inapplicable here. The motion and the requisition proceed on an *ex parte* basis as a matter of law.
3. **Satisfaction of Rule 314 Timelines:** Rule 314(1) dictates that a requisition must be filed within 10 days after the expiration of the time for the respondent's record. Because the Respondents defaulted under Rule 305, their right to file a record never materialized and has structurally lapsed. Rule 309(1) has been fully satisfied by the Applicant.

707 4. **Pending Written Hearing Tomorrow (Rule 369):** My Motion Record (NOM #1) to compel the Certified Tribunal Record under Rule 318 was submitted via E-Filing under Confirmation Number 2026-06-11-0960124814350. Because the Respondents have no standing to respond, this motion is structurally ripe for *ex parte* judicial determination on my chosen written hearing date of **tomorrow, Wednesday, June 17, 2026**.

I have also filed supplementary **Written Representations based on Fresh Evidence** today to finalize the record.

I kindly request that my Rule 35 Requisition, Motion Record, the Form 314 Requisition for Hearing, and today's Written Representations be placed immediately before the Motions Judge for adjudication tomorrow morning under Rule 369.

Thank you for your assistance in processing these files to the judiciary.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)
68 Abell Street, Toronto
mclean@searchandseizure.ca

[Quoted text hidden]

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>
To: fc_reception_cf@cas-satj.gc.ca, Maggie.Lau@cas-satj.gc.ca, Todd.Desanti@cas-satj.gc.ca
Cc: "Mercieca, Tristan" <Tristan.Mercieca@cas-satj.gc.ca>

Fri, Jun 19, 2026 at 4:49 PM

Subject: *URGENT – Outstanding Filings and Resubmitted Requisition for Hearing (Court File No. T-2448-26)*

To:
Maggie.Lau@cas-satj.gc.ca; Todd.Desanti@cas-satj.gc.ca; Tristan.Mercieca@cas-satj.gc.ca; fc_reception_cf@cas-satj.gc.ca;

Dear Registry Officers,

I write further to my correspondence and filings in *Court File No. T-2448-26* to address the **urgent** status of several outstanding documents submitted for filing on **June 3, June 10, and June 11, 2026**, as well as the **resubmitted Requisition for Hearing - Application ("RFHA")** transmitted on **June 19, 2026** (Confirmation No. **2026-06-19-9957964156529**).

As detailed in the attached cover letter, the following filings—each submitted with valid confirmation numbers—remain unprocessed in the Court's electronic system:

- **Application Record** – Confirmation No. *2026-06-03-1192357147322*
- **Memorandum of Fact and Law** – Confirmation No. *2026-06-03-0007422788029*
- **Cover Letter** – Confirmation No. *2026-06-03-8359215481736*
- **Notice of Motion in Writing (June 10)** – Confirmation No. *2026-06-10-0635652712965*
- **Motion Record (June 11)** – Confirmation No. *2026-06-11-0960124814350*

These documents were accepted by the E-Filing System and assigned confirmation numbers, but they do not yet appear as processed or filed. Respectfully, had these filings been processed in the ordinary course, the concerns raised in Mr. Mercieca's June 16, 2026 email would not have arisen.

To avoid any further delay, I confirm that I am willing, **as a courtesy**, to provide the confirmation documents themselves by separate email for ease of reference.

708 Procedural Posture and Respondents' Absolute Default

For clarity, the Respondents:

- have **not served or filed a Form 305 Notice of Appearance** within the 10-day period mandated by **Rule 305**, or at all;
- have **not opposed the Judicial Review Application (Form 301)**;
- have **not objected** to the Rule 317 Request within the 20-day period mandated by **Rule 318**, or at all;
- have **not transmitted a Certified Tribunal Record**; and
- did **not oppose NOM #1**, which proceeded unopposed on **June 17, 2026**.

There is **no Application for Leave** in this proceeding. The reference to such a process in the June 16 correspondence is respectfully unclear, as the matter before the Court is a **substantive Judicial Review Application**, issued on **May 19, 2026**, supported by a Rule 317 Request and a complete Application Record.

Urgency and the Need for the Matter to Be Sub Judice Before Summer Recess

Given the nature of the issues raised—including matters of public importance, statutory interpretation, and the Respondents' complete procedural default—it is essential that the Requisition for Hearing be processed **no later than June 30, 2026**, such that the matter is formally **sub judice** and awaiting adjudication before the commencement of the Court's summer recess.

Kindly ensure that your records are reflected regarding the matters supra and by the referenced documents.

The amended Form 314 Requisition for Hearing was resubmitted on **June 19, 2026**. Because the E-Filing System would not permit resubmission using the original confirmation number, I paid the filing fee again to avoid any delay.

Requested Action

Accordingly, I respectfully request that the Registry:

1. **Process and formally accept** the outstanding filings submitted on June 3, 10, and 11, 2026;
2. **Confirm acceptance** of the Requisition for Hearing submitted June 19, 2026; and
3. **Update the Court file to reflect the complete procedural history**, as this will allow any future misapprehensions or misunderstandings to be avoided, given that **no notice of steps or service is required on the Respondents** and the **only outstanding obligations are those of the RCMP Tribunal under Rule 318**, which may be addressed by way of Order from the motions judge presiding over NOM #1.

I remain available at any time should clarification or further information be required.

Thank you for your attention to these urgent and outstanding matters.

Respectfully submitted,

Kevin A. McLean (BA, JD, CIM)

Applicant, Self-Represented

mclean@searchandseizure.ca

[Quoted text hidden]

3 attachments



Form 314 - RFHA Applicant - 19-June-2026 - E-Sig.pdf
231K



Cover Letter - Outstanding Issues - RFHA - June 19-26.pdf
2546K



FILING CONFIRMATION - June 19 2026 - Requisition for Hearing and Cover Letter - Applicant - Mr McLean -.pdf

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>
To: Maggie.Lau@cas-satj.gc.ca, Todd.Desanti@cas-satj.gc.ca

Mon, Jun 22, 2026 at 9:23 AM

Subject: RESPECTFULLY URGENT: Filing of additional documents (to be included in an updated and amended for current purposes Application Record (supplemental to the June 3, 2026, submitted Application Record) – Court File No. T-2448-26 (*McLean v. RCMP et al.*))

Dear Registry Officers Ms. Lau and Mr. Desanti,

I hope this email finds you well.

Please be advised that I have successfully transmitted the **Applicant's Supplementary Application Record** through the E-Filing portal this morning (Federal Co... p. 1).

- **Submission Timestamp:** June 22, 2026, at 9:08:47 AM ET (Federal Co... p. 1).
- **Portal Confirmation Number:** 2026-06-22-0652978947347 (Federal Co... p. 1).

Because this filing contains self-authenticating electronic business records under the *Canada Evidence Act* establishing critical institutional contradictions, it is entirely time-critical to my outstanding **Form 314 Requisition for Hearing** submitted on June 19, 2026 and on June 12 2026 (twice paid now).

As the Respondents remain in total default under Rule 305/308, this Proceeding proceeds on an entirely unopposed basis.

To ensure strict compliance with the Federal Courts Rules, I reproduce Rule 314:

"Requisition for hearing

314 (1) An applicant shall, within 10 days after service of the respondent's record or the expiration of the time for doing so, whichever is earlier, serve and file a requisition, in Form 314, requesting that a date be set for the hearing of the application"

As the Respondents were required to file a Notice of Appearance within 10 days after having been served on May 19, 2026, and the Respondent RCMP Tribunal was required to "transmit" the CTR by no later than 20 days after May 19, 2026 (June 10 2026 at the latest), I move expeditiously with my Requisition for Hearing Application on June 12, 2026. Moreover, within 10 days could not be any later than June 19, 2026.

I respectfully request that this package be synchronized and routed directly to the Judicial Administrator alongside my Form 314 paperwork to secure the final summary determination requested for **June 29 or June 30, 2026**, prior to the upcoming summer recess. This will be on an interim basis because I will provide in short order an updated

710 Application Record that will include the documents from the Motion Record (heard in writing on June 17, 2026) but nonetheless to assist out of respect for the public purse but the finite and valuable resources of the Federal Court of Canada.

The submitted for filing letter and the confirmation submission are attached for ease of reference and convenience all on an urgent basis in light of the mistaken, by Mr. Mercieca (without any castigation of him (nota bene: noting that the RCMP and some of the Respondents de facto are responsive in ATIA requests but not before the Federal Court of Canada in this Proceeding which provides self-evident conclusions (i.e. that the RCMP will participate in other arenas but not this one)) that the initially paid for Requisition For Hearing - Application could not be accepted at said time. Nonetheless, I made some minor housekeeping amendments to the same to ensure absolute and strict compliance (i.e. dates in which I would not be available).

Thank you for your continued diligence and vital assistance in managing this Proceeding. Should anything be unclear or require any response, please let me know. Otherwise, I will presume all is in order and the outstanding submitted filings will be processed accordingly and the either of the dates for a presumed in writing hearing (subject to the FCC Presiding Application Judge wishing to hear from me orally on a remote basis) are acceptable.

My update Application Record will follow to include this seminal and significant evidence so the Presiding Applications Judge has a full, true and accurate representation of the relevant documents, evidence and positions (de facto and de jure - however misapprehended and inconsistent (internally and externally)) at the time of Hearing (see: FCR, definitions).

Thank you kindly.

[Quoted text hidden]

2 attachments



Ltr - Head Registrar - Support - Urgent - Req Hearing App - Applicant - 22-June-26.pdf
2043K



Federal Court - Submission Confirmation - Letter with attachments (A to G) - June 22 2026.pdf
762K

TAB 22

712
Monday, June 22, 2026

TO:

Federal Court of Canada
Registry Office – Toronto Region

Physical address:

180 Queen Street West,
Suite 200
Toronto, Ontario
M5V 3L7

ATTENTION: JUDICIAL ADMINISTRATOR / MANAGER OF COURT OPERATIONS / REGISTRY OFFICERS (MS. MAGGIE LAU AND MR. TODD DESANTI)

File Number: Court File No.: T-2448-26
Short Style of Cause: *Kevin A. McLean v. Royal Canadian Mounted Police et al.*
Sender: Mr. Kevin A. McLean (BA, JD, CIM)
Sender's status: Applicant

URGENT STATUTORY NOTIFICATION, ADDITIONAL EVIDENCE (PROVIDED EXPEDITIOUSLY) REGARDING JOINDER OF INSTITUTIONAL BREACHES, AND EVIDENTIARY SUBMISSION OF FINAL ADMINISTRATIVE REFUSAL UNDER THE ATIA REQUEST #2

Dear Head Registrar Ms. Lau and Director of Operations Mr. Desanti,

1. I write regarding the above.
2. Please accept this correspondence for immediate electronic filing as the structural cover and legal foundation which *will be* the accompanying the Applicant's **Supplementary Application Record** in the within proceeding pursuant to applicable legal precedents underscoring the 1992 CanLII 57 (SCC)).
3. This urgent filing is made pursuant to the *Federal Courts Rules*, SOR/98-106, and sections 30 and 31.1 of the *Canada Evidence Act*, R.S.C. 1985, c. C-5, to permanently place a final, self-authenticating record of institutional default, statutory breach, and bad-faith administrative evasion directly before the reviewing Judge.
4. The Applicant confirms that this is an **urgent filing** designed to complete the uncontradicted evidentiary matrix and directly supplement the Applicant's existing Application Record to ensure the complete procedural layout of this file is *sub judice* prior to the proposed adjudication of this Application on **June 29 or June 30, 2026**, as set out in the Form 314 Requisition for Hearing resubmitted to your specific attention on June 19, 2026 (Confirmation No. 2026-06-19-9957964156529). For the explicit guidance of the Registry and the Judicial Administrator, the

INGESTION OF SELF-AUTHENTICATING ELECTRONIC BUSINESS RECORDS

5. The materials enclosed herewith are compiled systematically within this record (1992 CanLII 57 (SCC)). Pursuant to **sections 30 and 31.1 of the *Canada Evidence Act***, this comprehensive, unbroken communication corpus functions as a series of self-authenticating electronic documents originating directly from a federal institution.
6. Because these records consist of direct, unaltered electronic transmissions and formal letterheads exchanged between the Applicant and the Royal Canadian Mounted Police (“RCMP”) Access to Information and Privacy (“ATIP”) Branch, they require no supplementary affidavit text to be entered into the court record. This strategic architecture ensures that the uncontradicted documentary facts speak entirely for themselves, thereby rendering any cross-examination or dilatory mechanisms under the *Federal Courts Rules* wholly inapplicable to this uncontested file.
7. The unique additions incorporated into this Supplementary Record as of today’s date comprise three critical, interconnected digital artifacts:
 - a. **Tab A:** The Inbound Electronic Transmission from the RCMP ATIP Branch body corporate;
 - b. **Tab B:** The Formal *ATIA* Request #2 Response Letter executed by the RCMP ATIP Branch; and
 - c. **Tab C:** The Applicant’s Final Rejection Response transmitted directly to the Respondent this morning, June 22, 2026.

PART 2: THE CRITICAL STATUTORY DISTINCTION UNDER SECTION 10(1)(A) OF THE *ATIA*

8. The primary justification for this supplementary filing is the receipt of a formal response correspondence from the RCMP ATIP Branch dated **June 18, 2026 (File No.: A-2026-01933)**, signed by Director Curtis Mathews, which has been entered at **Tab B**. In this correspondence, the Respondent asserts that a multi-branch corporate search was executed across Corporate Management, National Specialized Services, and the Digital Program, and declares that the RCMP is “**unable to locate records**” regarding the procurement, licensing, and lifecycle logs of the GrapeCity/MESCIUS SDK software footprint.
9. The Applicant explicitly alerts this Honourable Court to a profound, bad-faith statutory defect embedded within this administrative refusal. Parliament has strictly mandated under **Section 10(1)(a) of the *Access to Information Act (ATIA)*** that when access to a record is refused, the head of the institution must categorically state that the record “**does not exist**”. Director Mathews’ correspondence conspicuously shifts and mutates this mandatory terminology, stating only that the RCMP was “*unable to locate records*”.
10. This underscores the prerogative writ relief sought in the nature of mandamus and provides further uncontested and self-evident evidence in relation to the same albeit under the *ATIA* Request #2 (see: Judicial Review Application

11. As you also know, the RCMP, which meets the definition of a “Tribunal” or “Other Tribunal” under the Federal Courts Rules and Federal Courts Act has failed to transmit a Certified Tribunal Record (or “CTR”) within 20 days of service which occurred on May 19, 2026.
12. There is an absolute, immutable legal distinction between an administrative assertion that a record *does not exist* and an admission that an institution is *unable to find it* or “unable to locate the Records (see: *ATIA*, definitions)”. I pause to fully grasp that statement, yet again, “unable to locate the Records”.
13. I will, in the interim, denote for ease of preparation for the Hearing of the Application, by way of the now twice paid “Requisition for Hearing – Application” that under *ATIA* Request #1 from mid April 2026 (see: Application Record (June 3, 2026), Tab 9; Motion Record (June 11, 2026), Tab 13) that one Ms. Tina Beaudoin (another “director” of the RCMP ATIP Branch albeit on her LinkedIn profile, she has represented herself to be a “team leader” on a national level) that the *ATIA* Request #1 is in retrieval phase.
14. By formally stating that it cannot find the requested records, the RCMP has legally admitted to a deficient, blind, or wholly inadequate search methodology. Consequently, this failure to issue a valid statutory notice under Section 10(1) triggers an immediate, unextended **Deemed Refusal under Section 10(3)** of the *ATIA*.

PART 3: STRUCTURAL IRRECONCILABILITY AND BREACH OF THE DUTY TO ASSIST

15. This “unable to locate records” determination represents a severe, bad-faith breach of the RCMP’s non-discretionary statutory obligations under **Section 4(1) and Section 4(2.1) of the *ATIA***. The statutory “Duty to Assist” codifies a rigorous, initiative-taking mandate requiring the head of a federal institution to make *every reasonable effort* to respond accurately and completely.
16. As detailed exhaustively in the original request parameters dating back to **May 5, 2026**, the **GrapeCity.Documents for PDF v. 6.0.2.0** engine leaves undeniable, permanent, machine-readable digital traces (including Fast Web View linearization protocols, raw legacy %PDF-1.3 header forcing anomalies, and custom Adobe XMP Core 9.1 toolkits) on the underlying files.
17. For an enterprise-level federal law enforcement ecosystem operating under modern Treasury Board cloud guardrails and multi-million-dollar modernizations, asserting that a thorough search yielded zero licensing agreements, value-added reseller expenditure approvals, security matrices, or system lifecycle tickets for software currently embedding its literal cryptographic footprint onto active police records is a structural and mathematical impossibility. It stands as objective proof of an intentional failure to comply with the Act.

PART 4: A DOCUMENTED HISTORY OF EXECUTIVE AND CORPORATE NOTICE

715 18. This supplementary record conclusively demonstrates that the RCMP's institutional silence is not the result of an administrative oversight, but rather a coordinated campaign of evasion. The chronological chain within **Tab A** and **Tab C** locks in actual, corporate notice to the highest echelons of senior command:

- a. **May 11, 2026:** The RCMP ATIP Branch issued a boilerplate acknowledgment stating it was “currently proceeding” but failed to articulate valid statutory grounds or a definitive duration under Section 9(1). Per the Federal Court of Appeal's binding decision in *Statham v. CBC*, the failure to statutorily notify an applicant of the precise grounds for an extension renders any processing delay an absolute nullity *ab initio*.
- b. **June 8, 2026:** Upon the expiration of the un-extended 30-day statutory window, the Applicant served a formal Notification of Statutory Non-Compliance, establishing the crystallization of an absolute deemed refusal.
- c. **June 10, 2026:** Explicit electronic notice of this ongoing statutory delinquency and a formal inquiry regarding the notification of the Information Commissioner under Section 9(2) were served directly to **RCMP Commissioner Michael Duheme, Director General Mr. Stephane Brisson, and Deputy Commissioner Bryan Larkin** (acting with full executive authority during the Commissioner's concurrent absence on duty).

TAB 5: INGESTION OF TAB D, E, F, AND G: UNASSAILABLE STRUCTURAL CONTRADICTIONS BETWEEN THE PRIVACY ACT REQUEST AND ATIA REQUESTS #1 AND #2

19. The Applicant added to the enclosed record to feature four distinct alphabetical units (**Tabs D, E, F, and G**) comprising the unbroken, interlocking statutory history of this dispute. Pursuant to **sections 30 and 31.1 of the Canada Evidence Act**, these direct institutional artifacts function as self-authenticating, uncontradicted electronic proof of an irreconcilable operational paradox and systemic bad faith orchestrated by the Respondent's ATIP directorate:

- a. **Tab D (Privacy Act Request, March 8, 2026):** Documents the Respondent's threshold administrative refusal, cross-referencing active contentions from the interlocutory Motion Record wherein Director Jeff Ball explicitly asserted that the Respondent was not statutorily entitled or technologically required to search the backend mainframe architecture (Tab A to G... pp. 8, 14);
- b. **Tab E (ATIA Request #1, April 14, 2026):** Establishes the concurrent, targeted corporate infrastructure requisition tracking the underlying CPIC transaction logs and system architecture data ledger fields (Tab A to G... pp. 18, 41);
- c. **Tab F (ATIA Request #2 Response, June 18, 2026):** Contains Director Curtis Mathews' defective notice asserting the RCMP is '*unable to locate records*' regarding the GrapeCity/MESCIUS SDK procurement footprints (Tab A to G... pp. 5, 7); and
- d. **Tab G (ATIA Request #1 Status Email, June 16, 2026):** Features the formal transmission from Team Leader Tina Beaudoin confirming that the antecedent infrastructure records are actively situated within the '*retrieval stage*' (Tab A to G... pp. 41-42).

- 716
20. The Applicant submits that this expanding administrative matrix is completely incoherent, logically irreconcilable, and fatal to the Respondent's legal credibility. It is factually and *de jure* unsustainable for Director Curtis Mathews to formally certify to the Applicant on June 18, 2026 (**Tab F**), that an exhaustive multi-branch search across National Specialized Services and the Digital Program yielded absolutely zero records (Tab A to G... pp. 5, 7), while Team Leader Tina Beaudoin maintained a formal, active representation on June 16, 2026 (**Tab G**), that those identical technical infrastructure logs are actively being processed and collected within the '*retrieval stage*' (Tab A to G... pp. 41-42). An institution cannot logically spend weeks actively gathering a specific technical file while simultaneously certifying that the target files do not exist within their systems.
21. Furthermore, this exposure completely strips the Respondent of its foundational shielding defense advanced under the *Privacy Act* stream (**Tab D**). In the underlying Motion Record, the Respondent—via Director Jeff Ball—vehemently contended that the Applicant maintained zero entitlement to an infrastructure search, asserting a sweeping, baseline defense that the Foundational Metadata, the Offline Historical Database, and the overarching Personal Information Bank (**PIB RCMP PPU 005**) were entirely unsearchable and legally remote from the ATIP branch's extraction duties (Tab A to G... pp. 11, 14).
22. However, by subsequently placing the identical infrastructure parameters of **ATIA Request #1** into an active "retrieval stage" (**Tab G**), the Respondent has generated an impossible institutional contradiction (Tab A to G... pp. 41-42). The active retrieval status ledger entries executed by Ms. Beaudoin operate as a formal, binding concession that these precise database logs exist, are fully searchable, and are readily accessible for administrative processing (Tab A to G... pp. 41-42). The RCMP cannot plead technological incapacity and a complete inability to search the Personal Information Bank to block a *Privacy Act* correction application, while simultaneously extracting those exact structural mainframe rows under an active *Access to Information Act* file.
23. This flagrant, documented conflict, which is inconsistent on its face (pardon the pun in light of the False Information Package that was filed at a transferee courthouse of OCJ 10 Armoury Street Courthouse (the "Transferee Courthouse") removes any residual doubt regarding the absolute urgency of this Application. It proves that the RCMP's shifting positions are an artificial visual smokescreen engineered solely to prevent judicial oversight of its backend CPIC data-manipulation frameworks. A final, binding **Court Orders to Compel** remains the singular mechanism to pierce this institutional stonewalling and extract the true, unmanipulated Certified Tribunal Record before the upcoming summer recess which can be accomplished with the Hearing of the Judicial Review Application being under sub judice with the ancillary relief involving leave to the Applicant to address the same.

PART 6: CONSOLIDATION OF EVIDENCE, DOCUMENTS ET AL FOR THE JUNE 29 OR 30 SUMMARY ADJUDICATION

- 717** 24. To prevent the fragmentation of legal resources, avoid cross-cutting jurisdictions, and block the Crown from deploying the “adequate alternative remedy” trap, the Applicant has elected **not** to lodge an administrative complaint with the Office of the Information Commissioner at this stage. Instead, this profound administrative default is being consolidated exclusively within this judicial review proceeding to allow for an immediate, unified resolution.
25. The Respondents have completely failed to file a Notice of Appearance within the mandatory 10-day window under **Rule 305**, they have failed to transmit the Certified Tribunal Record within the 20-day window under **Rule 318(1)**, and they have failed to lodge a formal written objection under **Rule 318(2)**. Pursuant to **Rule 308**, they are formally disentitled to notice of any steps or service of any documents, having completely waived their right to oppose this Application on the merits.
26. The uncontradicted digital evidence and the self-authenticating business records contained within this Supplementary Application Record establish that the RCMP is actively withholding essential metadata to shield its backend CPIC data-manipulation frameworks from judicial review. The Court retains full summary jurisdiction under **Sections 49 and 50** of the Act to look past these administrative denials, draw the necessary adverse inferences from the RCMP’s silence, and issue immediate, binding orders to produce.
27. This urgent filing completes the supplementary evidentiary substrate. The Applicant confirms that his primary Application Record is being amended and supplemented accordingly to reflect these critical additions. The Applicant respectfully requests that the Registry immediately route these materials directly to the Judicial Administrator to ensure they are synchronized with the Form 314 Requisition for the final summary hearing on **June 29 or June 30, 2026**.
28. Again, I wish to note in relation to those dates, I appreciate that once my Judicial Review Application (Form 301) is sub judice, there may be follow up clarifications or questions from the Federal Court of Canada. To the extent that the Federal Court of Canada wishes to hear from orally, I can be present remotely via videoconference on June 30, 2026. Kindly advise if that will be necessary and I can reserve a private and confidential office for the same.
29. As per the above, the Respondents, although having received notice of the same through the *ATIA* Request #2, are not entitled to be served with any documents until they have sought and obtained leave to serve, file, with proof of service a Form 305.
30. Thank you for your continued diligence and prompt attention to the processing of these time-sensitive materials.
31. I extend my gratitude for the administrative processing of the outstanding submitted for filing documents, which were not rejected or “not accepted” and of which there was no notice to me like there was my initial Form 301 Application¹, so that the Record Of Proceeding herein is complete, true and accurate.
32. I shall work diligently to ensure all materials, documents, evidence and submissions are perfectly calibrated and organized for either June 29 or 30 of next week as I appreciate the public purse and the finite resources of the Federal Court of Canada.

33. Thank you kindly in advance for your anticipated compliance.

718

Yours truly,

A handwritten signature in black ink, appearing to read 'Kevin A. McLean', with a stylized flourish at the end.

Mr. Kevin A. McLean (BA, JD, CIM)

Applicant (Self-Represented)

68 Abell Street (Receptionist desk)

Toronto, Ontario M6J 0B1

Email: mclean@searchandseizure.ca

Enclosures (Tab A to G of the foregoing particularized documents)

ⁱWhich was on account of the Federal Court of Canada's (Toronto Court Office) position that it was too lengthy.

Tab A

Access to Information Request A-2026-01933 / F320 - Response

1 message

ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>
To: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Thu, Jun 18, 2026 at 9:07 AM

Good day,

Please find attached our office's response to your *Access to Information Act* request A-2026-01933.

Regards,

Kyra Beauregard-Briscoe

ATIP-AIPRP@rcmp-grc.gc.ca

RCMP's Access to Information and Privacy Branch (ATIP) | Accès à l'information et de la protection des renseignements personnels de la GRC (AIPRP)

ATIP Intake Unit | Unité de traitement AIPRP

73 Leikin Drive | [73 promenade Leikin](#)

Mailstop #61 | Boîte postale 61

Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'aviser immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

 **A-2026-01933 - Response.pdf**
164K

Tab B



June 18, 2026

Kevin McLean
68 Abell Street
Toronto, Ontario M6J 0B1

Dear Kevin McLean:

This is in response to your request under the *Access to Information Act*, which was received by this office on May 8, 2026, to obtain:

SUBJECT: Formal request under the ATIA - software procurement, licensing, NTOP onboarding, embedded IT architecture, and azure cloud utilization records (GrapeCity / MESCIUS SDKs (Software Development Kit))

This request is strictly focused on objective, administrative, and technological procurement data regarding specific enterprise-grade software capabilities deployed within the federal law enforcement Information Technology (IT) ecosystem, specifically intersecting with the RCMP's "Cloud-First" regulatory framework and backend server-side document manipulation infrastructure.

I am formally requesting access to the following specific classes of records under the control of the RCMP, encompassing the comprehensive timeframe of January 1, 2018, to the present date (May 8, 2026):

a. Indirect and Direct Procurement/Licensing Records: Any and all records, including purchase orders, end-user licensing agreements (EULAs), vendor contracts, invoices, expenditure approvals, Software Licensing Supply Arrangement (SLSA) call-ups, or budgetary line items demonstrating that the RCMP (or SSC on behalf of the RCMP) has purchased, licensed, or procured GrapeCity/MESCIUS Software Development Kits (SDKs) and/or API access, either directly from the developer or via third-party resellers (e.g., Insight Canada, Softchoice, ComponentSource).

b. NTOP Onboarding and Compliance Records: All records, matrices, and security evaluations generated by the National Technology Onboarding Program (NTOP) regarding the approval, rejection, or conditional use of MESCIUS/GrapeCity developer tools. This must include any GC Cloud Guardrail compliance checks and data residency agreements executed to permit this software to interact with Protected B data on Microsoft Azure servers.

c. Embedded IT Architecture, Server-Side Integration, and Mega-Project Logs: Any internal software architecture diagrams, deployment records, backend integration scripts, vendor technical specifications, or embedded library logs specifically related to

the Microsoft 365/SharePoint Migration, the CFDSS (Accenture), the Axon DEMS projects, or the "Internal Solution" data silo, indicating that GrapeCity/MESCIUS PDF manipulation tools, SpreadJS, ActiveReports, Document APIs, or .NET/JavaScript grids are embedded within these server-side systems.

d. Software Lifecycle and Version Control Logs: Any IT change-management logs, update tickets, developer requisition forms, or system administration records documenting the installation, upgrading, deprecation, or patching of GrapeCity.Document.PDF (specifically referencing version 6.0.2.0 or subsequent iterations) within the RCMP network, developer workstations, or CPIC-interfacing servers.

e. User Manuals, Document Integrity Protocols, and Internal Directives: Any internal training materials, IT support tickets, developer manuals, Threat Risk Assessments (TRAs), or administrative directives referencing the utilization of GrapeCity or MESCIUS SDKs for the specific operational purposes of automated backend document creation, programmatic PDF generation, headless PDF redaction, algorithmic document alteration, or metadata manipulation by RCMP personnel or contracted developers. Consistent with the OPC's 2023-2024 directives to Parliament, this explicitly includes any Privacy Impact Assessments (PIAs) conducted to validate the use of these tools against public privacy rights.

Based on the information provided, a search for records was conducted with **Corporate Management, National Specialized Services, the Digital Program and the Access to Information and Privacy Branch's Privacy Management Division**. Unfortunately, we were unable to locate records which respond to your request.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:
<https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, you may contact Kyra Beauregard-Briscoe at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this letter.

Regards,



For/ Curtis Mathews, Director, Access to Information
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

Tab C

Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Mr. Kevin McLean <mcleansettlement@gmail.com>

To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>, "Duheme, Michael (RCMP/GRC)" <Michael.Duheme@rcmp-grc.gc.ca>, "Brisson, Stéphane (RCMP/GRC)" <stephane.brisson@rcmp-grc.gc.ca>, "Ball, Jeff (RCMP/GRC)" <Jeff.ball@rcmp-grc.gc.ca>
Cc: mclean@searchandseizure.ca

Date: June 22, 2026

Subject: RE: Formal Request under the ATIA - File No: A-2026-01933 (GrapeCity / MESCIUS SDK Procurement & Lifecycle Architecture)

CC:

Commissioner Michael Duheme (Michael.Duheme@rcmp-grc.gc.ca)

Deputy Commissioner Bryan Larkin (Bryan.Larkin@rcmp-grc.gc.ca)

Director General Mr. Stéphane Brisson (Stephane.Brisson@rcmp-grc.gc.ca)

Director, ATIP Branch of the RCMP, Mr. Curtis Matthews (Curtis.Matthews@rcmp-grc.gc.ca)

Director, Mr. Jeff Ball

SUBJECT: RESPONSE TO A-2026-01933 / F281

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I am in receipt of your correspondence dated June 18, 2026, signed by Director Curtis Mathews, asserting that a search was conducted and that the Royal Canadian Mount responding to my targeted procurement request (A-2026-019... p. 1).

Please consider this transmission formal notification that the Applicant rejects this determination as a severe, bad-faith breach of the RCMP's explicit statutory obligations A-1 (the "Act") (RSC 1985, ... p. 1). The RCMP's position is non-compliant on the face of the statutory text, as detailed below:

1. DEFECTIVE NOTICE AND THE SECTION 10(1)(A) DISTINCTION

Parliament has strictly mandated under **Section 10(1)(a)** of the Act that when access is refused, the head of the institution must explicitly state that the record "**does not ex** correspondence conspicuously shifts this language, stating only that the RCMP was "**unable to locate records**" (A-2026-019... p. 2).

There is an absolute, immutable legal distinction between a record *not existing* and an institution being *unable to find it*. By admitting that you simply cannot find the reco: 2026-019... p. 2). This failure to issue a valid statutory notice under Section 10(1) triggers an immediate **Deemed Refusal under Section 10(3)** of the Act (RSC 1985, ... p

2. BREACH OF SECTION 4(1) AND SECTION 4(2.1) (THE DUTY TO ASSIST)

The statutory mandate places a strict, non-discretionary duty on the head of the institution to make *every reasonable effort* to assist a requester and to respond *accurately a* original **May 5, 2026 Request, the GrapeCity.Documents for PDF v. 6.0.2.0** engine leaves undeniable, machine-readable digital traces (including Fast Web View lineari: (Gmail - AT... pp. 3-4).

Asserting that zero procurement contracts, software licensing supply arrangement (SLSA) call-ups, change-management tickets, or National Technology Onboarding Prog currently embedded within your backend architecture is a structural impossibility (Gmail - AT... p. 7). It represents a fatal failure of the mandatory duty to assist (RSC 198

3. CHRONOLOGICAL RECORD OF CORPORATE AWARENESS

Senior executive command possesses documented, actual notice of this statutory delinquency, eliminating any defense of administrative oversight:

- **May 5, 2026:** The formal, multi-tiered ATIA request was validly submitted to the RCMP ATIP Branch (Gmail - AT... p. 1).
- **May 11, 2026:** Your office issued a boilerplate acknowledgment ("currently proceeding") that failed to cite specific statutory grounds or a definitive duration under nullity *ab initio* under *Statham v. CBC* (Gmail - Ac... pp. 1-2).
- **June 8, 2026:** Upon the crystallization of your un-extended statutory deadline, I served a formal Notification of Statutory Non-Compliance establishing your state o
- **June 10, 2026:** Explicit notice of this ongoing delinquency was served directly to Commissioner Duheme, DG Brisson, and Acting Commissioner Deputy Commiss

4. DIRECT FEDERAL COURT ESCALATION AND STATUTORY STRATEGY

To prevent the fragmentation of legal resources and avoid crossing up jurisdictions, **I will not be lodging at this time an administrative complaint with the Office of th this stage** (RSC 1985, ... p. 25).

Instead, because the RCMP's administrative failure to locate its own procurement data stands in direct contradiction to the objective forensic metadata, **this entire commu request, the May 11 non-compliant acknowledgment, the June 8 crystallization notice, and your June 18 refusal—is being filed directly into the Federal Court of Supplementary Application Record in Court File No. T-2448-26.** (Gmail - AT... p. 1, Gmail - Ac... pp. 1, 9, A-2026-019... p. 1)

Pursuant to **Sections 30 and 31.1 of the Canada Evidence Act**, these direct electronic communications from the RCMP ATIP Branch function as self-authenticating, uncor supplementary affidavit text to be entered into the record, thereby rendering any cross-examination mechanisms under the *Federal Courts Rules* wholly inapplicable.

726 Subjective, institutional record will be deployed as a primary evidentiary anchor for my upcoming Hearing (see: Federal Courts Rules, section 2) of my Application (see: [my Application](#)). I request that you past your administrative denials under Sections 49 and 50 and issue an immediate order to conduct yet another search and then produce to avoid a multiplicity of hearings. Justice delayed is justice denied.

In my view, this is a complete breakdown of government which underscores why the hearing of my unopposed and uncontested by the non-appearing Respondents in my Judgment is the month as per my paid for "Requisition for Hearing – Application". This serves as formal notice that I reserve the right to rely upon this correspondence for any lawful judgment and information technology systems.

Thank you.

Be guided accordingly.

Sincerely,

Mr. Kevin A. McLean (BA, JD, CIM)

On Wed, Jun 10, 2026 at 4:35 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:
Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I received the auto-reply from Mr. Duheme as per the Appendix. As such, Mr. Larkin is copied (see: Bryan.Larkin@rcmp-grc.gc.ca).

Appendix

Automatic reply: Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Duheme, Michael (RCMP/GRC)
to me

Prenez note que je serai absent en devoir à compter du 21 mai au 19 juin. Sous Commissaire Bryan Larkin agira à titre de Commissaire par intérim. Vous pouvez le rejoindre à [Bryan.La](mailto:Bryan.Larkin@rcmp-grc.gc.ca)

The 21st May to 19 June, I will be away on duty , Deputy Commissioner Bryan Larkin will be the acting Commissioner. He can be reached at Bryan.Larkin@rcmp-grc.gc.ca

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)
Chartered Investment Manager
Email: mcleansettlement@gmail.com
Fax: 416.981.7117
Phone number: 647.370.9354

On Wed, Jun 10, 2026 at 4:31 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:
Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I am copying the following to this email for self-evident reasons:

1. RCMP Commissioner Mr. Duheme; and
2. Director General Mr. Brisson

I will follow up more formally for the Head of the Institution and the chief privacy officer of the RCMP with a summary of status et al. However, in the interim, would Information Commissioner of Canada of your purposed extension of time?

Thank you.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Tab D

PRIVATE AND CONFIDENTIAL

DATE: February 27, 2026

DELIVERY METHOD: Via MAIL

TO: Royal Canadian Mounted Police Access to Information and Privacy Branch
73 Leikin Drive, Mail Stop #61

Ottawa, Ontario

K1A 0R2

SUBJECT I: Statutory Request for Access to Personal Information under the *Privacy Act* (Canada)

SUBJECT II: Exaction of Canadian Police Information Centre Metadata Pertaining to the Promulgation of Judicial Authorizations and Concomitant Arrest Warrants

SUBJECT III: Formal Demand for the Production of Offline Historical Database Audit Trails, Transaction Logs, Originating Agency Identifiers, and Systemic Non-Repudiation Artifacts

Dear Sirs/Mesdames:

I. INTRODUCTION, CONTEXTUAL FRAMEWORK, AND QUASI-CONSTITUTIONAL IMPERATIVES

1. Correspondence is heretofore initiated with respect to the aforementioned matters, wherein the immediate, unmitigated, and comprehensive exaction of specified forensic metadata archived within the digital and physical federal repositories is sought. The present requisition is advanced not as a routine administrative issue, nor as a peripheral, academic, or vexatious pursuit of archival data, but rather as a fundamental, paramount, and non-derogable exercise of quasi-constitutional entitlements. The exaction of these records is an indispensable prerequisite for the vindication of rights that reside at the very core of the *lex terrae*, serving as the only viable mechanism to restore the *status quo ante* in the face of systemic administrative failure, technological vitiation, and jurisdictional overreach.
2. Reliance is unequivocally placed upon the established and binding jurisprudence, notably *Dagg v Canada (Minister of Finance)*, 1997 2 SCR 403 (the "**Dagg**") at para 61, wherein the quasi-constitutional status of access rights is unambiguously affirmed by the Supreme Court of Canada. These statutory entitlements are specifically engineered, deliberately constructed, and statutorily enshrined such that the citizenry is empowered to scrutinize, challenge, and definitively rectify the purported deployment of vitiated judicial instruments—*acta* which have facilitated a profound, potentially *ultra vires* deprivation of physical liberty. The right of access is not a mere procedural adjunct; it is a substantive pillar of democratic accountability designed to prevent the state from operating in a vacuum of unreviewable discretion, thereby mitigating the profound democratic deficit inherent in clandestine law enforcement databases.
3. The contravention of these strictures constitutes an **Irremediable Nullity** which vitiates the law of the land and obviates any pretense of lawful detention, rendering the actions of the state functionally indistinguishable from arbitrary coercion and unlawful confinement. It is posited that the structural integrity, procedural fairness, and moral authority of the Canadian criminal justice system are inextricably tethered to the absolute accuracy, verifiable provenance, and jurisdictional legitimacy of the administrative records that authorize state coercion. A justice system that operates upon the basis of fraudulent or "metamorphosed" digital records is one that has abandoned the rule of law in favour of systemic expediency, effectively rendering the *Canadian Charter of Rights and Freedoms* (the "**Charter**") a series of hollow platitudes rather than a living instrument of protection.
4. The federal government, acting as the ultimate steward, architect, and host of the paramount law enforcement database, bears the ultimate, inescapable, and non-delegable burden of ensuring this requisite transparency is maintained. Consequently, the demand for absolute, unvarnished transparency regarding the systemic inception, precise digital timestamping, and exact geographical origin of these judicial authorizations constitutes a foundational democratic imperative. The state cannot wield the ultimate sword of physical arrest while simultaneously cloaking the shield of administrative accountability in bureaucratic darkness, as the lack of transparency invites the very corruption and documentary "metamorphosis" that the *Privacy Act* (the "**Privacy Act**") was designed to illuminate and rectify.

5. Furthermore, the complex intersection of federal informational control and provincial criminal administration mandates an extraordinarily rigorous standard of hygiene for all digital entries that precipitate a physical deprivation of liberty. A warrant is not merely an administrative convenience or a digital flag; it is a profound constitutional mechanism that overrides the fundamental freedom of movement. It is respectfully submitted that an arrest effectuated upon a digitally manipulated, retroactively generated, or deliberately post-dated warrant is legally and constitutionally indistinguishable from an arbitrary kidnapping perpetrated under the colour of right. The validity of such an instrument is contingent upon its temporal and jurisdictional accuracy, both of which are currently subjected to intense forensic scrutiny due to the discovery of irreconcilable internal contradictions within the municipal paper trail.
6. Appended hereto are the ensuing documents, submitted for the concomitant purposes delineated herein, and specifically calibrated to facilitate the expeditious processing of this statutory requisition while proactively circumventing any preliminary institutional requests for supplementary identity verification or procedural obfuscation:
 - a. A reproduction of the Canadian passport pertaining to Kevin A. McLean (the "**Applicant**"), provided exclusively for the strict circumscription of identity verification and the absolute, preemptive satisfaction of all legislative authentication thresholds mandated by the institution's internal administrative directives. This enclosure serves to extinguish any preliminary jurisdictional or standing-based objections *in limine* and ensures that the institution cannot rely upon identity-based prevarication to delay the thirty-day statutory response window.
 - b. A reproduction of the vitiated information package and associated documentation (the "**False Information Package**"). In a spirit of profound cooperation and *bona fides*, this document is enclosed to explicitly demonstrate the imperative necessity for the exhaustive nature of the present statutory requisition. It is noted with immense legal gravity that the fraudulent character of this document has been corroborated by the Ministry of the Attorney General, specifically by counsel situated within the civil document request division. This corroboration establishes a *prima facie* case for the existence of an **Irremediable Nullity** within the municipal records that requires federal metadata for definitive resolution.
7. As heretofore noted, it is expressly confirmed via the signature appended to this requisition and the concomitant provision of identity documentation that Kevin A. McLean was subjected to a physical deprivation of liberty on October 2, 2024, purportedly pursuant to a represented arrest warrant. Notwithstanding the representation of authority, it is posited that the Toronto Police Service (the "**TPS**") failed to maintain a valid or accurate iteration of the authorizing instrument, instead relying upon a technologically corrupted version of the intake court endorsement (the "**Intake Court Endorsement**") which was factually inaccurate and fundamentally devoid of any legal or factual nexus to Kevin A. McLean. This corruption is not merely an aesthetic or clerical flaw; it is a fundamental breakdown in the chain of judicial authorization, rendering the subsequent detention a profound violation of the principles of fundamental justice and a manifestation of state action that is strictly *extrajudicial*.

II. FACTUAL MATRIX AND FORENSIC DATABASE PARTICULARS

8. It is legally necessitated that access be unequivocally granted to the specific algorithmic, structural, and foundational fields within the Canadian Police Information Centre (the "**CPIC**") database. This requisite access encompasses, but is absolutely not limited to, the exact, unredacted nomenclature of the authorizing judicial officer, the specific judicial tier and territorial jurisdiction of said officer, the precise temporal date and immutable algorithmic timestamp of initial systemic entry into the federal ledger, and the precise law enforcement divisions responsible for the primary data input and any subsequent digital modifications. The exaction must include the "Time-to-Live" (the "**TTL**") parameters and the terminal identification numbers (the "**Terminal Identification Numbers**") utilized during the primary data transmission.
9. The **CPIC** database operates as the supreme, centralized nervous system of Canadian law enforcement, dictating real-time liberty deprivations across all provincial, territorial, and municipal boundaries. It is fundamentally acknowledged that **CPIC** is a highly complex, federated system, wherein the relevant repository for active, unexecuted warrants is specifically designated as the investigative data bank (the "**Investigative Data Bank**"). The personal information housed within the

Investigative Data Bank is legally governed, strictly regulated, and administratively audited under the formal federal designation of personal information bank rcmp ppu 005 (the "**PIB RCMP PPU 005**").

10. Because an entry within **CPIC** instantaneously transforms an individual into a subject of national state coercion, empowering every sworn officer across the dominion to effectuate a physical arrest upon mere systemic confirmation, the metadata underlying that entry transcends mere administrative trivia. It is the absolute digital *acta* upon which constitutional rights are either respected or irreparably breached. The database is the digital embodiment of the sovereign's coercive power, and its logs are the only unimpeachable evidence of its exercise, providing a "single source of truth" that remains insulated from the potential for local, municipal-level record manipulation or localized software "glitches" that conveniently obscure jurisdictional errors.
11. The primary occurrence number is definitively recorded as Toronto Police Service occurrence number 2024-2028093 (the "**Primary Occurrence**"), established on September 15, 2024 (the "**Primary Date**"), and administratively managed by Officer Eric Tang, bearing badge number 10942 (the "**Primary Case Manager**"). This specific cipher establishes the temporal genesis of the investigatory phase, marking the initial engagement of the municipal constabulary and establishing the foundational timeline against which all subsequent digital entries must be forensically measured for chronological fidelity.
12. The secondary occurrence number, which appears to govern the immediate custodial trajectory of the matter and the physical effectuation of the arrest itself, is recorded as Toronto Police Service occurrence number 24-2082035 (the "**TPS Occurrence Number**"), dated September 22, 2024 (the "**Secondary Date**"), and managed by Detective Constable Michael Kolankowski, bearing badge number 82239 (the "**Secondary Case Manager**"). The administrative bifurcation of the investigation into dual occurrences necessitates a highly precise temporal mapping of all judicial authorizations applied within the local municipal records management system (the "**Local RMS**"), as such fragmentation is often indicative of procedural anomalies intended to bypass the scrutiny of a single judicial oversight officer.
13. A concomitant identification cipher, critical to the central archival indexing of the prosecution and the integration of physical court records, is noted as Toronto Police Service case identification number 457197 (the "**Police Case ID Number**"). The multiplicity of these labyrinthine tracking digits further exacerbates the necessity for a pristine, federally verified chronological timeline, as disparate occurrences frequently signify deliberate administrative compartmentalization explicitly designed to obscure jurisdictional overreach or the unauthorized "stacking" of occurrences to justify a warrantless apprehension *ex post facto*.
14. The purported date of the formal commencement of proceedings, as explicitly indicated upon the physical face of the impugned documentation and purportedly sworn under oath, is September 23, 2024 (the "**Commencement Date**"). This date is the absolute temporal fulcrum upon which the legality of all subsequent state actions, including the physical detention, fundamentally balances. If the digital entry into **CPIC** post-dates this moment, or if the metadata reveals a "retroactive addition" transaction, the entire prosecution is infected with a fatal chronological defect that cannot be cured by the *Rules of Civil Procedure* (the "**Civil Rules**").
15. It is further confirmed that as a result of any court or judge being **Coram Non JUDGE** or **Factum A JUDGE, Quod Ad Officium Jure Non Pertinet, Ratum Non Est** on account of the **False Information Package**, which is attached for ease of reference albeit a false document or false documents, it will also be 18 months since the time of the declaring of an Information (Criminal Code Form 2) albeit with the incorrect name involving Court Officer (Toronto Region) Christyn Frugoni-Rojas and incorrect data therein along with the **Intake Court Endorsement** not being the correct document either and presumably a problem of modern technology.
16. In relation to the 18th month window, it is also pursuant to *R v Jordan*, 2016 SCC 27 (the "**Jordan**") that in any matter involving a matter before the Ontario Court of Justice, of which the Crown Counsel elected to proceed summarily and the arrest warrant (the correct one) that a trial must be held and concluded within 18 months. That terminal date would be March 23, 2026. As such, although every judge was **Coram Non JUDGE** and any act, step, or document was subject to **Factum A JUDGE, Quod Ad Officium Jure Non Pertinet, Ratum Non Est**, Kevin A. McLean provides that for ease of reference noting the thirty-day time window for the fulfillment of this statutory requisition.
17. The informant of record is identified as Court Officer Christyn Frugoni-Rojas (the "**Informant**"). It is noted with profound, overarching legal significance that Christyn Frugoni-Rojas was acting not merely

- as a civilian administrative clerk, but in the highly specialized, deputized, and statutorily augmented capacity of a special constable. This designation inherently engages the coercive apparatus of the state and significantly elevates the standard of exactitude, procedural fairness, and duty of candour required in the swearing of the underlying information and the subsequent generation of any resultant arrest warrants. The sworn statements of a special constable carry the full weight of the Crown; any falsehood, temporal inaccuracy, or "technological corruption" therein constitutes a fundamental breach of the duty of *uberrima fides* (the "**Utmost Good Faith**").
18. The sworn information number, serving as the unique identifier for the specific charging document contained on the Form 2, is formally recorded as 4810 998 24 48129169 (the "**Information Number**").
 19. An intake court endorsement was purportedly effectuated on the **Commencement Date**, bearing a digital signature purportedly attributed to Justice of the Peace George Jiri (the "**Authorizing Officer**") of the Brampton Ontario Court of Justice (the "**Non-Originating Courthouse**"). It is observed with the utmost, grave concern that said endorsement is entirely devoid of the requisite geographical, territorial, and temporal indicators explicitly corresponding to the Toronto region, where the alleged offense and investigation were inextricably localized.
 20. The sterile application of a digital signature by a judicial officer stationed within the Peel Region, affixed to a strictly Toronto-based prosecution—without the explicit, recorded invocation of inter-jurisdictional transfer protocols or telewarrant provisions delineated within the *Criminal Code*—constitutes an act of **Factum A Judice, Quod Ad Officium Jure Non Pertinet, Ratum Non Est**. Because the judicial officer lacked the requisite territorial jurisdiction and the inherent authority to promulgate such an order outside their assigned venue, the resulting process is an absolute, irredeemable nullity. The exercise of judicial power outside its statutory ambit is a jurisdictional vacuum that cannot be cured by subsequent administrative action, as it strikes at the heart of the court's competence.
 21. Furthermore, as any appearance before a judicial officer lacking such authority is strictly **Coram Non JUDGE**, the entire procedural foundation of the arrest is structurally unsound. The fundamental common law maxim *nemo dat quod non habet* (no one gives what they do not have) dictates that a judicial officer cannot confer lawful authority over a jurisdiction to which they are not temporally or geographically assigned; thus, a Brampton justice possesses zero inherent jurisdiction to issue a Toronto warrant absent strict statutory compliance, which is entirely absent from the face of the record.
 22. The presumed originating venue as of the **Commencement Date**, dictated inflexibly by the strict territorial strictures of the alleged offense and the locus of the police investigation, is the Ontario Superior Court of Justice South Toronto Criminal Division (the "**Originating Courthouse**"). This constitutes the only proper, constitutionally sound venue for the promulgation of the *acta*.
 23. The presumed originating police division, universally vested with the primary investigatory jurisdiction and operational oversight, is the Toronto Police Service 52nd Division (the "**Originating Police Division**"). Within the highly secure architecture of **CPIC**, every single entry is inextricably tethered to a specific originating agency identifier (the "**ORI**"), which serves as the unforgeable digital signature for every transaction and irrevocably traces the exact terminal and data input back to a specific law enforcement division. The **ORI** prevents any local agency from disclaiming responsibility for a fraudulent, extra-jurisdictional, or "technologically corrupted" entry.
 24. The effectuation of the physical arrest transpired on October 2, 2024 (the "**Arrest Date**") at the Toronto Police Service 14th Division (the "**Non-Originating Police Division**"). Subsequent to the initial arrest at the **Non-Originating Police Division**, the specialized attendance, custodial transfer logistics, and interrogatory presence within the holding cells were singularly conducted by Detective Abdulhameed K. Virani (the "**Deciding Detective**"), who is operationally attached to the **Originating Police Division**.
 25. The release documentation, effectuated via a Form 10 (the "**Release Order**"), incorporated the **TPS Occurrence Number** but fundamentally and inexplicably omitted the **Police Case ID Number**. The omission of this universally required central indexing digit on a mandatory release document suggests that the document may have been generated entirely outside the primary **Local RMS** architecture, potentially as a manual, offline override deliberately utilized to bypass locked systemic safeguards that strictly require verified antecedent warrants before a formal **Release Order** can be generated by municipal software.
 26. It is fundamentally acknowledged that the removal of a WANT record from the active **CPIC** interface upon the execution of an arrest constitutes a mere functional illusion of deletion. Systemic architecture requires that operational statuses be updated via highly specific command codes, namely the

clearance transaction (the "**CLEAR Transaction**") indicating a successful execution, or the cancellation transaction (the "**CANCEL Transaction**") indicating withdrawal or profound procedural error. Execution of these terminal transactions triggers the immediate migration of the data into an insulated repository formally designated as the offline historical database (the "**Offline Historical Database**"). Any deviation whatsoever between the physical paper trail and the digital federal ledger is unconditionally indicative of institutional malfeasance, unauthorized data entry, and deliberate documentary metamorphosis intended to cure jurisdictional defects post-arrest.

III. MEMORANDUM OF LEGAL ANALYSIS: STATUTORY MANDATES FOR DISCLOSURE

The Statutory Right of Access: Section 12(1) and the Breadth of Federal Control

27. Pursuant to Section 12(1) of the **Privacy Act**, a robust, quasi-constitutional right of access is conferred upon Kevin A. McLean to acquire personal information concerning themselves that is under the control of a federal government institution (the "**Institution**"). This statutory entitlement transcends mere procedural courtesy; it operates as a substantive jurisprudential bedrock intended to ensure absolute governmental accountability and guarantee strict, unwavering adherence to the *lex terrae*. The right to know the basis of one's detention is the cornerstone of *habeas corpus*, now modernized into the digital realm via the **Privacy Act**. The ontological status of the digital warrant, being the primary vehicle for the deprivation of physical liberty, mandates that the subject of such a record possess the unmitigated ability to verify its provenance and chronological integrity.
28. The Royal Canadian Mounted Police (the "**RCMP**"), acting in its capacity as the paramount architect and supreme custodian of the **CPIC** database infrastructure, is deemed by well-established appellate authority to be in absolute legal control of the records entered into that national system. This expansive definition of "control" is utterly unaffected by the inter-agency principle of "originator control." Established jurisprudence from the Office of the Privacy Commissioner of Canada unequivocally confirms that the **RCMP** bears the ultimate, non-delegable responsibility for ensuring that all information hosted across the **CPIC** network complies strictly with federal statutes, regardless of which agency performed the initial keystrokes.
29. The Supreme Court of Canada, in *Canada (Information Commissioner) v Minister of National Defence*, 2011 SCC 25 (the "**National Defence**"), affirmed that physical possession, systemic administration, and structural integration satisfy the highest threshold for "control" under federal access legislation. The hosting institution cannot disavow the contents of its own digital ledger, nor can it outsource its strict privacy obligations to the constituent municipalities who utilize its infrastructure. Consequently, a non-derogable obligation is imposed upon the **RCMP** to provide unfettered, unredacted access to the specific **CPIC** metadata fields requested herein. The inter-jurisdictional nature of the data entry provides no legal sanctuary from the disclosure obligations imposed upon the federal host.

Systemic Audit Trails, Non-Repudiation, and the Mandate for Informational Veracity: Section 6(2)

30. The architecture of **CPIC** relies upon the principle of absolute non-repudiation. Every systemic interaction generates a permanent, immutable entry within the system's underlying transaction logs (the "**Transaction Logs**"). This includes the initial addition of data (the "**ADD Transaction**") and any subsequent alterations (the "**MODIFY Transaction**"). These logs capture forensic-level details including the exact millisecond of execution, the unique user identifier of the operator, and the internet protocol address (the "**IP Address**") of the originating terminal. The Principle of Non-Repudiation serves as a cryptographic and administrative guarantee that a digital record cannot be disowned or surreptitiously altered by its creator without leaving an indelible audit trail.
31. Section 6(2) of the **Privacy Act** stipulates that the **Institution** shall take all reasonable steps to ensure that personal information utilized for an administrative purpose is as accurate as possible. When the coercive power of the state is mobilized based upon hosted digital data, the tolerance for systemic inaccuracy is reduced to an absolute nullity. A false entry in **CPIC** is a digital loaded weapon pointed at the liberty of the citizen. Should the **Transaction Logs** reveal a **MODIFY Transaction** that inexplicably alters the judicial officer's name to an extra-territorial jurisdiction post-arrest, institutional fraud is established. The doctrine of *fraus omnia corrumpit* (fraud unravels all) dictates that a judicial process infected by deliberate fraud is void *ab initio*.

Judicial Accountability, the Functus Officio Doctrine, and the Status Quo Ante

32. The exaction of the authorizing judicial officer's nomenclature and the precise, verified tier of the authorizing court are critical, non-negotiable imperatives for establishing the substantive jurisdictional validity of an arrest *ab initio*. At the exact moment of execution, the issuing judicial officer becomes

entirely *functus officio* with respect to that specific warrant. Reliance is placed upon the principles

articulated in *Chandler v Alberta Association of Architects*,

1989

2 SCR 848 (the "**Chandler**"), wherein the Court affirmed that once a judicial officer has finally decided a matter and issued their order, their jurisdiction over that specific matter is entirely exhausted.

33. Consequently, the authorization itself crystallizes into administrative, historical records of a definitively concluded judicial process (*acta*). The statutory shield of investigative privilege cannot be contorted or retrofitted to conceal procedural anomalies, jurisdictional overreaches, or the *post facto* generation of documents explicitly designed to sanitize a botched apprehension. Once the custodial phase has culminated in the issuance of a **Release Order**, the foundational details of the warrant's authorization transcend the protected realm of active law enforcement investigative techniques and must be subjected to public and judicial scrutiny to maintain the integrity of the administration of justice.

The Jordan Ceiling and the Imperative for Expedited Remediation

34. The temporal trajectory of these proceedings is governed by the strictures delineated in *R v Jordan*. As the Crown Counsel elected to proceed summarily, the presumptive ceiling for the completion of the trial is established at 18 months from the date of the commencement of proceedings. Given the **Commencement Date** of September 23, 2024, the terminal date for the vindication of the right to a trial within a reasonable time is March 23, 2026. This impending deadline exacerbates the urgency for the exaction of the **Offline Historical Database** records.
35. Any delay precipitated by the **RCMP's** failure to provide unvarnished access to the forensic metadata constitutes a direct impediment to the **Applicant's** ability to make full answer and defence. If the proceedings are structurally vitiated due to jurisdictional nullity, the continuation of the prosecution beyond the **Jordan** ceiling would constitute a double breach of constitutional guarantees—both as to the legality of the initial detention and the reasonableness of the ensuing delay. The state cannot use its own technological "corruption" or administrative obfuscation to extend the custodial or prosecutorial shadow over the citizenry.

Triangulating Truth and Statutory Remedies: Section 12(2) and the Charter

36. To definitively prove institutional manipulation, the digital *acta* procured from the federal **RCMP** must be subjected to a strict discrepancy analysis against the primary, originating physical legal instruments. This forensic methodology of "Triangulating Truth" ensures that independent judicial branch records are meticulously cross-referenced with federal **RCMP** offline security infrastructure, exposing any discrepancies introduced by municipal police intermediaries. This triangulation is the only method to expose the "documentary metamorphosis" that occurs when municipal files are surreptitiously updated to match federal entries.
37. Should the discrepancy analysis confirm systemic manipulation, the profound remedial provisions of Section 12(2) of the **Privacy Act** shall be immediately invoked. Kevin A. McLean possesses the right to demand the formal, immediate correction of erroneous or fabricated information or the attachment of a notation of disagreement (the "**Notation of Disagreement**"). Under Section 24(1) of the **Charter**, a comprehensive remedy may be sought for an unlawful or arbitrary detention.
38. The jurisprudence of *R v Garofoli*,
1990
2 SCR 1421 (the "**Garofoli**"), establishes the absolute right of an accused to challenge the underlying validity of a judicial authorization; this right is rendered illusory if the metadata proving its invalidity is systematically withheld. The pursuit of constitutional remedies, including the exclusion of evidence under Section 24(2) based upon the principles in *Hunter v Southam Inc*,
1984
2 SCR 145, is utterly contingent upon the procurement of the systemic metadata substantiating the illegality. In the face of undeniable fraud, the **Irremediable Nullity** must be recognized, and Kevin A. McLean optimally positioned to seek prerogative writs such as *certiorari* to quash the vitiated proceedings *in limine*.

IV. FORMAL DEMANDS FOR EXACTION AND SYSTEMIC DISCLOSURE

39. In absolute summation, it is unequivocally and forcefully submitted that the **RCMP** is legally bound, without the option for discretionary refusal, to disclose the entirety of the requested metadata particulars. It is formally demanded that the **Institution** immediately conduct a comprehensive offline

search (the "**Offline Search**") of the highly secure **Offline Historical Database** to retrieve all artifacts associated with the **PIB RCMP PPU 005** repository.

40. This explicit demand for exaction encompasses the following specific forensic artifacts, which are indispensable for the forensic reconstruction of the record:
 - a. The retrieval of all active, cleared, canceled, or purged WANT Records associated with Kevin A. McLean spanning the entirety of the year 2024, including historical status codes (the "**Historical Status Codes**").
 - b. The unredacted production of all system **Transaction Logs**, audit trails, and hexadecimal dumps (the "**Hexadecimal Dumps**") governing the entire lifecycle of the warrant entry, including all **ADD**, **MODIFY**, **CLEAR**, and **CANCEL** Transactions, and any supervisor override actions recorded within the federal mainframe.
 - c. The explicit disclosure of the associated timestamps (accurate to the millisecond), the **ORIs**, the unique user IDs of terminal operators, the precise terminal hardware addresses, and the entirety of the narrative and remarks fields (the "**Narrative Fields**") for each sequential transaction, demonstrating the evolutionary history of the data entry and any unauthorized "metamorphosis."
41. Given the severe allegations of systemic metamorphosis and inter-jurisdictional fraud, the stipulation for electronic transmission directly to Kevin A. McLean (the "**Transmission Method**") is strictly necessary. The **Institution** is statutorily obligated to fully accommodate this method of secure delivery to protect the strict integrity of the data and the absolute privacy of Kevin A. McLean, shielding it from potential interception or further manipulation by originating municipal agencies currently under scrutiny.
42. The **RCMP** is firmly reminded of the strict statutory thirty-day timeline governing the disposition of access requests under the **Privacy Act**. Due to the significant legal ramifications tethered to its contents and the impending **Jordan** ceiling of March 23, 2026, it is formally demanded that all responsive records be collated and transmitted exclusively via the designated **Transmission Method**, entirely devoid of any redactions, omissions, or obfuscations whatsoever. Any failure to comply will precipitate immediate escalation to the Office of the Privacy Commissioner of Canada and the subsequent pursuit of a writ of *mandamus* before the Federal Court of Canada.

All of which is respectfully submitted.

Mr. Kevin A. McLean (BA, JD, CIM)

Enclosures (copies of): i. Passport of Kevin A. McLean (the "**Applicant**" or "Requestor"); Driver's License of the Applicant (G Drivers Licence) (Nota bene: NotaDO NOT SEND TO THIS ADDRESS – TERRIBLE MAIL COLLECTION and MISDIRECTED MAIL TO WRONG PERSONS – IF MAIL RETURN IS REQUIRED – PLEASE SEND TO 68 Abell St
Toronto, ON M6J 0B1 (Prime Medical, Rehab Mechanics for Mr. Kevin A. McLean (BA, JD, CIM)); and (iii) Health Card from Ontario Government for Mr. McLean

NOTA BENE: Only reply via email or fax.

Tab E

736
DELIVERY METHOD: Via Registered Mail & Electronic Transmission

TO:

Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone: 647.370.9354

REFERENCE: Formal Request under the *Access to Information Act* (ATIA)

CROSS-REFERENCE: *Privacy Act* Request File P-2025-16999 / F339

SUBJECT: FORMAL SPECIFICATION OF REQUISITIONS UNDER THE ACCESS TO INFORMATION ACT (ATIA) – CPIC SYSTEMIC INTEGRITY, METADATA EXTRACTION, AND INTER-AGENCY COMMUNICATIONS

Dear ATIP Coordinator,

Please accept this correspondence as a formal request for access to records under the *Access to Information Act* (ATIA), R.S.C. 1985, c. A-1. The prescribed statutory application fee of \$5.00 is enclosed with the physical transmission of this document.

This ATIA requisition operates as a concurrent and supplementary filing to my existing *Privacy Act* request (RCMP File P-2025-16999 / F339). While the *Privacy Act* requisition strictly concerns my personal information and localized metadata, this ATIA request serves a broader, more profound democratic function: it targets the

737
overarching institutional records, systemic metadata architecture, and inter-agency communications held by the Royal Canadian Mounted Police (RCMP).

As the supreme governance authority for the Canadian Police Information Centre (CPIC), the RCMP holds the ultimate fiduciary and statutory duty to maintain the uncorrupted "trust architecture" of the national law enforcement database. The CPIC apparatus is decidedly not a mere repository of administrative trivia, nor is it a passive bulletin board for municipal police forces. It is the central, incorruptible nervous system of the Canadian law enforcement apparatus. The entirety of the Canadian criminal justice system relies absolutely, without exception, on the unbroken chain of custody of sworn judicial documents. When a municipal constabulary engages a private citizen, the data retrieved from the CPIC terminal dictates the immediate trajectory of that citizen's physical liberty.

Therefore, when the cryptographic provenance of a sworn document is severed by state actors utilizing commercial manipulation software to alter jurisdictional realities, the resulting documentation ceases to operate as a lawful warrant. It devolves into a mere instrument of arbitrary coercion. The RCMP possesses a unique, extra-jurisdictional duty to ensure that its federal infrastructure is not being utilized as a digital laundry for the sanitization of local jurisdictional nullities.

The following specific technical artifacts and institutional records are formally requisitioned to verify the cryptographic provenance, expose the algorithmic manipulation, and confirm the jurisdictional integrity of the CPIC records associated with file P-2025-16999 / F339:

1. Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.

- **Contextual Justification:** Standard CPIC "Persons" file queries, which are utilized by frontline patrol officers on the street, are fundamentally insufficient for this inquiry. The graphical interface available to a patrol officer is subject to algorithmic filtering and reflects only the contemporaneous, operational status of a file. Only the immutable systemic ledgers housed deep within PPU 005—capturing the precise chronological sequence of ADD, MODIFY, CLEAR, and CANCEL commands—can definitively expose the temporal trajectory of state-actor malfeasance. The architectural reality of the CPIC database ensures that while a fraudulently altered warrant may be ostensibly excised from the active operational interface to hide the evidence of an unlawful arrest, the underlying digital artifact and the footprint of the user who deleted it are decidedly not eradicated from the federal infrastructural matrix.

2. Hexadecimal Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.

738 • **Contextual Justification:** This mathematical data is strictly required to bypass the visual homogenization inherent to the standard Graphical User Interface (GUI). The GUI is merely a presentation layer; it can be manipulated to display a facially valid warrant even when the underlying data structure is fatally corrupted. Only the uninterpreted binary and hexadecimal records—complete with exact cryptographic memory offsets and ASCII/EBCDIC decoded text translations—can provide the mathematical certitude required to prove vector morphology collapse. These immutable binary ledgers circumvent human interpretation entirely. A raw hexadecimal dump shows the binary reality of the database entry, demonstrating exactly when the foundational metadata was algorithmically disfigured without lawful judicial authorization, and confirming if the payload matches the physical forged documents.

3. Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.

- **Contextual Justification:** This data is critical to establishing the physical and geographical locus of the data entry, invoking the foundational legal maxim *nemo dat quod non habet* (no one gives what they do not have). If an instrument purportedly authorized by a Superior Court Chief Justice operating out of the 361 University Avenue courthouse was actually inputted from a municipal police division's back-office terminal (e.g., TPS 52nd Division or 14th Division), the ORI routing codes will incontrovertibly prove the jurisdictional nullity. The RCMP cannot hide behind the "originator control" principle to avoid disclosing the very records that prove the originating municipal agency committed a forgery. Once a municipal agency enters data into the federal mainframe, that metadata becomes a federal record, subject to federal transparency laws.

4. Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.

- **Contextual Justification:** When a catastrophic software failure occurs during the ingestion of a judicial document, it generates automated system alerts and IT troubleshooting tickets. This requisition specifically targets communications regarding the authentication of the corrupted judicial initials ("CL (M)"), the resolution of vector collapse errors, and any inquiries regarding jurisdictional discrepancies between the physical court filings and the electronic mainframe entries during the September-October 2024 epoch. This includes any communications with specialized operational units or local registries regarding the failure of the mandatory "Matching Protocol." A system error of this magnitude would not exist in a vacuum; there is an administrative paper trail of IT professionals attempting to reconcile the corrupted digital artifacts.

739
5. PDF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.

- **Contextual Justification:** This is particularly targeted at system interactions involving the GrapeCity Documents PDF suite (specifically version 6.0.2.0 and the documented DOC-6507 bug). Forensic analysis confirms this enterprise-level developer software was utilized with the specific *mens rea* to unlawfully flatten the document, forcefully delete the transparent electronic image signature of Chief Justice Geoffrey B. Morawetz, and algorithmically disfigure the underlying text to bypass standard criminal intake procedures. Specifically, the software's flattening engine violently clipped the mathematical bounding box of the "J" into an "L" and crushed the initials "G.B." into parentheses "()". Furthermore, records concerning the subsequent, deliberate superimposition of a civilian clerk's digital certificate (Court Officer Christyn Frugoni-Rojas) directly over the corrupted artifact to act as a visual smokescreen, and the appending of a decoy Justice of the Peace signature line (George Jiri), are requisitioned.

6. Offline Historical Search Results: The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.

- **Contextual Justification:** The municipal record currently presents a glaring chronological impossibility: an arrest executed on October 2, 2024, followed by the inexplicable expungement of the purported warrant from provincial systems via the Integrated Court Offences Network (ICON) on October 3, 2024. A lawful warrant does not evaporate the day after its execution; it is filed as a return to a justice. The RCMP's offline historical data stands as the singular remaining mechanism to pierce this localized spoliation trap. Furthermore, this data is necessary to expose the retaliatory "Digital Spoliation" orchestrated by the Justice Sector Security Office (JSSO), which weaponized cybersecurity infrastructure by utilizing a 403 Forbidden Error to block my IP address from the Ontario Courts Public Portal upon the initial discovery of this nullity.

7. System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

- **Contextual Justification:** This includes all operational directives establishing the responsibilities of the CPIC Coordinator to ensure that the electronic data entered perfectly mirrors the physical judicial order. There exists a mandatory "Air Gap" between the judiciary and the police; judges possess no direct terminal access to input data into CPIC. Therefore, the structural integrity of the system relies entirely on police compliance with this Matching Protocol. Manuals detailing the rigorous, distinct standards required

740 for the intake of Superior Court of Justice (SCJ) warrants versus provincial Ontario Court of Justice (OCJ) take endorsements are required to prove exactly how these systemic checks and balances were bypassed to manufacture a facsimile of authority.

Notice Regarding Statutory Exemptions and Public Interest Override (Section 19(2))

To the extent that the institution contemplates the application of discretionary exemptions under the ATIA—specifically those pertaining to the "personal information" of state actors, internal governmental deliberations, or law enforcement investigative privilege—such redactions are hereby preemptively challenged, legally vitiated, and fundamentally dismantled in limine.

As established exhaustively in my concurrent *Privacy Act* filings, the records sought relate directly to profound documentary metamorphosis, systemic spoliation, and an Irremediable Nullity orchestrated by state actors acting under the mere colour of authority. The legal maxim *fraus omnia corrumpit* (fraud vitiates everything) fundamentally dictates that a judicial process infected by deliberate digital manipulation is irreparably compromised across all subsequent administrative tiers. The invocation of privacy laws to shield the identities of those who authored a forgery is a perverse subversion of the legislation's intent.

When public officials utilize enterprise developer applications to digitally forge the authorizations of a Superior Court, they irrevocably forfeit the traditional immunities and privacy expectations afforded to them in the standard, lawful execution of their duties. As determined by the Supreme Court of Canada in *Dagg v. Canada (Minister of Finance)*, the fundamental objective of access legislation is the rigorous scrutiny of state action, effectively diminishing the privacy expectations of public officials engaged in the execution of official duties. The names, terminal IDs, and ORI routing codes of state actors operating a federal database are professional metrics, not intimate biographical details.

Pursuant to Section 19(2) of the ATIA, the paramount public interest in ensuring the constitutional legitimacy, democratic accountability, and algorithmic integrity of the national CPIC database decisively and unequivocally overrides any residual privacy expectations of the professional actors involved. The institution cannot rely upon the "mosaic effect"—the theory that disclosing seemingly innocuous administrative metadata could allow for the re-identification of state actors—to justify the withholding of data. In cases of alleged state malfeasance and the arbitrary deprivation of liberty, the public's right to reconstruct the "mosaic of forgery" is the paramount democratic interest.

If the Privacy Commissioner previously ruled in the prominent "Suicide Disclosure Case" that CPIC cannot be utilized for the unauthorized dissemination of sensitive mental health data due to the severe collateral damage it inflicts, it *a fortiori* cannot be utilized as a secure digital vault for the preservation of municipal-level documentary forgery. The public possesses an absolute, inalienable right to ascertain whether the coercive apparatus of the state is mobilized upon legitimate judicial authority or a "Frankenstein" algorithmic fabrication.

741
A justice system that operates on altered PDFs and falsified metadata is a system that has lost the consent of the governed.

In the spirit of our access partnership, I am fully prepared to assist the ATIP branch in clarifying any technical parameters of this request to ensure efficient, streamlined processing prior to the expiration of the statutory deadline.

I look forward to your formal acknowledgment of this ATIA request and the timely, unredacted provision of the responsive records.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Appendix #1: Access to Information Act Excerpts**Personal Information**

19 (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Part that contains personal information.

Where disclosure authorized

(2) The head of a government institution may disclose any record requested under this Part that contains personal information if

- (a) the individual to whom it relates consents to the disclosure;
- (b) the information is publicly available; or
- (c) the disclosure is in accordance with section 8 of the Privacy Act.

R.S., 1985, c. A-1, s. 19 2019, c. 18, s. 9 2019, c. 18, s. 41(E)

APPENDIX #2: PRIVACY ACT, SECTION 8**Disclosure of personal information**

- **8 (1)** Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

- **Where personal information may be disclosed**

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

- **(a)** for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;
- **(b)** for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;
- **(c)** for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;
- **(d)** to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

- (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;
- (f) for the purpose of administering or enforcing any law or carrying out a lawful investigation, under an agreement or arrangement between the Government of Canada or any of its institutions and any of the following entities or any of their institutions:
 - (i) the government of a foreign state,
 - (ii) an international organization of states or an international organization established by the governments of states,
 - (iii) the government of a province,
 - (iv) the council of the Westbank First Nation,
 - (v) the *council of a participating First Nation* as defined in [subsection 2\(1\)](#) of the [First Nations Jurisdiction over Education in British Columbia Act](#),
 - (vi) the council of a *participating First Nation* as defined in [section 2](#) of the [Anishinabek Nation Education Agreement Act](#),
 - (vii) a *First Nation Government* or the *Anishinabek Nation Government*, as defined in [section 2](#) of the [Anishinabek Nation Governance Agreement Act](#), or an Anishinaabe Institution, within the meaning of section 1.1 of the *Agreement*, as defined in [section 2](#) of that Act,
 - (vii.1) the *Whitecap Dakota Government*, as defined in [section 2](#) of the [Self-Government Treaty Recognizing the Whitecap Dakota Nation / Wapaha Ska Dakota Oyate Act](#);
- (g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;
- (h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;
- (i) to the Library and Archives of Canada for archival purposes;
- (j) to any person or body for research or statistical purposes if the head of the government institution
 - (i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and
 - (ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

- **(k)** to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;
- **(l)** to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and
- **(m)** for any purpose where, in the opinion of the head of the institution,
 - **(i)** the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or
 - **(ii)** disclosure would clearly benefit the individual to whom the information relates.
- **Personal information disclosed by Library and Archives of Canada**

(3) Subject to any other Act of Parliament, personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes.
- **Copies of requests under paragraph (2)(e) to be retained**

(4) The head of a government institution shall retain a copy of every request received by the government institution under paragraph (2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make those copies and records available to the Privacy Commissioner.
- **Notice of disclosure under paragraph (2)(m)**

(5) The head of a government institution shall notify the Privacy Commissioner in writing of any disclosure of personal information under paragraph (2)(m) prior to the disclosure where reasonably practicable or in any other case forthwith on the disclosure, and the Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to whom the information relates of the disclosure.
- **Definition of *Indian band***

(6) In paragraph (2)(k), ***Indian band*** means

 - **(a)** a band, as defined in the [Indian Act](#);
 - **(b)** the band, as defined in [subsection 2\(1\)](#) of the [Naskapi and the Cree-Naskapi Commission Act](#);
 - **(c)** the *shíshálh Nation*, as defined in subsection 2(1) of the *shíshálh Nation Self-Government Act*; or
 - **(d)** a first nation named in Schedule II to the [Yukon First Nations Self-Government Act](#).

- **Definition of *aboriginal government***

745

(1) The expression ***aboriginal government*** in paragraph (2)(k) means

- (a) Nisga'a Government, as defined in the Nisga'a Final Agreement given effect by the *Nisga'a Final Agreement Act*;
- (b) the council of the Westbank First Nation;
- (c) the Tlicho Government, as defined in [section 2](#) of the [Tlicho Land Claims and Self-Government Act](#);
- (d) the Nunatsiavut Government, as defined in section 2 of the *Labrador Inuit Land Claims Agreement Act*;
- (e) the council of a participating First Nation as defined in [subsection 2\(1\)](#) of the [First Nations Jurisdiction over Education in British Columbia Act](#);
- (e.1) the Tla'amin Government, as defined in subsection 2(2) of the *Tla'amin Final Agreement Act*;
- (f) the Tsawwassen Government, as defined in subsection 2(2) of the *Tsawwassen First Nation Final Agreement Act*;
- (f.1) the Cree Nation Government, as defined in [subsection 2\(1\)](#) of the [Cree Nation of Eeyou Istchee Governance Agreement Act](#) or a Cree First Nation, as defined in subsection 2(2) of that Act;
- (g) a Maanulth Government, within the meaning of [subsection 2\(2\)](#) of the [Maanulth First Nations Final Agreement Act](#);
- (h) Sioux Valley Dakota Oyate Government, within the meaning of subsection 2(2) of the *Sioux Valley Dakota Nation Governance Act*;
- (h.1) the Whitecap Dakota Government, as defined in [section 2](#) of the [Self-Government Treaty Recognizing the Whitecap Dakota Nation / Wapaha Ska Dakota Oyate Act](#);
- (i) the council of a *participating First Nation* as defined in [section 2](#) of the [Anishinabek Nation Education Agreement Act](#); or
- (j) a *First Nation Government* or the *Anishinabek Nation Government*, as defined in [section 2](#) of the [Anishinabek Nation Governance Agreement Act](#), or an Anishinaabe Institution, within the meaning of section 1.1 of the *Agreement*, as defined in [section 2](#) of that Act.

- **Definition of *council of the Westbank First Nation***

(8) The expression ***council of the Westbank First Nation*** in paragraphs (2)(f) and (7)(b) means the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the [Westbank First Nation Self-Government Act](#).

- R.S., 1985, c. P-21, s. 8
- R.S., 1985, c. 20 (2nd Supp.), s. 13, c. 1 (3rd Supp.), s. 12

- 1994, c. 35, s. 39
- 2000, c. 7, s. 26
- [2004, c. 11, s. 37](#), c. 17, s. 18
- [2005, c. 1, ss. 106, 109](#), c. 27, ss. 21, 25
- [2006, c. 10, s. 33](#)
- [2008, c. 32, s. 30](#)
- [2009, c. 18, s. 23](#)
- [2014, c. 1, s. 19](#), c. 11, s. 24
- [2017, c. 32, s. 18](#)
- [2018, c. 4, s. 132](#)
- [2022, c. 9, s. 4](#)
- 2022, c. 9, s. 45
- [2023, c. 22, s. 20](#)

APPENDIX #3: SYNTHESIS OF KEY LEGAL PRINCIPLES

Seamless Code

The ATIA and the Privacy Act are of equal legal status. One does not trump the other; they are a harmonious framework (established in *Dagg*). Parliament explicitly designed these statutes to operate in tandem as a "seamless code." The protection of personal information under the Privacy Act is intrinsically linked to the exceptions provided under the ATIA, meaning the RCMP cannot artificially separate the public interest analysis from the privacy analysis. When interpreting the right to access against the right to privacy, the institution must view the legislation as a unified mechanism designed to facilitate democratic oversight.

Positive Obligation to Consider

The head of a government institution cannot simply spot personal information, apply ATIA 19(1), and abruptly halt the analysis. They have an affirmative, positive statutory obligation to exercise their discretion and consider whether the public interest override under 19(2)(c) and 8(2)(m) applies. A "blanket refusal" to even consider the override constitutes a jurisdictional error. The institutional head must actively, explicitly, and contextually weigh the public's right to know against the individual's right to privacy on a rigorous, case-by-case basis. Failing to document this balancing act renders the denial of access fundamentally arbitrary.

High Threshold ("Clearly Outweighs")

The public interest in disclosure must not just be present; it must clearly outweigh the invasion of privacy. Mere curiosity, media sensationalism, or a general desire for transparency is rarely enough to breach an individual's privacy rights. However, the threshold is uniquely calibrated when state malfeasance is alleged. In the context

747
of "Hexadecimal Dumps" and hardware routing metadata—information that is purely administrative, professional, and devoid of intimate personal biographical content—the invasion of privacy is negligible. Conversely, the public interest in ensuring the cryptographic integrity of the national warrant database is absolute, thereby easily satisfying the "clearly outweighs" standard.

Deferential Review

Because PA s. 8(2)(m) explicitly delegates the balancing test to the "opinion of the head of the institution," courts apply a deferential reasonableness standard of review to that decision (established in the *Prime Minister* case). Courts will check if the head actually conducted the balancing exercise and if their conclusion was rational, rather than deciding the public interest question completely from scratch. Therefore, it is imperative that the RCMP conducts a logically sound and thoroughly documented balancing exercise in the first instance. If the institution decides that shielding the professional identities of officers who allegedly forged a Chief Justice's signature is more important than the integrity of the CPIC database, that decision will face a standard of "reasonableness" review that it cannot logically survive.

Tab F

May 5, 2026

749

DELIVERY METHOD: Via Registered Mail (Tracking) (copy to be provided via email)

Classification: Private and Confidential

TO:

Access To Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone: 647.370.9354

SUBJECT: FORMAL REQUEST UNDER THE *ACCESS TO INFORMATION* ACT (*ATIA*) – SOFTWARE PROCUREMENT, LICENSING, NTOP ONBOARDING, EMBEDDED IT ARCHITECTURE, AND AZURE CLOUD UTILIZATION RECORDS (GRAPECITY / MESCIUS SDKS)

Dear ATIP Coordinator,

1. Please accept this correspondence as a formal, highly specific, and multi-tiered statutory request for access to records under the *Access To Information Act (ATIA)*, R.S.C. 1985, c. A-1. The prescribed statutory application fee of \$5.00 is enclosed and/or processed concurrently with this transmission.
2. This request is strictly focused on objective, administrative, and technological procurement data regarding specific enterprise-grade software capabilities deployed within the federal law enforcement Information Technology (IT) ecosystem, specifically intersecting with the RCMP's "Cloud-First" regulatory framework and backend server-side document manipulation infrastructure.

I. STATUTORY RIGHT OF ACCESS, THE DUTY TO ASSIST, AND HEIGHTENED INSTITUTIONAL SCRUTINY

3. I make this request pursuant to Section 4(1) of the *Access To Information Act*:

4 (1) Subject to this Part, but notwithstanding any other Act of Parliament, every person who is
(a) a Canadian citizen, or

(b) a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act,
has a right to and shall, on request, be given access to any record under the control of a government institution.

4. Furthermore, I remind the ATIP Directorate of its absolute, mandatory obligations under Section 4(2.1) of the *ATIA*, which codifies the “Duty to Assist.” The institution is legally required to make every reasonable effort to assist the requester, to respond accurately and completely, and to provide timely access to the records in the format requested.
5. In the context of highly technical IT procurement, this duty strictly precludes the artificial narrowing of the scope of this request. It prohibits the reliance on rigid semantic technicalities to justify a “Nil” response (e.g., claiming no direct vendor contract exists when the software is procured indirectly or embedded).

INSTITUTIONAL CONTEXT & THE OPC 2023-2024 ANNUAL REPORT:

6. The ATIP Directorate is acutely aware that the RCMP is currently operating under intense, heightened external oversight regarding its use of third-party cloud services, embedded software applications, and algorithmic digital tools. This scrutiny has been explicitly codified in the **Office of the Privacy Commissioner of Canada’s (OPC) 2023-2024 Annual Report to Parliament on the Privacy Act, entitled “Trust, innovation, and protecting the fundamental right to privacy in the digital age.”** Following scathing OPC investigations (such as the “Project Wide Awake” report), the RCMP was heavily criticized for prioritizing digital innovation over fundamental rights by failing to conduct sufficient, legally mandated Privacy Impact Assessments (PIAs) prior to utilizing third-party data providers. In direct response to these parliamentary rebukes, the RCMP’s 2024–2025 Annual Report detailed a mandatory five-year modernization plan intended to clear ATIP backlogs and overhaul privacy systems. Given this explicit, publicly documented mandate to ensure that “innovation in the digital age” does not subvert constitutional rights, any attempt to obfuscate or delay this highly specific software inquiry will be viewed as a continuing, systemic breach of the very reforms the RCMP has promised Parliament it would implement.

II. DEFINITIONS, CORPORATE REBRANDING, AND SCOPE OF SEARCH: THE SDK DISTINCTION

7. To assist your Information Technology (IT), Procurement, and Shared Services Canada (SSC) liaison branches in conducting a thorough, legally compliant, and precise search, please be advised of the specific corporate and technological parameters of this request.
8. The software developer previously known globally as “**GrapeCity**” recently underwent a comprehensive corporate rebranding. The developer now operates under the corporate entity “**MESCIUS**” (or MESCIUS, USA). The corporate description for this vendor and its enterprise software suite is formally listed in industry indices as follows:

“We are Now MESCIUS, USA! Same great products. Same commitment to excellence. MESCIUS’ (pronounced mesh-ē-us) product line provides developers, designers, and architects with the ultimate collection of award-winning JavaScript and .NET grids, reporting, spreadsheets, document APIs, viewers, and mobile controls. Our tools help to quickly solve problems so you can focus on creativity, innovation, and optimization.”

9. For the purposes of this search, the software architectures targeted include, but are not strictly limited to, products previously named “**GrapeCity Documents for PDF**” (GcDocs), “**GrapeCity.Document.PDF**” (including specifically version 6.0.2.0, adjacent legacy versions, and subsequent patches), “**SpreadJS**,” “**ActiveReports**,” or any current iterations operating under the “**MESCIUS Document APIs**” nomenclature.

751 10. **Crucial Technical Distinction:** This software is highly specialized. It is a **Software Development Kit (SDK)**, not a standard end-user desktop application (like Adobe Acrobat or Microsoft Word). It is an enterprise-grade library utilized exclusively for server-side, programmatic, “headless” generation, modification, algorithmic compression, redaction, and morphological alteration of PDF documents at the hexadecimal and Bezier-curve vector level, entirely bypassing standard Graphical User Interfaces (GUIs). Procurement of an SDK implies the existence of dedicated software developers, custom codebases, and backend server infrastructure.

III. FORENSIC JUSTIFICATION: SDK AUTOMATION, EXIF METADATA, AND THE CPIC “SINGLE SOURCE OF TRUTH”

11. The necessity of querying RCMP and SSC procurement records for GrapeCity/MESCIUS specifically stems from irrefutable, cryptographically sound forensic metadata extracted from a highly suspect, facially void Intake Court Endorsement utilized to detail and detain the Applicant. An independent EXIF data and metadata extraction report performed on the target file—identified as **Information Package 4810 998 24 48129169-00 (4).pdf** (File Size: 336 kB)—yields critical, incontrovertible structural anomalies that point directly to federal, non-provincial server-side software tools and programmatic spoofing.
12. These forensic indicators establish the absolute necessity of this *ATIA* request:
 - a. **The SDK / Automated Back-End Infrastructure Implication:** The identification of “GrapeCity Documents for PDF version 6.0.2.0” as the document producer is the ultimate forensic pivot. Because GrapeCity is an SDK, its presence dictates that the document was not manually scanned or generated via a localized courthouse copier. It was generated through an automated back-end system—likely a specialized integration within a localized federal police records management system or an enterprise-level government portal. This capability allows for the precise, automated “spoofing” of standard Ontario Court pro forma layouts.
 - b. **Intentional Assembly and XMP Toolkit Imprints:** The embedded structural metadata explicitly identifies the xmp_toolkit as **Adobe XMP Core 9.1-c001 79.675d0f7, 2023/06/11-19:21:16**, interacting in tandem with underlying GrapeCity document generation algorithms. This definitively proves the document in question was assembled and manipulated digitally using advanced enterprise code, utilizing developer APIs to overlay, redact, or inject text into existing templates.
 - c. **Linearization and Web Optimization:** The metadata formally confirms the document's structure as **linearized: Yes**. Linearization (also known as “Fast Web View”) is a highly specific file-saving protocol that requires enterprise-level document APIs to reorganize the PDF's internal byte structure, allowing it to be streamed over web servers byte-by-byte. Routine provincial court scanners do not output linearized PDFs. This proves the file was engineered, re-saved, and optimized by an advanced IT system designed for federal-level cloud or CPIC database transmission.
 - d. **Hexadecimal Raw Header Anomaly:** The raw hex dump of the document header reads **25 50 44 46 2D 31 2E 33** (which decodes to the legacy standard %PDF-1.3). Generating a legacy PDF-1.3 structural header while simultaneously utilizing a modern 2023 Adobe XMP core toolkit is a hallmark of enterprise software (like the GrapeCity SDK) operating in a highly restricted, heavily customized backend environment intentionally forcing compatibility with legacy mainframe systems (such as CPIC).
 - e. **Atypical Tooling and the 5-Page Mathematical Impossibility:** Most legitimate Ontario Court documents are generated natively by the Integrated Court Offence Network (ICON) or Criminal Justice Digital Design (CJDD). Finding a GrapeCity enterprise producer tag embedded within these files is highly irregular for a standard provincial court output. Furthermore, the proper provincial pro forma dictates a 6-page layout, yet the exact structural extraction confirms the fabricated file contains exactly **page_number: 5**. This mathematical certainty corroborates the forensic conclusion that a critical page was programmatically, surgically, and intentionally removed during the GrapeCity digital assembly process.
 - f. **The Subversion of Jurisdictional Integrity and the CPIC Repository:** The GrapeCity SDK was utilized to manufacture a front-end document that successfully bypassed standard administrative standards (e.g., misapplying family-law intake standards to a criminal endorsement). Consequently, the physical PDF itself has been irrevocably de-authenticated. This elevates the **Canadian Police Information Centre (CPIC)** transaction logs to the role of

the definitive repository—the “Single Source of Truth”—for verifying the temporal and jurisdictional legitimacy of the underlying warrant. The tools that fed that repository are the GrapeCity/Mescius APIs requested herein.

IV. INTAKE COURT ENDORSEMENTS AND ARREST WARRANTS - PROTECTED B CLASSIFICATION

13. To provide necessary operational context for the IT systems being queried, it must be acknowledged that judicial instruments such as Intake Court Endorsements and arrest warrants signed by judges are strictly classified as **Protected B** information. The Treasury Board of Canada Secretariat explicitly defines Protected B as information that, if disclosed without authorization, could cause serious injury to an individual, organization, or the government.
14. Arrest warrants and judicial endorsements inherently meet this “serious injury” threshold for the following reasons:
 - a. **Information about Legal Proceedings:** Government security guidelines specifically classify records of active legal proceedings or criminal investigations within the Protected B category.
 - b. **Sensitive Personal Identifiers:** Warrants contain hyper-sensitive data, including a person's full name, address, date of birth, and highly protected administrative/biometric identifiers. Unauthorized leaks constitute a severe privacy breach.
 - c. **Operational Risk:** The unauthorized disclosure of a warrant prior to its execution carries severe operational risks, potentially subverting the ends of justice, compromising surveillance, or endangering officers.

HANDLING REQUIREMENTS FOR PROTECTED B INSTRUMENTS:

15. Because these judicial instruments are Protected B, the RCMP and all interfacing federal agencies are bound by strict, non-negotiable safeguarding protocols. Consequently, any software SDK—such as MESCIUS or GrapeCity—used to programmatically draft, manipulate, render, or redact these instruments must be utilized within a framework that complies with the following:
 - a. **Digital Storage:** Digital versions must be saved in secure, highly restricted systems like GCdocs or Protected B-compliant cloud environments (e.g., Microsoft Azure's Canadian regions).
 - b. **Physical Security:** When not in active use, physical derivatives must be stored in lockable containers exhibiting signs of attempted entry.
 - c. **Access Protocols:** Only personnel maintaining a valid Reliability Status screening, operating strictly on a “need-to-know” basis, are authorized to access, alter, or interact with these documents via digital software systems.

V. PROTECTED B CLOUD ARCHITECTURE, AZURE INTEGRATION, AND GC CLOUD GUARDRAILS

16. The RCMP currently manages its digital infrastructure and cloud storage through a highly regulated, “Cloud-First” strategy mediated by Shared Services Canada (SSC). For the sensitive **Protected B** information detailed above, the RCMP primarily utilizes **Microsoft Azure** as its enterprise standard.
17. Because MESCIUS (GrapeCity) developer SDK libraries are fundamentally engineered to operate seamlessly within Microsoft .NET and Azure environments, the integration of these server-side PDF-rendering APIs into the RCMP's Azure-based digital evidence and records management systems is highly probable. **Therefore, the ATIP office must extend its search parameters to include the following regulatory and architectural frameworks:**
 - a. **The National Technology Onboarding Program (NTOP):** All new operational technologies—ranging from Axon's “Draft One” AI-powered report drafting tools to specialized document redaction APIs and SDKs—must be formally onboarded through NTOP. This program is responsible for ensuring cloud-based tools meet strict legal, ethical, and GC Cloud Guardrail standards before deployment. *The ATIP search must query NTOP records for any onboarding evaluations, security clearances, or rejections associated with MESCIUS, GrapeCity, or their underlying SDK components.*

- b. **GC Cloud Guardrails and Data Residency:** To host Protected B data, the RCMP must comply with mandatory security configurations, including Multi-Factor Authentication (MFA) and the “principle of least privilege.” While the Sovereign Cloud Initiative (2025) pushes for Canadian-owned providers to eliminate risks associated with foreign legislation (e.g., the US CLOUD Act), personal information is still routinely hosted on US-based providers (like Microsoft Azure) provided comparable written security agreements are executed. *The search must identify any written security agreements, data residency waivers, or GC Cloud Guardrail compliance matrices associated with the deployment of MESCIUS (a US-based corporate entity) SDKs within the RCMP’s Protected B infrastructure.*
- c. **The “Internal Solution” Silo and Physical Safeguards:** Highly sensitive data (including cybercrime investigative records or restricted terminal logs) is often segregated into specialized analytical triage repositories, such as the “Internal Solution.” *The search must query IT architecture records to determine if GrapeCity/MESCIUS SDK APIs are utilized to automatically generate, redact, or encrypt documents originating from or entering the “Internal Solution” data silo.*

VI. TARGETED ALIGNMENT WITH 2020–2025 RCMP MEGA-PROJECTS

18. Preliminary forensic research into federal IT expenditures via the Open Government Portal and CanadaBuys databases yields no immediate public record of a direct, department-wide, standalone contract awarded by the RCMP directly to MESCIUS or GrapeCity.
19. However, it is a well-established federal IT reality that tools like GrapeCity/MESCIUS function as “invisible” foundational components. They are highly compatible developer libraries that are fundamentally embedded within the custom, large-scale backend applications built by the RCMP’s primary macro-vendors. **Therefore, I am explicitly directing the ATIP office to query the project managers, software architects, and procurement officers associated with the following specific RCMP IT acquisitions (2020-2025) where MESCIUS/GrapeCity libraries are highly likely to be embedded:**
 - a. **Microsoft 365 and SharePoint Online Migration (2024–2025):** The RCMP is currently undergoing a massive modernization of its security assessment processes and document management architectures utilizing Microsoft 365. MESCIUS Document Solutions and ActiveReports are industry-standard libraries specifically utilized by enterprise developers to automate the headless generation, manipulation, and rendering of complex PDFs directly from SharePoint data repositories and Azure .NET environments.
 - b. **Canadian Firearms Digital Services Solution (CFDSS):** This massive cloud migration and modernization project, actively managed by **Accenture Inc.**, was commissioned to replace outdated, legacy client-facing portals. Large-scale digital portals of this magnitude routinely and inevitably utilize third-party backend SDKs (such as MESCIUS APIs) to handle the high-volume, secure algorithmic generation of complex legal documents without crashing the server infrastructure.
 - c. **Axon Digital Evidence Management System (DEMS):** The RCMP’s sprawling **\$136.4 million contract** with Axon encompasses advanced, AI-powered tools for transcribing, managing, and, crucially, *redacting* digital evidence and generating evidentiary reports. While Axon operates as a largely closed ecosystem, the specialized PDF-viewing, redaction, and reporting utilities embedded within their “Productivity Suite” frequently rely on licensed, underlying enterprise architectural components identical or analogous to those offered by MESCIUS/GrapeCity.

VII. PROCUREMENT PATTERNS AND AUTHORIZED RESELLER DIRECTIVES

20. Government departments rarely, if ever, purchase backend developer libraries directly from entities like MESCIUS. Instead, these libraries are sourced through Value-Added Resellers (VARs) who hold active federal Software Licensing Supply Arrangements (SLSAs). **I am formally directing the ATIP office to search procurement logs**

- a. **Insight Canada**
- b. **Softchoice**
- c. **SHI Canada (SHI International)**
- d. **ComponentSource** (Operating as a Master Distributor for developer SDK components)
- e. **SoftwareONE** and **Compugen**

21. If the RCMP procured GrapeCity/MESCIUS SDK developer licenses, they were almost certainly routed through the SLSA framework via one of the aforementioned corporate entities.

VIII. THE REQUESTED RECORDS

22. I am formally requesting access to the following specific classes of records under the control of the Royal Canadian Mounted Police (RCMP), encompassing the comprehensive timeframe of **January 1, 2018, to the present date**:

- a. **Indirect and Direct Procurement/Licensing Records:** Any and all records, including purchase orders, end-user licensing agreements (EULAs), vendor contracts, invoices, expenditure approvals, Software Licensing Supply Arrangement (SLSA) call-ups, or budgetary line items demonstrating that the RCMP (or SSC on behalf of the RCMP) has purchased, licensed, or procured GrapeCity/MESCIUS Software Development Kits (SDKs) and/or API access, either directly from the developer or via third-party resellers (e.g., Insight Canada, Softchoice, ComponentSource).
- b. **NTOP Onboarding and Compliance Records:** All records, matrices, and security evaluations generated by the National Technology Onboarding Program (NTOP) regarding the approval, rejection, or conditional use of MESCIUS/GrapeCity developer tools. This must include any GC Cloud Guardrail compliance checks and data residency agreements executed to permit this software to interact with Protected B data on Microsoft Azure servers.
- c. **Embedded IT Architecture, Server-Side Integration, and Mega-Project Logs:** Any internal software architecture diagrams, deployment records, backend integration scripts, vendor technical specifications, or embedded library logs specifically related to the **Microsoft 365/SharePoint Migration, the CFDSS (Accenture), the Axon DEMS projects, or the “Internal Solution” data silo**, indicating that GrapeCity/MESCIUS PDF manipulation tools, SpreadJS, ActiveReports, Document APIs, or .NET/JavaScript grids are embedded within these server-side systems.
- d. **Software Lifecycle and Version Control Logs:** Any IT change-management logs, update tickets, developer requisition forms, or system administration records documenting the installation, upgrading, deprecation, or patching of GrapeCity.Document.PDF (specifically referencing version 6.0.2.0 or subsequent iterations) within the RCMP network, developer workstations, or CPIC-interfacing servers.
- e. **User Manuals, Document Integrity Protocols, and Internal Directives:** Any internal training materials, IT support tickets, developer manuals, Threat Risk Assessments (TRAs), or administrative directives referencing the utilization of GrapeCity or MESCIUS SDKs for the specific operational purposes of automated backend document creation, programmatic PDF generation, headless PDF redaction, algorithmic document alteration, or metadata manipulation by RCMP personnel or contracted developers. Consistent with the OPC's 2023-2024 directives to Parliament, this explicitly includes any **Privacy Impact Assessments (PIAs)** conducted to validate the use of these tools against public privacy rights.

IX. SEVERABILITY AND PRESERVATION OF RECORDS

23. Should any portion of the requested procurement records contain sensitive third-party financial data (e.g., specific negotiated unit pricing with a VAR like Softchoice or Insight Canada) that the institution deems exempt under

755 Section 20 of the *ATIA*, I remind the coordinator of the strict statutory obligation under Section 25 to sever the exempt financial material and disclose the remainder of the record. **The factual existence of a software license, its NTOP onboarding status, or its presence in a backend IT architecture diagram cannot be withheld merely because its purchase price is protected.**

24. Furthermore, given the extreme technical specificity of this request regarding backend IT infrastructure, SDK deployments, and active mega-projects, I hereby put the RCMP on formal notice to institute an **immediate administrative and IT preservation hold** on all responsive records. This includes directing the IT Directorate, the NTOP governance board, and the project managers for the M365, CFDSS, and Axon deployments to prevent the routine automated purging, overwriting, or deletion of software inventory logs, deployment metadata, and licensing repositories while this *ATIA* request is being processed.

X. FORMAT OF DISCLOSURE

25. I request that all responsive records be provided in an electronic format (searchable PDF).

XI. ENCLOSURES, PDF BOOKMARK DIRECTIVES, AND FEE CONFIRMATION

26. As this physically signed and couriered document serves as the formal *ATIA* request, please consider this section as explicit confirmation that the mandatory statutory application fee of **five dollars (\$5.00)** is enclosed herewith.
27. Furthermore, to assist your technical review and provide operational context for the requested software architectures, the enclosed PDF package contains embedded bookmarks of critical evidentiary importance. The ATIP office and consulting IT directorates are explicitly directed to observe the following bookmark architecture:
- a. **Front Page:** Directs to Page 1.
 - b. **Adjournment:** Directs to Page 1.
 - i. *Subheading under Adjournment:* “**MCLEAN, KEVIN**” directs to Page 4 of 5.
 - c. **Back Page (sic):** Directs to Page 5 of 5.
28. These navigational markers denote specific structural anomalies and document mutations that underscore the absolute necessity of obtaining the GrapeCity/MESCIUS architectural and SDK utilization records requested herein.
29. The reason for providing this in advance of when the 30 statutory (day) clock commences is to provide the electronic copy of the “False Information Package” so you can utilize the PDF (Adobe) bookmark navigation and clearly review the embedded “Document Properties” and associated EXIF/metadata outputs (as cross-referenced in Section III). Once received, you can respond under this thread.
30. The underlying necessity for these specific architectural and procurement records should be self-evident to your IT infrastructure, federal procurement, and compliance directorates. Should you require any clarification regarding the technical parameters, vendor networks, or search methodology of this request, please contact me immediately via email to avoid unnecessary statutory delays or constructive refusals.
31. Thank you for your prompt attention to this statutory imperative. I will confirm via email when the hard copy document with statutory fee has been delivered so we work together in this access partnership.

Sincerely,

Electronically signed



Mr. Kevin A. McLean

Enclosures:

756

1. The False Information Package as obtained from the OCJ 10 Armoury Street Courthouse (which was identical to the document obtained by counsel to the TPS in an HRT0 Proceeding in March 2025 but for amendments to case history);
2. The standard Lincoln County Law Association (Niagara) Adult Common Form Information Package

Tab G

Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

Mr. Kevin McLean <mcleansettlement@gmail.com>

Tue, Jun 16, 2026 at 10:17 AM

To: "Beaudoin, Tina (RCMP/GRC)" <tina.beaudoin@rcmp-grc.gc.ca>, Bryan.Larkin@rcmp-grc.gc.ca, "Brisson, Stéphane (RCMP/GRC)" <stephane.brisson@rcmp-grc.gc.ca>, "Ball, Jeff (RCMP/GRC)" <Jeff.ball@rcmp-grc.gc.ca>, "Simpson, Melissa (RCMP/GRC)" <melissa.simpson@rcmp-grc.gc.ca>

Date: June 16, 2026

Creation method: Dictated with voice recognition software (reserve rights to amend any errors involving syntax, spelling, grammar or incorrect double negatives but the substance will remain the same)

TO:

RCMP ATIP Branch

Email: ATIP / AIPRP ATIP-AIPRP@rcmp-grc.gc.ca;

Kind attention:

Beaudoin, Tina (RCMP/GRC) tina.beaudoin@rcmp-grc.gc.caLarkin, Bryan (RCMP/GRC) Bryan.Larkin@rcmp-grc.gc.ca;Brisson, Stéphane (RCMP/GRC) stephane.brisson@rcmp-grc.gc.ca;Simpson, Melissa (RCMP/GRC) melissa.simpson@rcmp-grc.gc.ca

And others

SUBJECT: RE: ACCESS TO INFORMATION ACT REQUEST A-2026-00761 / F339 – RESPONSE TO MS. TINA BEAUDOIN’S EMAIL OF TODAY’S (JUNE 16, 2026) DATE

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

INTRODUCTION AND PRELIMINARY OBSERVATIONS

<i>A. INTEGRATION OF THE FACTUAL RECORD</i>

1. Receipt is hereby formally acknowledged concerning the electronic correspondence disseminated by the government institution (the “**Government Institution**” or “Institution”) on June 16, 2026. The **Institutional** postulation that the substantive access to information request (the “**Access To**

Information Request”) which was delivered to the RCMP on April 14, 2026, bearing file designation A-2026-00761, remains situated within a routine retrieval stage is **categorically repudiated** as being entirely bereft of legal foundation.

- 2. I adopt the definitions from previous correspondence for ease of reference.
- 3. I refer to myself in the third person for ease of reference and convenience, and for situational and context purposes.
- 4. I understand that Ms. Beaudoin is a federal team leader with ATIP since March 2018.
- 5. The aforementioned correspondence explicitly concedes that no statutory extensions were effectuated upon the operative file. This is a false statement on a de facto and de jure basis. While no legal statutory extensions were taken under the applicable section of *ATIA*, there have been vague references to 60 day time extensions to make a complaint. The time to make a complaint is at the time of the purported or alleged extension.
- 6. Through the formalization of this specific admission, the absolute crystallization of a statutory default on the part of the Royal Canadian Mounted Police is irrevocably confirmed. The recipients are hereby formally directed to govern subsequent actions in strict adherence to the delineated legal realities.

2.0 CHRONOLOGICAL MATRIX AND STATUTORY DEFAULT

B. TABULAR REPRESENTATION OF THE ACTA

- 3. The following tabular representation meticulously delineates the objective procedural timeline, fundamentally eviscerating any **Institutional** claim to ongoing administrative processing latitude:

Date	Procedural Event	Statutory Implication
April 14, 2026	Constructive possession of the Access To Information Request and the statutorily prescribed financial instrument of five dollars.	Immediate commencement of the non-discretionary thirty-day statutory processing limitation.
April 23, 2026	Institutional demand for clarification and unlawful threat of file closure.	An <i>ultra vires</i> mechanism engineered to orchestrate spoliation by delay and a nullity <i>ab initio</i> .
May 4, 2026	Arbitrary Institutional deadline demanding clarification regarding the physical location of personal information bank (the “ Personal Information Bank ”) RCMP PPU 005.	A fundamentally impermissible statutory interpretation designed to subvert the paramount right of access.
May 14,	Expiration of the paramount statutory limitation period.	Crystallization of a deemed refusal under <i>Subsection 10(3)</i> of the <i>Access</i>

		<i>to Information Act.</i>
June 15, 2026	Dissemination of the final legal notice of default.	Integration of the deemed refusal as compounding evidence of bad faith into active litigation.
June 16, 2026	Institutional admission that the file remains in the retrieval stage and no extensions were taken.	Absolute forfeiture of residual administrative discretion.
June 17, 2026	Impending interlocutory proceeding in the Federal Court of Canada.	Adjudication of the failure to adhere to the non-discretionary mandate of <i>Rule 318</i> of the <i>Federal Courts Rules</i> .

3.0 ALLEGATIONS OF FORGERY AND THE DOCTRINE OF SPOILIATION

C. CRYPTOGRAPHIC PROVENANCE AND PUBLIC INTEREST DISCLOSURE

4. The foundational requisition was explicitly formulated to compel the extraction or disclosure of unredacted audit trails, transaction ledgers inherent to the Canadian police information centre (the “**Canadian Police Information Centre**”), and systemic governance manuals. The profound necessity of this overarching public interest disclosure is predicated upon severe, substantiated allegations of warrant forgery perpetrated via portable document format (the “**Portable Document Format**”) manipulation software.

5. The central operational matrix of the Canadian criminal justice paradigm is entirely predicated upon the unbroken chain of custody inherent to sworn judicial instruments. When the cryptographic provenance of a formally sworn document is deliberately severed by state actors deploying commercial manipulation software to falsify jurisdictional realities, the resultant documentation ceases to operate as a lawful authorization. It devolves into a mere instrument of arbitrary coercion.

6. The overarching democratic imperative demands the preservation of the *status quo ante*, compelling rigorous adherence to the supreme governing principles established in *Landreville v. Town of Boucherville*, [1978] 2 SCR 801 (the “*Landreville Decision*”) and *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403 (the “*Dagg Decision*”), which dictate that fraud and synthetic document fabrication systematically unravel everything they touch.

4.0 CRYSTALLIZATION OF DEEMED REFUSAL AND JURISDICTIONAL NULLITY

D. THE ABSOLUTE EXTINGUISHMENT OF ADMINISTRATIVE DISCRETION

7. Insofar as a temporal duration significantly exceeding sixty days has elapsed since the crystallization of constructive possession, and noting the explicit **Institutional** admission that no legally valid statutory abeyance or extension was properly effectuated, the Government Institution has inexorably descended into an automatic state of deemed refusal.

8. Such a transgression of paramount legislative dictates cannot be artificially diminished as a mere procedural irregularity; rather, owing to its direct contravention of the overarching parliamentary statute, it manifests as an absolute jurisdictional nullity *ab initio*. By strict operation of law, the effectuation of a deemed refusal completely eradicates any residual administrative discretion previously vested within the administrative apparatus.

5.0 ACTIVE FEDERAL COURT ENFORCEMENT AND MANDAMUS

E. THE INTERLOCUTORY PROCEEDING AND RULE 318

9. It must be articulated with unequivocal precision that the present statutory default is not tethered to a passive administrative queue. This profound **Institutional** default has been concurrently integrated as compounding *prima facie* evidentiary proof of bad faith directly into the active, unmitigated litigation presently situated before the Federal Court of Canada, bearing the designation of **Court File Number T-2448-26**.
10. The structural and procedural defaults perpetrated by the respondents—encompassing the total, inexcusable failure to adhere to the non-discretionary imperative codified within *Rule 318* of the *Federal Courts Rules*—shall be forcefully and vigorously prosecuted during the impending interlocutory proceeding on June 17, 2026.

F. THE PREROGATIVE WRIT OF MANDAMUS

11. It is advanced through complex syllogistic reasoning that the balance of convenience weighs overwhelmingly and absolutely in favor of the issuance of a prerogative writ of mandamus. A clear, positive, and non-discretionary public legal duty is affixed to the **Government Institution**; said executory duty is owed explicitly to the applicant; a formal demand has been effectuated *in limine*; and an absolute constructive refusal has materialized *ipso facto* through the expiration of strict temporal parameters.
12. While it is a recognized jurisprudential precept that mandamus cannot dictate a specific, discretionary substantive outcome, it possesses the absolute, unyielding authority to compel the performance of a specific, ministerial, and executory duty. The extraction of the requisitioned hexadecimal and routing metadata ledgers is not an exercise of administrative judgment, but rather a purely mechanical, technological imperative mandated by the statute. Any **Institutional** refusal to execute this technological extraction transcends a mere irregularity and constitutes a jurisdictional nullity.

- 762** 13. The Respondents' failure to serve and file a **Form 305 Notice of Appearance** does not block the operation of Rule 317 and Rule 318 under the Federal Courts Rules. While the Federal Courts Rules and ATIA are distinct in the former being a regulation and the latter being a statute, the analogy, consonance or parallel can be drawn involving the similar fact evidence of failing to comply with "Source Laws" or "Enactments" in an obstructionist manner.
14. Our relations herein are one of an access partnership and the RCMP ATIP Branch is failing not only me but the public.
15. By failing to step into the litigation formally, they are attempting to lock the court record, matching the exact "spoliation by delay" tactics they are executing within the ATIP branch. The Applicant will draw the same to the attention of the FCC with due dispatch.

6.0 STATUTORY PURPOSE AND THE CONTRAVENTION OF LEGISLATIVE INTENT

G. The Paramountcy of Accountability and Transparency

13. The foundational architecture of the *Access to Information Act* is explicitly codified within *Subsection 2(1)*, which unequivocally mandates the enhancement of the accountability and transparency of federal institutions. It is submitted that the deliberate obfuscation of metadata and the persistent suppression of chronological transaction logs fundamentally subvert this paramount statutory objective, a legislative framework enacted specifically to promote an open and democratic society and to enable robust, unimpeded public debate concerning the conduct of state institutions.
14. This democratic imperative is further operationalized by *Subsection 2(2)(a)* of the *Access to Information Act*, which enshrines a positive, quasi-constitutional right of access to records situated under the control of the Government Institution. The supreme governing principle dictates that state-held information must be made intrinsically available to the public sphere. Concomitantly, any requisite exceptions to this overarching right of access are legally compelled to be construed as stringently limited and highly specific. The **Institutional** deployment of manufactured administrative ambiguities and unenumerated extensions to forestall disclosure manifests as a direct contravention of this principle of narrow interpretation, effectively shielding **Institutional** conduct from the independent review mandated by the legislature.

H. Proactive Disclosure and Syllogistic Extrapolation

15. Moreover, in contemplation of *Subsection 2(2)(b)* of the *Access to Information Act*, which establishes stringent requirements for the proactive publication of information, the systemic failure to surrender the requisitioned audit trails elucidates a profound departure from the doctrine of proactive transparency. Through the application of complex syllogistic reasoning, it becomes intrinsically self-evident that the continued obstruction of these cryptographic matrices transcends mere procedural irregularity; it constitutes an absolute jurisdictional nullity and a substantive evisceration of the fundamental democratic oversight expressly envisioned by the Parliament of Canada.

7.0 COMPLAINT TO THE OFFICE OF THE INFORMATION COMMISSIONER

I. Incontrovertible Chain of Custody and the Fiction of Administrative Delay

16. It is formally recorded that the *ultra vires* delays engineered by the ATIP Branch necessitated the institution of a formal investigative complaint before the office of the information commissioner (the “**Office of the Information Commissioner**”), distinct from the Office of the Privacy Commission, on April 24, 2026. This complaint meticulously delineated the deliberate **Institutional** subversion of binding statutory timeframes through the issuance of an extra-statutory demand for clarification, coupled with an unlawful threat to summarily terminate the processing of the requisition.
17. The physical package encompassing the formal requisition, inclusive of the statutorily prescribed application fee in the form of a certified financial instrument, was transmitted via Canada Post Xpresspost and objectively delivered on **April 14, 2026**. Internal bureaucratic inefficiencies cannot be weaponized by the state to unlawfully abridge an applicant’s statutory timelines or retrospectively alter the legally operative date of receipt.

J. THE SUBSTANTIVE NULLITY OF THE SECTION 6 “CLARIFICATION” DEMAND

18. The **Institutional** attempt to invoke *Section 6* of the *Access to Information Act*—predicated upon a feigned inability to comprehend a requisition drafted with unparalleled forensic precision—was formally denounced as an absolute statutory nullity. The requisition explicitly targeted specific algorithms, originating agency identifiers, media access control addresses, and hexadecimal mainframe dumps. The assertion that an experienced employee fails to understand standard enterprise-level IT nomenclature is an administrative fiction designed solely to orchestrate spoliation by delay.
19. The initial access request under *ATIA*, which I have defined through as “*ATIA* Request #1” explicitly targeted infrastructure metadata and systemic mainframe transaction logs, which are not personal information bank records. Demanding a clarification based on an irrelevant personal data category to delay a structural IT infrastructure search is a bad-faith application of Section 6 of the Act.

8.0 APPENDIX A: MANDATORY PRODUCTION FORMATS FOR CPIC RECORDS

K. THE STRICT PRESERVATION OF NATIVE DIGITAL ARCHITECTURE

19. To preemptively forestall any subsequent, disingenuous **Institutional** assertions of technical incomprehension regarding the specific database artifacts requisitioned, the following matrix delineates the exact, immutable morphology of the requested categories of CPIC records. Any substantive deviation from these rigorous, native data structures—specifically the unauthorized substitution with homogenized, graphical presentation summaries—shall be construed *prima facie* as a deliberate, sanctionable spoliation of electronic records.

Item No.	Requisition Category	Contextual Justification and Legal Imperatives	Mandatory Format of Production (Native Architecture)

1.	Investigative Data Bank Audit Trails	The graphical interface accessible to a patrol officer is subjected to algorithmic filtering. Only the immutable systemic ledgers housed deep within PPU 005—capturing the precise chronological sequence of ADD, MODIFY, CLEAR, and CANCEL commands—can definitively expose the temporal trajectory of state-actor malfeasance.	Native tabular database extractions (e.g., CSV, SQL output) derived directly from the mainframe transaction ledger, strictly preserved without redaction of operational syntax or timestamp modification.
2.	Hexadecimal Mainframe Dumps	This mathematical data is strictly required to bypass the visual homogenization inherent to the standard graphical user interface. Only the uninterpreted binary and hexadecimal records—complete with exact cryptographic memory offsets and decoded text translations—can provide the absolute mathematical certitude required to prove vector morphology collapse.	Raw, continuous hexadecimal and binary outputs (e.g., .HEX files or raw binary dumps), purposely bypassing the visual homogenization inherent to the graphical user interface.
3.	Hardware and Terminal Metadata	This data is critical to irrevocably establishing the physical and geographical locus of the data entry, directly invoking the foundational legal maxim <i>nemo dat quod non habet</i> (no one gives what they do not have).	Extracted network session logs explicitly delineating ORI routing codes, MAC addresses, and IP assignments associated with the session token.
4.	Inter-Agency Communication Logs	A systemic error of this profound magnitude does not exist in a vacuum; a highly documented administrative paper trail of IT professionals attempting to reconcile the corrupted digital artifacts is inevitably created, especially regarding the absolute failure of the mandatory matching protocol.	Internal IT troubleshooting ticket exports (e.g., native ServiceNow, Jira data outputs) and raw systemic error alerts generated automatically by the CPIC input gateway parsing engine.

5.	PDF Flattening and Vector Analysis Reports	Forensic analysis confirms enterprise-level developer software was utilized with the specific <i>mens rea</i> to unlawfully flatten the document, forcefully eradicate the transparent electronic image signature, and algorithmically disfigure the underlying text to bypass standard criminal intake procedures.	Native system alerts, proprietary software ingestion logs, and raw vector diagnostic exports demonstrating morphological collapse.

9.0 JURISPRUDENTIAL FRAMEWORK: STATUTORY DEADLINES AND DEEMED REFUSALS

L. THE NON-DISCRETIONARY THIRTY-DAY MANDATE

20. It is a well-established jurisprudential precept that the strict temporal limitations imposed upon government institutions under the *Access to Information Act* are foundational to the operationalization of democratic transparency. Pursuant to *Section 7* of the *Access to Information Act*, a non-discretionary public legal duty is affixed to the Government Institution to render written notice regarding the requested records within thirty days.
21. The jurisprudence articulated in *Rundel v. Canada*, *Coderre v. Canada*, and *Teal Cedar Products Ltd. v. Canada* unequivocally predicates judicial intervention upon the **Institutional** failure to strictly adhere to this baseline statutory deadline. A contravention of this temporal mandate is decidedly not a mere procedural irregularity; owing to its evisceration of the citizen’s right to prompt access, it is an absolute jurisdictional nullity.

M. The Doctrine of Deemed Refusal

22. Upon the expiration of the initial thirty-day limitation period, absent a procedurally valid and properly enumerated extension, the institution descends automatically into a state of deemed refusal, codified within *Subsection 10(3)* of the *Access to Information Act*.
23. As authoritatively established by the Federal Court of Appeal in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56, and further elucidated in *Iris Technologies Inc. v. Canada*, the expiration of this deadline without a legally operative extension instantaneously vests the applicant with the absolute right to seek extraordinary **equitable remedies**.
24. It is trite that the relief sought in my FCC Application of May 15, 2026, seeks various equitable remedies including what were known as ancient prerogative writs like mandamus and prohibition.
25. The failure to produce the Records operates as a continuous statutory breach, thereby empowering the reviewing courts to issue a prerogative writ of mandamus to compel executory performance.
26. Under the *Minister of National Defence* FCA framework, once a 30-day timeline expires without a formal *Section 9* extension, the institution is stripped of all processing latitude. A self-serving

administrative claim that a file is in a “retrieval stage” cannot legally toll a crystallized statutory default. Again, the reference to another 60 days for a complaint to be exercised is not founded in any “Source Law” or jurisprudence. If you feel that the Applicant is incorrect, kindly cite some authority in this regard.

27. As such, this document will be relied upon for lawful purposes with notice.

N. Judicial Scrutiny of Unenumerated Extensions

24. Furthermore, as codified in *Biogénie Canada Inc. v. Canada*, the reviewing courts apply exacting scrutiny to determine whether an **Institutional** attempt to artificially toll the foundational thirty-day window is genuinely supported by objective evidentiary realities. Extra-statutory delays, manufactured administrative ambiguities, or unenumerated extensions are invariably classified as *ultra vires* actions, thereby rendering the subsequent withholding of information a fundamentally impermissible exercise of state authority.

10.0 FINAL CONCLUSION AND RESERVATION OF RIGHTS

O. Comprehensive Preservation of Equitable Entitlements

25. The Government Institution is strictly prohibited from preemptively conflating the anticipated application of an exemption with the primary duty to conduct the mandated digital extraction. All rights, privileges, and remedies, whether existing in fact, at common law, or in equity, are hereby comprehensively and irrevocably reserved.

26. Govern yourselves accordingly.

Respectfully submitted,

/s/Mr. Kevin A. McLean (BA, JD, CIM)

Mr. Kevin A. McLean (BA, JD, CIM)
Chartered Investment Manager

On Tue, Jun 16, 2026 at 7:47 AM Beaudoin, Tina (RCMP/GRC) <tina.beaudoin@rcmp-grc.gc.ca> wrote:

Good morning,

I am writing to provide a status update further to your recent inquiry.

Your request is currently in the retrieval stage, and efforts are ongoing to identify and collect all records responsive to your request. Kindly note that no extensions were taken on your file. Rest assured that your request continues to be actively processed, and a response will be issued once all required steps have been completed.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada

30 Victoria Street, 7th Floor

Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:

<https://www.oicci.gc.ca/en/submitting-complaint>

We appreciate your patience and understanding in this matter.

Tina Beaudoin

From: Mr. Kevin McLean <mcleansettlement@gmail.com>

Sent: June 15, 2026 1:54 AM

To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>; Simpson, Melissa (RCMP/GRC) <Melissa.Simpson@rcmp-grc.gc.ca>; Brisson, Stéphane (RCMP/GRC) <Stephane.Brisson@rcmp-grc.gc.ca>; Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>; Mirsky, Tanya (RCMP/GRC) <Tanya.Mirsky@rcmp-grc.gc.ca>; Larkin, Bryan (RCMP/GRC) <Bryan.Larkin@rcmp-grc.gc.ca>

Subject: Re: Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

Date: June 15, 2026

**SUBJECT: IMMEDIATE LEGAL NOTICE: ATIA REQUEST A-2026-00761 / F339 —
DEEMED REFUSAL UNDER LAW AND URGENT STRATEGIC NOTICE OF
PENDING FEDERAL COURT ENFORCEMENT (COURT FILE NO. T-2448-26)**

DELIVERY METHOD:

Via Electronic Transmission & Immediate Record Logging into Federal Court File T-2448-26

TO:

- **Mr. Bryan Larkin**, Acting Commissioner, Royal Canadian Mounted Police (Bryan.Larkin@rcmp-grc.gc.ca)
- **Mr. Stéphane Brisson**, Chief Privacy Officer and Director General, ATIP Branch (stephane.brisson@rcmp-grc.gc.ca)
- **Ms. Melissa Simpson**, Access to Information and Privacy Branch (melissa.simpson@rcmp-grc.gc.ca)
- Ms. Tanya Mirsky;
- Mr. Jeff Ball
- **Central ATIP Intake Branch**, Royal Canadian Mounted Police (ATIP-AIPRP@rcmp-grc.gc.ca)

REFERENCE: Formal Requisition under the Access to Information Act (*ATIA*) — File A-2026-00761 / F339 (unlike the botching on the Privacy Act request referencing "2025" (sic))

CONCOMITANT JUDICIAL PROCEEDING: Federal Court of Canada, Court File Number: T-2448-26

UPCOMING MOTION HEARING: June 17, 2026 (Motion Number One)

UPCOMING HEARING ON THE MERITS: June 29 OR 30, 2026 (Hearing for Requisition) (nota bene: prior to the summer recess when general sittings of the FCC are less abundant)

Dear Acting Commissioner Ms. Larkin, Chief Privacy Officer Monsieur Brisson, Ms. Mirsky, Mr. Ball and Ms. Simpson,

1. This correspondence serves as an unyielding, final legal notice identifying the total statutory default and crystallization of a Deemed Refusal by the Royal Canadian Mounted Police (RCMP) as of today, **June 15, 2026**. This notice links the ongoing administrative evasions of the RCMP ATIP Branch directly into the active, unmitigated litigation currently pending before the Federal Court of Canada in **Court File Number: T-2448-26** (Motion Rec... p. 1).
2. As you know, this *ATIA* request has been outstanding since April 14, 2026, but to assist Acting Commissioner Mr. Larkin, and the response by Ms. Simpson on April 28, 2026, was not compliant with *ATIA* in terms of what appears to be an arbitrary, unlawful and unknown to the Parliamentary statute in *ATIA* purported extension of time
3. To ensure that any reviewing body fully grasps the structural gravity of the records being withheld, the depth of the seven targeted technical classifications is detailed below. These items represent the inescapable operational footprint of the CPIC database (p. 22):

INVESTIGATIVE DATA BANK AUDIT TRAILS (RCMP PPU 005):

- a. Restricted to the critical temporal epoch of **September 22 to October 4, 2024** (p. 3). Frontline Graphical User Interfaces (GUIs) show only contemporaneous operational filtering (pp. 3, 21). Only the deep, immutable ledger captures the exact chronological sequence of ADD, MODIFY, CLEAR, and CANCEL commands, exposing when a state actor sought to excise data to mask an unlawful arrest (p. 3).

HEXADECIMAL MAINFRAME DUMPS:

- b. The raw binary logs associated with the target warrant (p. 3). The presentation layer of a standard user terminal can be disfigured to display a facially valid warrant (p. 4). Only uninterpreted hexadecimal dumps reveal cryptographic memory offsets and EBCDIC decoded translations, proving the exact moment a document's morphology collapsed (p. 4).

HARDWARE AND TERMINAL METADATA:

- c. The internal ORI mappings, Media Access Control (MAC) addresses, and hardware IP pathways used during the target sessions (p. 4). Invoking *nemo dat quod*

non habet, if a document supposedly authorized by a Superior Court Chief Justice was actually inputted from a municipal police division’s back-office terminal, the ORI codes will incontrovertibly expose the jurisdictional nullity (p. 4).

INTER-AGENCY COMMUNICATION LOGS:

d. All internal emails, system alerts, and IT troubleshooting tickets shared between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch (p. 4). This explicitly isolates the communications regarding the catastrophic failure of the mandatory “Matching Protocol” during the ingestion of corrupted judicial initials (p. 4).

PDF FLATTENING AND VECTOR ANALYSIS REPORTS:

e. All system logs concerning OCR interpretation failures or “whitespace bugs” caused by the deployment of the GrapeCity Documents PDF suite (version 6.0.2.0, bug DOC-6507) (p. 5). This software was weaponized with explicit *mens rea* to violently flatten a document, erase the transparent electronic signature of Chief Justice Geoffrey B. Morawetz, and superimpose a civilian clerk’s digital certificate as a visual smokescreen (p. 5).

OFFLINE HISTORICAL SEARCH RESULTS:

f. The unredacted results of the specialist search into the Investigative Data Bank archives (p. 5). This is required to pierce the chronological impossibility of an arrest executed on October 2, 2024, followed by an immediate provincial system expungement on October 3, 2024, alongside retaliatory cybersecurity blocking via a 403 Forbidden Error (p. 5).

SYSTEM GOVERNANCE MANUALS:

g. Unredacted copies of the CPIC Reference Manual and Memorandums of Understanding governing the “Judicial Firewall” (p. 5). This evidence is vital to demonstrating exactly how the mandatory “Air Gap” separating the independent judiciary from law enforcement entry teams was compromised (p. 5).

4. I draw your attention to section 9 of the *ATIA* which states:

“Extension of time limits

9 (1) The head of a government institution may extend the time limit set out in section 7 or subsection 8(1) in respect of a request under this Part for a reasonable period of time, having regard to the circumstances, if

(a) the request is for a large number of records or necessitates a search through a large number of records and meeting the original time limit would unreasonably interfere with the operations of the government institution,

(b) consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit, or

(c) notice of the request is given pursuant to subsection 27(1)

by giving notice of the extension and, in the circumstances set out in paragraph (a) or (b), the length of the extension, to the person who made the request within thirty days after the request is received, which notice shall contain a statement that the person has a right to make a complaint to the Information Commissioner about the extension.

Notice of extension to Information Commissioner

(2) Where the head of a government institution extends a time limit under subsection (1) for more than thirty days, the head of the institution shall give notice of the extension to the Information Commissioner at the same time as notice is given under subsection (1).”

5. While section 9 of the *ATIA* is distinct in some respects from section 15 of the *Privacy Act*, the question arises based upon the Ms. Simpson email if you do not comply with providing access by tomorrow because it would exceed more than 30 days as to whether you have notified the Commissioner. If you do not do so and do not provide full, complete and lawful disclosure of the requested Records, I will notify if the Commissioner unless you represent to me that you have done so with a copy of said letter on a forthwith basis.

6. For Ms. Simpson’s edification, the time limit of extension commences when the access request is received, which was April 14, 2026 so the 60 days would have commenced, if valid which it was not on April 14, 2026, and with 31 days in May 2026,

it would have been on **June 13, 2026**, but that was a Saturday so one must expect forthwith production, access and disclosure tomorrow morning.

7. Moreover, since the notice required to the Commissioner under ss. 9(2) of the *ATIA* would have been required at the time given and not at the time of receipt of the notice as Ms. Simpson would have it (see: Appendix).

FINAL EXPIRATION OF THE STATUTORY CONTINUUM AND NOTICE OF DEEMED REFUSAL

8. The final, non-negotiable statutory window for the RCMP to deliver complete, unredacted access to the architectural metadata governing the Canadian Police Information Centre (CPIC) database has officially closed today, June 15, 2026. While I have continuously rejected your branch's procedurally defective attempts to use Section 6 of the *ATIA* to feign a systemic inability to comprehend basic database arrays, your administrative processing latitude is now entirely exhausted.

9. Because no responsive records, phased disclosures, or rolling extractions have been delivered by the close of business on this date, the RCMP is in a state of absolute statutory default. Pursuant to Section 10(3) of the *ATIA*, this default operationalizes an absolute **Deemed Refusal**. By operation of law, this text completely strips the head of the institution of any remaining administrative discretion or processing flexibility over this file.

IMMEDIATE INTEGRATION INTO ACTIVE FEDERAL COURT PROCEEDING T- 2448-26

10. Let there be no ambiguity: this default will not be deferred to external regulatory complaint structures. It is being injected directly into the active litigation before the Federal Court of Canada (Motion Rec... p. 1). As documented in the attached **Motion Record filed on June 10, 2026**, the Respondents are already in profound procedural default for failing to serve and file Form 305 Notices of Appearance within the mandatory 10-day window (Motion Rec... pp. 1, 26). You are explicitly reminded that under the strict terms of Form 301, your failure to oppose this application means judgment may be rendered in your absence and without further notice (Motion Rec... p. 1).

11. The ongoing refusal to search for and extract the raw hexadecimal mainframe logs and Personal Information Bank (PIB) RCMP PPU 005 audit trails is a continuation of

the exact institutional recalcitrance detailed in my pending motion (Motion Rec... pp. 1, 14). This statutory default will serve as immediate, compounding evidence of bad faith and a total failure to perform public legal duties (Motion Rec... pp. 31-32).

**THE NON-DISCRETIONARY MANDATE OF RULE 318 AND THE UPCOMING
JUNE 17, 2026 MOTION**

12. Your attention is directed to **Notice of Motion Number One**, which is formally scheduled to be heard and decided by the Federal Court on **Wednesday, June 17, 2026, at 9:30 a.m.** (Motion Rec... p. 24). This motion proceeds entirely unopposed due to your structural default (Motion Rec... pp. 2, 20).

13. The relief sought on June 17, 2026, focuses on the RCMP's flagrant contravention of its mandatory duties under **Rule 318 of the Federal Courts Rules** (Motion Rec... pp. 1, 25). Under Rule 318(1), the tribunal has no discretion: it *shall* transmit a certified copy of the requested material to the Registry within 20 days (Motion Rec... p. 2). You have failed to comply, failed to file a formal objection, and instead elected to remain silent (Motion Rec... pp. 40-41). This Court will be forcefully asked to:

- a. Issue a **Mandatory Order** compelling the RCMP Tribunal to fully comply with Rule 318 by transmitting the complete Certified Tribunal Record within twenty-four (24) hours of the order (Motion Rec... p. 25);
- b. Grant the Applicant explicit leave to bring immediate **Contempt Proceedings** against the specific institutional and individual actors facilitating this intentional breach (Motion Rec... p. 25).

14. Any such failure to comply with the *ATIA*, having failed to even have conducted a search in the *Privacy Act* request of myself from early March 2026, along with having failed to have complied with my second *ATIA* request of May 7, 2026, will be further evidence in support of some or all of the above and contained in the Motion Record #1.

15. I can also confirm that I have paid the "Requisition for Hearing – Application" as of Friday, June 12, 2026, which is to be set for June 29 or 30, 2026.

**JUDICIAL ENFORCEMENT OF SECTION 8(2)(M) AND SECTION 19 AT THE
JUNE 29/30, 2026 HEARING**

16. The crystallization of today's Deemed Refusal provides the final evidentiary bridge required for the upcoming **Hearing for Requisition scheduled for June 29 and 30, 2026**. At this upcoming hearing, the Federal Court will exercise its full superintending and equitable jurisdiction to adjudicate the core failures that your branch has desperately sought to conceal (Motion Rec... pp. 25, 32). Specifically, the court will directly enforce:

- a. **The Mandatory Discretion Under Section 8(2)(m) of the *Privacy Act*:** The total failure of the RCMP Commissioner to turn his mind to or exercise his statutory duty to consider the public interest override (Motion Rec... pp. 26, 31).
- b. **The Application of Section 19 of the *ATIA*:** Piercing the institutional stonewalling regarding purely professional metadata—such as Originating Agency Identifier (ORI) mapping, MAC addresses, and EBCDIC decoded text translations (Motion Rec... pp. 3, 14).

17. The depth of the evidence now filed in Court File No. T-2448-26 proves that the underlying documents—including the disfigured Ontario “Information Package” bearing commercial GrapeCity Software version 6.0.2.0 metadata—are absolute jurisdictional nullities *ab initio* (Motion Rec... pp. 5, 33, 38). Under the supreme governing principles established in *Landreville v. Town of Boucherville*, fraud, bad faith, and synthetic document fabrication unravel everything they touch (Motion Rec... pp. 8, 32).

**5. FINAL WARNING, STRICT LITIGATION HOLD, AND STATUTORY HOLD
MANDATE**

18. The RCMP through its ATIP Branch cannot leverage the technical complexity of decentralized databases or internal mailroom delays to insulate ultra vires state action from the superintending purview of the Federal Court (Motion Rec... pp. 36, 41, 43).

19. The formal litigation hold and anti-spoliation mandate remains fully active. Any routine or algorithmic overwriting of the raw PPU 005 audit trails, network terminal cache memory banks, or system error alerts generated during the September-October 2024 epoch will be treated *prima facie* as a **criminal obstruction of justice** and intentional spoliation of evidence (Motion Rec... p. 14).

20. While the Respondents have failed to appear in the FCC and defaulted on their obligations under Rule 318 of the Federal Courts Rules, the pending motions is up in the Federal Court of Canada on June 17, 2026, and at the final argument on June 29 or 30, 2026.

I trust whomever was behind this sort of misconduct is on leave and will be terminated. To be engaged in that sort of fraudulent manipulation of documents in any proceeding let alone a criminal

proceeding and to allow that kind of charade and fraud on the court is unforgivable. It nearly killed me but I am still standing through some sort of divine intervention.

21. I reserve all of my rights in fact and at law.

22. Govern yourselves accordingly.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

Enclosures

APPENDICES

<i>APPENDIX #1:</i>

ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>

Apr 28, 2026, 2:03 PM

to me

Dear Kevin Mclean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.
- Hexadecimal Mainframe Dumps: The raw, unadulterated “Hexadecimal Dumps” from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.
- Hardware and Terminal Metadata: The internal “Originating Agency Identifier” (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the “Frankenstein” Information Package.
- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.
- DF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or “whitespace bugs” during the processing of judicial PDF instruments.

777 - Offline Historical Search Results: The complete, unredacted results of the mandatory “Offline Search” conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.

- System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the “Matching Protocol” and the “Judicial Firewall.”

In order to process your request we require additional information:

- Location: Regarding the first point in your request, “Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.”- Please be advised that PIB PPU 005 is not a singular database, PIBs themselves are not a singular database but rather a way the government collects and stores personal information. Please specify which data base/location you would like to have searched.

You may reply to this email.

Please respond by May 4, 2026.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada

30 Victoria Street, 7th Floor

Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:
<https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

On Thu, May 14, 2026 at 9:25 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Date: May 14, 2026

Classification: Private and Confidential

Subject I: Expiration of Statutory Mandate, Crystallization of Deemed Refusal, and Procedural Nullity of Unenumerated Time Extension – File A-2026-00761 / F339

Subject II: Formal Requisition for Mandatory Consideration of Public Interest Disclosure pursuant to Section 19(2)(c) of the Access to Information Act

Sending method: Via Email

Your file number: A-2026-00761 / F339

To:

Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

779 (nota bene: inclusion of Mr. Ball (a director of ATIA and Privacy Branch and included due to crossover between section 8(2)(m) and section 19 of ATIA) and Ms. Tanya Mirsky whom was included by Mr. Ball and I understand to be a chief of staff)

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

1.0. Introduction, Provision of Foundational Acta, and the Doctrine of Constructive Possession

1.1. Correspondence is hereby formally directed regarding the aforementioned matters and the concurrent, interwoven statutory obligations affixed to the institution. It is submitted that the present matter transcends standard administrative inquiries and strikes directly at the foundational cryptographic integrity of the national law enforcement apparatus.

1.2. Appended hereto are the foundational documentary instruments and acta necessary for the adjudication of the principles articulated herein. These records irrevocably establish the chronological matrix and the consequent, unmitigated expiration of the statutory processing period. The incontrovertible evidence of delivery acts as the catalyst for the crystallization of the institution's strict statutory obligations.

1.3. It is categorically advanced that the chronological matrix is governed absolutely by the doctrine of constructive possession. The physical package encompassing the primary requisition, inclusive of the statutorily prescribed financial instrument, was transmitted via independent, state-sanctioned logistical frameworks. The objective delivery confirmation undeniably establishes receipt by the centralized institutional facility on April 14, 2026. At the precise moment the official representative of the state-sanctioned carrier executed the transfer of possession to the institutional receiving facility, the document entered the constructive and legal control of the government institution.

1.4. Internal bureaucratic inefficiencies, deliberate sorting bottlenecks, or localized lethargy in routing documentation from a centralized mail receiving facility to the specific intake analysts operating within the access to information and privacy branch (the "**ATIP Branch**") possess precisely zero legal capacity to artificially alter the statutorily operative date of receipt. The institutional obligations crystallized instantaneously upon physical delivery; any subsequent internal computation utilizing a delayed processing date is a mathematical and administrative fiction entirely unsupported by the *lex terrae*.

1.5. To permit an institution to unilaterally dictate the commencement of the statutory clock based entirely upon internal administrative convenience would be to completely subvert the quasi-constitutional nature of access legislation. The Supreme Court of Canada has consistently affirmed that the right of access is foundational to democratic accountability; therefore, the statutory timelines designed to facilitate that access must be strictly construed against the state and generously construed in favor of the applicant. The commencement date is irrevocably fixed, rendering the expiration date equally immutable.

2.0. The Absolute Procedural Nullity of the Unenumerated Time Extension and the Prohibition of Extra-Statutory Abeyance

2.1. It is formally recorded that the strict statutory limitation period for the provision of the requisitioned records has irrevocably expired as of May 14, 2026. The institution is presently

devoid of any lawful authorization to withhold the demanded metadata.

2.2. It is acknowledged that the institution previously disseminated correspondence purporting to rely upon a time extension (the "**Time Extension**"). However, it is forcefully advanced that the aforementioned correspondence completely neglected the mandatory statutory imperative to meticulously cite the operative subsections or clauses under section 9 of the *Access to Information Act* (the "**ATIA**").

2.3. By neglecting to formally invoke any of the constituent conditional subsections—specifically, the necessity of processing voluminous records pursuant to section 9(1)(a), the requirement for mandatory inter-departmental consultations pursuant to section 9(1)(b), or the explicit mandate for third-party notifications pursuant to section 9(1)(c)—the institution has effectively provided a tacit legal admission that none of the statutorily permissible circumstances for delay are actually present. An extension cannot exist in a jurisdictional vacuum; it must be tethered to a specific, enumerated legislative allowance.

2.4. Consequently, the purported extension constitutes a fundamental, explicit contravention of the statutorily prescribed schema. It is decidedly not a mere administrative irregularity or a curable defect of form; rather, owing to its direct contravention of a federal statute governing quasi-constitutional rights, it manifests as an absolute jurisdictional nullity *ab initio*. A nullity cannot be subsequently ratified or breathed into life by administrative fiat.

2.5. This principle is unequivocally ratified within federal jurisprudence. As authoritatively established by the Federal Court of Appeal in *Statham v. Canadian Broadcasting Corporation*, 2010 FCA 315 (the "*Statham Decision*"), and reinforced consequentially in *Hydro-Québec v. Canada (National Energy Board)*, 1997 CanLII 16223 (FC) (the "*Hydro-Québec Decision*"), an institutional failure to formally, explicitly, and contemporaneously notify an applicant of the precise statutory justifications for a delay operates as a fatal procedural breach. The reviewing courts have definitively concluded that Parliament did not intend to grant institutions a blanket, unreviewable power to delay access; the requirement to specify the subsection is the foundational accountability mechanism ensuring the delay is genuinely warranted.

2.6. Furthermore, as articulated with absolute clarity in *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2015 FCA 56 (the "*National Defence Decision*"), an invalid, procedurally defective, or entirely absent extension ensures that the original statutory clock remains completely uninterrupted. The legal fiction of the unenumerated extension simply evaporates, leaving the original thirty-day mandate fully operative.

2.7. **Nota Bene:** It is anticipated that the institution might subsequently attempt to retroactively cure this procedural defect by asserting an implied reliance upon administrative burdens, sheer volume, or external consultation requirements in future correspondence. Such an *ex post facto* rationalization is legally barren and must be summarily rejected. The doctrine of *expressio unius est exclusio alterius* mandates that statutory exceptions must be expressly invoked at the time they are relied upon. A failure to explicitly articulate the foundational clause *in limine* ensures that the original statutory clock remains uninterrupted and fully active. The institution is presently operating in a state of constructive refusal.

2.8. **Nota Bene:** Furthermore, any institutional reliance upon a manufactured demand for clarification under section 6 of the *ATIA* as a mechanism to unilaterally hold the statutory timeframe in abeyance is an *ultra vires* maneuver. The governing legislation contains no

781 statutory "pause" mechanism. The deployment of staggered, piecemeal clarification requests formulated weeks after the receipt of an exquisitely detailed, forensically precise requisition constitutes a recognized bad faith tactic designed solely to orchestrate spoliation by delay. The doctrine of paramountcy dictates that internal administrative policies cannot supersede explicit, mandatory statutory provisions enacted by the Parliament of Canada.

3.0. The Substantive Requisition, the Doctrine of Institutional Control, and the Paramount Duty to Search and Seize

3.1. To rigorously forestall any further administrative obfuscation, it is imperative to definitively reiterate the exact parameters of the foundational requisition. The extraction of specific digital artifacts was formally demanded, namely: raw hexadecimal mainframe dumps, immutable investigative data bank audit trails associated with personal information bank RCMP PPU 005, precise hardware and terminal routing metadata (encompassing originating agency identifiers, media access control metrics, and internet protocol assignments), comprehensive inter-agency communication logs, vector analysis reports, offline historical data archives, and system governance manuals.

3.2. It is categorically advanced that these digital artifacts and systemic ledgers reside absolutely within the statutory control of the institution. As the supreme governance authority and physical custodian of the Canadian Police Information Centre (the "CPIC") infrastructure, the institution exercises complete dominion over the mainframe architecture. The postulation that localized data was initially inputted by a municipal police force—frequently mischaracterized as the "originator control" principle—is wholly inapplicable to the systemic metadata, audit logs, and transaction ledgers generated automatically by the federal mainframe itself.

3.3. When a municipal actor engages the federal database, the interaction generates discrete, secondary data points (such as timestamps, network node routing paths, and system error codes) that are inherently authored and owned by the federal apparatus. Once data is injected into the federal apparatus, the corresponding digital footprint is *ipso facto* under federal control and fully subject to the strictures of the *ATIA*. The institution cannot artificially sever its ownership of the systemic architecture simply because a municipal actor utilized the interface.

3.4. Consequently, an absolute, positive statutory duty to execute a comprehensive search is immediately crystallized at the first instance. It is a fundamental tenet of administrative law that the obligation to locate and extract records is a distinct, preliminary operational mandate, entirely divorced from the subsequent, discretionary application of statutory exemptions. The institution is strictly prohibited from preemptively conflating the anticipated application of an exemption with the primary duty to conduct the search. A refusal to even interrogate the database on the speculative presumption that the resulting records might be exempt constitutes a catastrophic failure of the statutory duty to assist and a profound misunderstanding of the two-step processing paradigm.

3.5. Furthermore, should the extracted ledgers contain the personal information or personally identifiable information (the "PII") of third-party individuals other than the applicant (Mr. Kevin A. McLean), the institution is legally precluded from utilizing an "all-or-nothing"

withholding strategy. Section 25 of the *ATIA* mandates the rigorous application of the doctrine of severability. The institution must parse the record line-by-line, byte-by-byte.

3.6. Applying the foundational legal maxim *utile per inutile non vitiatur* (the useful is not vitiated by the useless), the institution is statutorily compelled to surgically sever any legitimate third-party personal information and disclose the remaining substantive metadata. For instance, if a network routing log contains the name of a civilian third party alongside the critical internet protocol address exposing a forged entry, the name must be redacted, but the metadata proving the structural collapse of the judicial instrument must be segregated and produced. The mere presence of third-party biographical data cannot be weaponized as a blanket justification to suppress the algorithmic reality of the underlying digital forgery.

3.7. **Nota Bene:** The institution may attempt to argue that the intermingling of municipal operational data with federal metadata renders the extraction technologically burdensome or legally ambiguous, thereby ostensibly excusing the failure to search. This postulation is a technical fiction and a legal nullity. The institution possesses enterprise-level database querying capabilities specifically designed to segregate audit trails based on precise temporal epochs and user identifiers. Any refusal to execute the search based on feigned technological paralysis or the misapplication of third-party privacy exemptions at the search phase constitutes an actionable subversion of the right of access.

4.0. Escalation to the Investigative Authority and the Crystallization of Extraordinary Judicial Remedies

4.1. In light of the aforementioned procedural nullity and the expiration of the operative timelines, formal notification is hereby provided that the issue of the fundamentally improper and *ultra vires* time extension shall be contemporaneously re-raised and prosecuted before the office of the information commissioner (the "**Office of the Information Commissioner**" or "**OIC**").

4.2. The crystallization of this deemed refusal empowers the investigative apparatus to bypass administrative friction and immediately compel the production of the foundational mainframe metadata.

4.3. It must be rigorously observed that pursuant to recent legislative amendments incorporated into section 36.1(1) of the *ATIA*, the Office of the Information Commissioner has undergone a profound jurisdictional transformation. No longer functioning merely as an advisory ombudsman restricted to issuing unenforceable recommendations, the OIC is now vested with explicit, binding order-making authority. Upon the substantiation of this constructive refusal, the investigatory body possesses the unmitigated statutory power to issue a formal, legally binding mandate compelling the immediate extraction and unredacted disclosure of the targeted hexadecimal dumps and systemic routing ledgers. The institution will be subjected to formal compliance orders.

4.4. Moreover, the crystallization of this deemed refusal on May 14, 2026, strips the institution of all discretionary latitude. The matter immediately ripens for extraordinary judicial remedies. The absolute right is fully preserved to seek an immediate prerogative writ of *mandamus* before the Federal Court of Canada.

4.5. The rigorous, multi-pronged legal test for the issuance of *mandamus* is conspicuously satisfied in the present circumstances: firstly, there exists a clear, non-discretionary public legal duty to act (the mandatory processing of the requisition under the *ATIA*); secondly, this

783 duty is owed directly to the applicant; thirdly, there is a clear right to the performance of that duty without extraneous administrative preconditions; fourthly, a formal demand has been explicitly articulated; and finally, a constructive refusal by the state apparatus to execute said duty has materialized through the expiration of the statutory deadline and the reliance on a void extension. An application for *mandamus* will inexorably expose the coordinated orchestration of spoliation by delay.

5.0. The Positive Statutory Obligation of the Head of the Government Institution and the Jurisprudential Imperative

5.1. Notwithstanding the systemic delays orchestrated by the administrative apparatus, an inescapable and non-delegable fiduciary obligation remains affixed to the head of the government institution (the "**Head of the Institution**"). Specifically, the Head of the Institution is statutorily compelled to meticulously evaluate whether a public interest disclosure is warranted regarding the profound institutional malfeasance previously delineated within the primary requisitions.

5.2. The underlying malfeasance involves profound documentary metamorphosis and an orchestrated vector morphology collapse. It has been extensively documented that enterprise-level developer software—specifically the GrapeCity Documents PDF suite, exploiting the documented DOC-6507 bounding-box anomaly—was utilized with precise *mens rea* to unlawfully flatten judicial instruments, forcefully eradicate transparent electronic image signatures, and algorithmically mutate underlying text strings to bypass standard criminal intake procedures.

5.3. This overriding obligation is inextricably rooted within the concomitant legislative frameworks governing the dissemination of federal records. The protections afforded to personal information must invariably be measured against the prevailing democratic imperative. Section 19(1) of the *ATIA* establishes the foundational prohibition against the disclosure of personal information; however, section 19(2)(c) of the *ATIA* immediately incorporates the explicit threshold for the overriding of localized privacy interests as codified within section 8 of the *Privacy Act* (the "**Privacy Act**"), specifically engaging the public interest override mechanism of section 8(2)(m).

5.4. It is a foundational precept of administrative law, as articulated by the Supreme Court of Canada in *Canada (Information Commissioner) v. RCMP*, 2003 1 SCR 66 (*the "RCMP Decision"*), that the Head of the Institution is strictly prohibited from issuing a boilerplate denial upon the mere detection of personal information. The statutory architecture mandates an active, non-delegable duty to exercise discretion and formally document the weighing of the public interest against the privacy invasion. A failure to conduct and document this rigorous balancing exercise constitutes a fundamental abdication of statutory jurisdiction and is universally recognized by the reviewing courts as a reversible error of law. The reviewing courts heavily scrutinize whether that discretion was exercised logically, transparently, and entirely free from improper motives or political interference.

5.5. The threshold for the public interest override, while exactingly high, is unequivocally met in the present circumstances. As delineated in *Mackenzie v. Canada (Minister of Health)*, 2006 FC 871 (*the "Mackenzie Decision"*) and *Fraser v. Canada (Attorney General)*, 2009 FC 272 (*the "Fraser Decision"*), a sharp, uncompromising distinction is drawn between matters of mere public curiosity or sensationalism and matters of genuine democratic public interest. The algorithmic disfigurement of Superior Court instruments, and the subsequent

784 subversion of the coercive apparatus of the state, strikes at the very heart of the democratic order. It represents a systemic corruption of the judicial supply chain, thereby easily vaulting the "clearly outweighs" standard demanded by the legislature.

5.6. Furthermore, the open court principle, robustly defended in *Ritchie v. Canada, 2016 FC 259* (the "*Ritchie Decision*"), dictates that when information is inextricably linked to the formal compulsion of the judicial system, the expectation of privacy is severely diminished, if not entirely extinguished. The utilization of the federal mainframe to manufacture a shadow justice system, shielded from public scrutiny by an impermissible invocation of the *Privacy Act*, is fundamentally anathema to this foundational constitutional principle. A justice system that operates on altered PDFs and falsified metadata is a system that has utterly lost the consent of the governed.

5.7. It is advanced through complex syllogistic reasoning that the alleged systemic algorithmic manipulation of the national law enforcement database—specifically the CPIC mainframe—fundamentally eclipses any residual privacy interests of the state actors involved in the initial transcription of the compromised data. As definitively expounded by the Supreme Court of Canada in *Dagg v. Canada (Minister of Finance), 19972 SCR 403* (the "*Dagg Decision*"), the fundamental legislative objective of access legislation is the rigorous, unyielding scrutiny of state action. Consequently, public officials engaged in the execution of official duties inherently possess a severely diminished expectation of privacy.

5.8. However, this diminished expectation is entirely obliterated when malfeasance is introduced. When these public officials abdicate their lawful mandates and actively deploy digital architecture to forge authorizations, they cease operating under the lawful execution of their duties. They operate merely under the "colour of authority." Any remaining vestiges of professional immunity are instantly evaporated.

5.9. Applying the foundational legal maxims curated by Herbert Broom, specifically *fraus omnia corrumpit* (fraud vitiates everything), *actus curiae neminem gravabit* (an act of the court shall prejudice no man), and *nemo dat quod non habet* (no one gives what they do not have), it becomes inherently self-evident that a judicial process infected by deliberate digital manipulation is irreparably compromised. A municipal agency possesses absolutely zero inherent jurisdiction to manufacture or disseminate a Superior Court warrant.

5.10. Therefore, the public interest in guaranteeing the cryptographic provenance and algorithmic integrity of the CPIC database is absolute. This overarching democratic imperative *ipso facto* and *prima facie* satisfies the rigorous standard codified within section 8(2)(m)(i) of the *Privacy Act*, as the preservation of the *status quo ante* undeniably outweighs any negligible invasion of the perpetrators' professional privacy. The names, terminal IDs, and ORI routing codes of state actors operating a federal database are professional metrics, not intimate biographical details.

5.11. Consequently, should the institution proceed with an application of the public interest override, the mandatory procedural safeguard codified within section 8(5) of the *Privacy Act* is immediately engaged, requiring proactive, written notification to the federal Privacy Commissioner to ensure rigorous ombudsman oversight over the state's calibration of transparency and privacy harms.

5.12. **Nota Bene:** It is ultimately cautioned that while the reviewing courts apply a deferential "reasonableness" standard to the ultimate opinion formulated by the Head of the Institution, an irrational determination—such as concluding that the professional anonymity

785 of state actors engaged in digital forgery supersedes the algorithmic integrity of the national warrant database—will unequivocally fail to survive even the most deferential judicial scrutiny. The Head of the Institution is bound by a positive obligation to explicitly document the balancing of these factors; a blanket refusal to engage in this statutory balancing exercise would constitute an actionable dereliction of duty, bereft of all reasonableness.

5.13. Nota Bene: The institution may attempt to posit the counter-argument that the disclosure of identifying metadata could precipitate the re-identification of specific law enforcement personnel via the mosaic effect. This postulation must be summarily discarded as a profound misapplication of the legislation. The identifying metadata sought—namely, originating agency identifier codes, terminal internet protocol addresses, and media access control metrics—constitutes purely professional, administrative metrics, entirely devoid of intimate biographical substance. The veil of statutory privacy must never be weaponized as an impenetrable sanctuary for the concealment of systemic jurisdictional nullities. In cases of alleged state malfeasance and the arbitrary deprivation of liberty, the public's absolute right to reconstruct the "mosaic of forgery" constitutes the paramount democratic interest.

5.14. Nota Bene: Furthermore, any institutional attempt to assert that the requisitioned metadata is overly complex, thereby necessitating sweeping redactions or non-disclosure based on internal technical illiteracy, is a legally fatal maneuver. Section 4(2.1) of the *ATIA* imposes a positive, overarching statutory duty to assist the requester. This duty mandatorily encompasses comprehensive inter-departmental consultations with specialized database architects and cybersecurity personnel. The institution is expressly prohibited from utilizing its own compartmentalized administrative ignorance as a bureaucratic shield.

6.0. Concluding Imperatives and the Crystallization of the Mandamus Remedy

6.1. The institution's prompt compliance with its non-delegable statutory obligations and the immediate discharge of its public duties *forthwith* are formally anticipated and demanded.

6.2. The requisite legal demands have been meticulously articulated, and irrefutable receipt thereof has been established via the doctrine of constructive possession. The institutional duty to act is unequivocal, absolute, and non-discretionary. Through the expiration of statutory timelines and the *ultra vires* reliance upon void administrative instruments, the state apparatus has fundamentally failed to discharge this executory duty in the face of a clear, corresponding right of performance.

6.3. It is formally submitted that no alternative, adequate administrative remedy remains extant. The relief sought before the Federal Court of Canada possesses immense, overarching practical value, as it serves to unilaterally restore the cryptographic provenance of the national law enforcement database and expose jurisdictional nullities.

6.4. Consequently, the balance of convenience does not merely tip in favor of granting a prerogative writ of *mandamus* to compel the execution of the foundational search; rather, it weighs overwhelmingly and absolutely in favor of issuing the judicial mandate. While it is a recognized jurisprudential precept that *mandamus* cannot dictate a specific, discretionary substantive outcome, it possesses the absolute, unyielding authority to compel the performance of a specific, ministerial, and executory duty—namely, the mandatory systemic search and the consequent extraction of the requisitioned hexadecimal and routing metadata ledgers.

786 I confirm for good faith purposes, the now comprehensively drafted, signed, and to be paid for and filed NOA (Form 301) will be provided in short order. Short leave to have the primary issues involving writs of mandamus will be sought prior to the commencement of a "long weekend" for some and a statutory holiday for others. I will provide notice to the lead and managerial legal counsel for the RCMP and seek whether they will accept service for the RCMP. If that is the case, all obligations herein and generally will remain.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

On Mon, May 4, 2026 at 9:31 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear RCMP (Access To Information Act Branch):

For ease of reference and continuity, I have copied and pasted your previous email herein. I repeat and rely upon the previous herein and cordially remind you of the deadline of May 14 2026. Thank you.

Mr. Kevin A. McLean (BA, JD, CIM)

Appendix

ATIP / AIPRP

Tue, Apr 28, 2:03 PM (6 days ago)
to me

Dear Kevin Mclean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.
- Hexadecimal Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.
- Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.
- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.
- DF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.
- Offline Historical Search Results: The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.
- System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

In order to process your request we require additional information:

- Location: Regarding the first point in your request, "Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction." - Please be advised that PIB PPU 005 is not a singular database, PIBs themselves are not a singular database but rather a way the government collects and stores personal information. Please specify which data base/location you would like to have searched.

You may reply to this email.

Please respond by May 4, 2026.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this

notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:

<https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message, including attachments, is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Fri, May 1, 2026 at 11:29 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DELIVERY METHOD: Via Electronic Transmission (ATIP-AIPRP@rcmp-grc.gc.ca)

TO:

Commissioner Michael Duheme, Head of the Institution

Mr. Stéphane Brisson, Chief Privacy Officer and Director General

Melissa Simpson, Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

FROM:

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

DATE: May 1, 2026

REFERENCE:

ATIA Request A-2026-00761 / F339

OIC Complaint File Number: ACC-2026-04-00379

SUBJECT: FORMAL REJECTION OF OBSTRUCTIVE CLARIFICATION TACTICS, EXPLICIT IDENTIFICATION OF DATABASE LOCATIONS, REBUKE OF WILLFUL BLINDNESS, AND REAFFIRMATION OF THE MAY 14, 2026 STATUTORY DEADLINE

1.0. PRELIMINARY OBSERVATIONS AND THE DOCTRINE OF BAD FAITH

1.1. Receipt is hereby acknowledged of the electronic correspondence dispatched by your office on April 28, 2026. In this correspondence, the Access to Information and Privacy (ATIP) Branch asserts a purported inability to locate the requisitioned records on the grounds that Personal Information Bank (PIB) RCMP PPU 005 is "not a singular database" but merely a classification method, and subsequently demands that I "specify which data base/location you would like to have searched."

1.2. This communication is formally and categorically rejected as a deliberately obtuse administrative maneuver, entirely devoid of substantive merit. It constitutes a secondary, transparent attempt to artificially pause the statutory clock under the guise of Section 6

of the Access to Information Act (ATIA). The institution is acutely aware that an active investigative file (ACC-2026-04-00379) has already been crystallized before the Office of the Information Commissioner (OIC) regarding this exact, documented pattern of manufactured ambiguity, arbitrary extensions, and statutory dereliction. In administrative law, the deployment of piecemeal, staggered requests for clarification—especially when deployed weeks after the initial receipt of a highly specified requisition—is routinely recognized by the Federal Courts as a bad faith tactic designed to orchestrate spoliation by delay. It is a systematic subversion of the legislative intent of the ATIA, which is predicated on timely, unencumbered public access.

1.3. The institutional attempt to weaponize Treasury Board Secretariat (TBS) definitions against an applicant is a profound misapplication of administrative procedure. It is a matter of foundational federal record-keeping that a Personal Information Bank describes the *nature* of the records, the class of individuals to whom the data pertains, and the statutory authority for their collection. It inherently does not, and was never intended to, dictate the physical topology of the server farm or the specific network pathways. The RCMP, as the sovereign custodian of these records, inherently possesses the internal architectural mapping that links the TBS classification (PPU 005) to the specific physical servers, virtual environments, and digital repositories where this data is housed. The master indices bridging policy classifications with IT infrastructure are entirely within your institutional control.

1.4. To demand that a civilian applicant provide the proprietary, internal server rack designations, exact software file-paths, or secure network node identifiers utilized by the RCMP Information Technology Directorate is an absurdity that borders on administrative malfeasance. The foundational premise of access to information legislation is that the government holds both the records and the corresponding indices required to locate them. You hold the master key; you are legally, statutorily, and ethically obligated to turn it. Attempting to shift the internal administrative burden of locating a federal server onto a private citizen represents a catastrophic failure of the ATIP Branch's statutory mandate and a glaring breach of the public trust. It operates on the legally bankrupt premise that an applicant must be a certified systems architect of the very institution they are seeking to hold accountable in order to exercise their quasi-constitutional rights.

2.0. EXHAUSTIVE SPECIFICATION OF DATABASE ARCHITECTURE AND LOCATION

2.1. The institution's assertion that it requires me to name the specific "database/location" is procedurally fatal and factually bankrupt. The original requisition, drafted with exacting, enterprise-level forensic precision, explicitly identified the target architectures. To feign ignorance of the targeted location when the "CPIC mainframe" and "Investigative Data Bank" were explicitly named in the very first bullet point of the primary request is an egregious exhibition of willful institutional blindness.

2.2. However, to permanently cure any residual, manufactured ambiguity, to completely exhaust the ATIP Branch's ability to rely upon feigned technical incomprehension or artificial ignorance, and to meticulously prepare the evidentiary record for the Federal

Court of Canada, you are hereby formally directed to execute the required digital extractions within the following specific, explicitly defined federal architectures:

A. The Canadian Police Information Centre (CPIC) Mainframe: Specifically, the foundational transaction logs and immutable audit ledgers housed deep within the core CPIC system architecture. This explicitly includes the uninterpreted hexadecimal and binary matrices—complete with EBCDIC/ASCII decoded text translations. It is an incontrovertible fact of database architecture that standard graphical user interfaces (GUIs) utilized by frontline officers are merely a presentation layer; they are entirely inadequate for this inquiry. The GUI acts as an operational smokescreen that visually homogenizes corrupted data to present a facially valid warrant to the end-user. Only the raw hexadecimal memory offsets can bypass this presentation layer to expose the algorithmic disfigurement and vector morphology collapse of the specified judicial instruments. These binary dumps are mathematically immune to human misinterpretation and will irrefutably demonstrate exactly when, and by whom, the enterprise-level GrapeCity Documents PDF suite (specifically version 6.0.2.0, utilizing the documented DOC-6507 bounding-box bug) was utilized to unlawfully flatten the document, algorithmically mutate the text, and forcefully delete the transparent electronic image signature of Chief Justice Geoffrey B. Morawetz.

B. The Investigative Data Bank (IDB): As explicitly referenced in my primary request ("Investigative Data Bank Audit Trails" and "Offline Historical Search Results"), this is the precise operational database wherein the historical chronology of transactions is preserved. The municipal record currently presents a glaring chronological impossibility: an arrest executed on October 2, followed by the inexplicable expungement of the purported warrant via the Integrated Court Offences Network (ICON) on October 3. In the realm of lawful judicial processes, a warrant does not magically evaporate the day after its execution; it is formally filed as a return to a justice. While a fraudulently altered warrant may be ostensibly excised from the active frontline interface to conceal an unlawful arrest and orchestrate localized spoliation, the underlying chronological footprint of the ADD, MODIFY, CLEAR, and CANCEL commands remains permanently and immutably inscribed within the IDB archives. Every keystroke generates a timestamped digital artifact; this request demands the extraction of those exact artifacts.

C. The National Police Information Services (NPIS) Infrastructure: This encompasses any centralized transaction ledgers, active mirror servers, localized terminal caches, or disaster recovery backup tape archives operating under the overarching NPIS umbrella. In a modern, enterprise-level federal law enforcement framework, true digital deletion is an absolute myth. Highly sophisticated asynchronous data replication redundancies ensure that when a corrupted file is purged from a local municipal terminal in a panic to hide evidence of forgery, it is immediately preserved in the federal disaster recovery backups. This request specifically targets the preservation of data that captures network session activity for the critical temporal epoch encompassing September 22 to October 4, 2024. The RCMP is strictly prohibited from allowing the routine overwriting of these specific backup tapes.

D. The CPIC Audit Log (CAL) / Systemic Routing Ledgers: The specific digital repository and network gateway logs where Originating Agency Identifiers (ORI), Media Access Control (MAC) addresses, and Internet Protocol (IP) terminal metadata are permanently recorded during data-entry sessions. This is specifically targeted at data originating from municipal partner agencies (namely, the Toronto Police Service). These routing metrics are fundamentally necessary to invoke the foundational legal maxim *nemo dat quod non habet* (no one gives what they do not have). If an instrument purportedly authorized by a Superior Court Chief Justice operating out of the 361 University Avenue courthouse was, in digital reality, inputted from a municipal police division's back-office terminal, the ORI routing codes and MAC addresses will incontrovertibly prove the jurisdictional nullity. A municipal agency possesses absolutely zero inherent jurisdiction to manufacture, authorize, or disseminate a Superior Court warrant. The metadata will expose the federal database being utilized as a secure digital vault for municipal-level documentary forgery.

3.0. BREACH OF THE DUTY TO ASSIST AND MANDATORY INTERNAL CONSULTATIONS

3.1. The burden of navigating the RCMP's proprietary internal server nomenclature does not rest upon the applicant, nor can the ATIP Branch utilize its own internal compartmentalization of technical knowledge as a bureaucratic shield against mandatory disclosure. Section 4(2.1) of the ATIA imposes a positive, overarching "duty to assist" upon the institution. This is not a passive suggestion, a mere administrative courtesy, or a set of guidelines to be followed when convenient; it is a rigorous, legally enforceable statutory mandate designed to facilitate transparency and dismantle institutional obstruction.

3.2. The Supreme Court of Canada has consistently and forcefully held that access legislation is not a game of blind man's bluff. An institution cannot hide behind administrative semantics or feigned technical illiteracy to deny access to clearly described records. As previously stated, the jurisprudence mandates that you process the request utilizing an "experienced employee." A standard administrative intake clerk in the ATIP mailroom may not immediately understand the physical network topology of where PPU 005 data resides, but a CPIC Database Administrator, a senior cybersecurity systems architect, or the Director of Information Management fundamentally does.

3.3. Your absolute failure to conduct this mandatory inter-departmental consultation prior to dispatching an obstructive, ten-day demand for clarification constitutes a highly actionable breach of process. The correct, legally mandated procedure upon receiving a highly technical request is to forward the parameters to the specialized operational unit (in this case, CPIC Systems Governance, IT Security, and the NPIS database architects) for extraction. If the ATIP analyst does not know where the PPU 005 audit trails are located, their strict legal duty is to ask the RCMP's internal systems administrators—not to bounce the requisition back to the applicant in a transparent attempt to exhaust civilian resources, create artificial administrative friction, and arrest the statutory timeline. Internal friction between the RCMP's ATIP division and its IT division is an

internal operational failure; it is not a valid statutory excuse for denying a Canadian citizen their quasi-constitutional rights.

4.0. ABSOLUTE CONTINUITY OF THE STATUTORY CLOCK AND REJECTION OF EXTRA-STATUTORY DEADLINES

4.1. The institution's attempt to unilaterally impose a new, arbitrary deadline of "May 4, 2026" to respond to this feigned incomprehension, coupled with the highly irregular implicit threat of summary file closure, is *ultra vires* the jurisdiction conferred by the governing legislation and legally void *ab initio*. The Access to Information Act does not contain an "abeyance mechanism," nor does it feature a "pause button" for administrative clarification once a request containing sufficient detail has been formally received.

4.2. To rigorously reiterate the doctrine of exhaustive enumeration (*expressio unius est exclusio alterius*), Parliament deliberately and specifically outlined the *only* valid reasons for delaying a request under Section 9 of the ATIA (specifically: massive volume of records, mandatory external consultations, or mandatory third-party notice). If Parliament had intended for federal institutions to possess the sweeping authority to arbitrarily pause the thirty-day clock simply because they wished to ask the applicant a clarifying question under Section 6, they would have explicitly legislated that extraordinary power. They decidedly did not. Therefore, this unilateral deadline is an invention of institutional convenience, a pure procedural phantom entirely unsupported by the *lex terrae*.

4.3. As previously and exhaustively detailed in my correspondence of April 24, 2026, the statutory clock commenced upon the objectively verified, third-party delivery of the original requisition via Canada Post on April 14, 2026. The Supreme Court of Canada and the Federal Courts recognize the doctrine of constructive possession. Internal mailroom inefficiencies, internal routing delays, sorting bottlenecks, and subsequent administrative tardiness by the ATIP Branch in physically opening the file on April 15, 2026, do not artificially alter the legally operative date of receipt. The institution was in constructive possession of the request on April 14; the legal obligations crystallized at that precise moment.

4.4. Furthermore, the institution failed entirely to secure a procedurally valid extension of time pursuant to Section 9 of the ATIA within the necessary timeframe. The jurisprudence is absolute on this matter: you cannot retrospectively repair a failure to invoke a formal Section 9 extension by generating an informal, extra-statutory Section 6 clarification delay as a stopgap measure. Therefore, the mandatory, legally binding deadline for the complete, substantive, and unredacted provision of these systemic records remains irrevocably, mathematically fixed at May 14, 2026.

4.5. I hereby confirm that the deadline to provide these records, as an absolute and unyielding statutory deadline, remains that of May 14, 2026. There will be no further extensions, no permitted abeyances, and no tolerance for further bureaucratic attrition.

5.0. IN LAYMAN'S TERMS

5.1. Breakdown of Institutional Misunderstanding

In layman's terms, Ms. Simpson is confusing a conceptual filing category with a physical storage location, and she is asking me to do her IT department's job for her. The request operates on the transparently bad-faith assumption that if the ATIP branch plays dumb long enough, the statutory deadline will quietly pass, and the applicant will simply abandon the pursuit of these critical records out of sheer administrative exhaustion.

Here is a breakdown of exactly what she is misunderstanding (or deliberately pretending to misunderstand to orchestrate delay):

5.1.1. The "Filing Cabinet" Analogy

A Personal Information Bank (PIB), like "PPU 005," is just a government classification code. It describes the *type* of information collected (e.g., investigative records, as opposed to employee payroll records, human resources data, or procurement contracts). Imagine going to a large, complex metropolitan hospital and asking the administration for a copy of your "Medical Records." Ms. Simpson's response is the exact equivalent of the hospital receptionist looking at you blankly and stating, *"Medical Records isn't a physical drawer; it's just a conceptual framework of how we group health data according to Ministry guidelines. Therefore, I cannot help you. Please tell me the exact floor, the specific room number, the specific filing cabinet serial number, and the exact manila folder where your papers are kept before I will even begin to look for them."* She is arguing that because PPU 005 is a category label, she doesn't know where to physically look. However, the RCMP's own database administrators absolutely know which specific servers, which specific mainframes, and which software systems hold "PPU 005" data. They built the systems. She simply hasn't asked them, preferring instead to feign paralysis.

5.1.2. The Bank Statement Analogy

To provide a secondary, equally damning analogy, this institutional response is akin to an individual requesting a transaction history from a major commercial bank for a specific date range, only for the bank teller to respond: *"A transaction history is just a classification of financial data. Please provide us with the exact IP address of the server rack in our underground data center where your specific digital ledger is hosted, otherwise we will close your inquiry."* It is an absurd, structurally illogical proposition designed solely to frustrate access and protect the institution from scrutiny.

5.1.3. The Library Analogy (Dewey Decimal System)

If the RCMP were a public library, PPU 005 is simply the Dewey Decimal code for "History." I have asked for a specific history book. Ms. Simpson is claiming she cannot fulfill the request because "History" is a category, not a physical shelf, and is demanding that I provide her with the exact GPS coordinates of the shelf in her own building. The librarian knows where the history section is; the ATIP branch knows where the PPU 005 records are stored.

5.1.4. Ignoring What I Already Told Her

She is pretending that I didn't give her a location. However, in the very first bullet point of my original request, I explicitly named the Canadian Police Information Centre (CPIC) mainframe and the Investigative Data Bank. I *did* give her the locations; she is simply ignoring those highly specific, globally recognized federal system names to falsely claim my request is too vague to process.

5.1.5. Shifting the Burden (Breach of Duty to Assist)

Under the law, she is strictly required to consult with an "experienced employee" (like an RCMP systems architect, a database engineer, or a network security officer) to figure out where to pull this data. Instead of doing her job and asking her own internal IT department, "*Hey, which internal database holds the PPU 005 transaction logs for CPIC?*", she is illegally bouncing the question back to me. She is effectively demanding that I, a civilian, provide the RCMP's proprietary, internal server names or highly specific classified network file paths—which is an impossible, unreasonable, and statutorily prohibited request.

Ultimately, her "misunderstanding" serves as nothing more than a convenient, highly manufactured bureaucratic excuse to illegally pause the 30-day statutory clock, frustrate the federal oversight process, and delay handing over the CPIC transaction logs I requested.

6.0. CONCLUSION, DEEMED REFUSAL, AND ESCALATION TO THE FEDERAL COURT

6.1. The continued utilization of these dilatory tactics creates a profound, inescapable circumstantial inference of bad faith. It is becoming manifestly obvious that these administrative delays are a coordinated attempt to conceal the algorithmic disfigurement of Superior Court instruments by state actors. By intentionally pushing the disclosure timeline past the imminent departure of Chief Justice Morawetz, the institution is seemingly attempting to obscure the *status quo ante*, run out the clock on the immediate jurisdictional issues, and evade contemporaneous judicial scrutiny regarding the integrity of the warrants issued under his purported authority.

6.2. Be formally advised that any failure to effectuate the complete, unredacted disclosure of the specified hexadecimal dumps, IDB audit trails, and ORI routing codes from the CPIC mainframes by the exact deadline of May 14, 2026, shall be automatically and decisively classified as a Deemed Refusal pursuant to Section 10(3) of the ATIA.

6.3. Statutory Order-Making Powers of the Information Commissioner: The institution is formally reminded that the Office of the Information Commissioner (OIC), in stark, profound contrast to the Office of the Privacy Commissioner, is vested with explicit, binding order-making authority under recent legislative amendments to the ATIA. Pursuant to Section 36.1(1) of the ATIA, should the Commissioner find this complaint of administrative stalling and constructive refusal to be well-founded, she possesses the statutory power to issue a formal, legally binding order compelling the Head of the Institution to disclose the requested records. The Information Commissioner does not

merely issue polite recommendations or operate as a toothless ombudsman; she wields the sword of compliance. The ATIP Branch's continued reliance on obstructive tactics will not merely result in adverse administrative findings; it will culminate in a binding legal mandate to disclose, accompanied by a highly damaging public report detailing the institution's obstruction.

6.4. Upon the crystallization of this Deemed Refusal on May 14, 2026, the institution is stripped of all discretionary latitude. This matter will ripen immediately for extraordinary judicial remedies. I fully reserve the right to seek an immediate prerogative writ of *mandamus* before the Federal Court of Canada to compel the physical production of these digital ledgers. The legal test for *mandamus* is clearly met here: there is a public legal duty to act, the duty is owed to the applicant, there is a clear right to the performance of that duty, and there has been a demand and a constructive refusal. A *mandamus* application will explicitly cite the institution's bad faith, the flagrant breach of the statutory duty to assist, deliberate administrative stalling, and the coordinated orchestration of spoliation by delay.

6.5. Furthermore, should it become necessary to engage the Federal Court to bypass this administrative blockade and pierce the veil of institutional secrecy, such an application will be accompanied by petitions for severe, punitive cost awards against the institution. It may also necessitate naming specific institutional heads, Directors General, and ATIP officers in their official capacities to answer directly to a Federal Court Justice for the systemic dereliction of their statutory duties.

6.6. Public Disclosure Notice and Statutory Balancing: I cordially remind the Commissioner of the RCMP, along with the Chief Privacy Officer, that the Head of the Institution is required by law to consider the requirement to issue a public disclosure notice. In my view, the systemic algorithmic manipulation of the national warrant database does not fall under standard complaint grounds; it is a matter of profound national security and constitutional integrity that would necessitate immediate judicial review. I note definitively that the Access to Information Act (specifically Section 19 regarding public interest overrides) and the Privacy Act (specifically Section 8 regarding the disclosure of personal information in the public interest) work in tandem as a seamless code. The overarching public interest in ensuring the Canadian law enforcement apparatus is not operating on algorithmically forged judicial instruments absolutely obliterates any residual privacy interests of the state actors who inputted the fraudulent data.

This document serves as full, final, and exhaustive clarification. There is no further ambiguity. The locations are identified. The databases are named. The analogies have been provided. Proceed with the substantive extraction of the records from the explicitly named databases immediately.

Respectfully submitted,

/s/ Kevin A. McLean

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Apr 23, 2026 at 2:27 PM ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca> wrote:

Dear Kevin McLean:

This is a follow-up to your request under the Access to Information Act, which was received by this office on April 15, 2026, for:

Requesting the Following:

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.***
- Hexadecimal Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant designated in the primary request.***
- Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.***
- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.***

- DF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.

- Offline Historical Search Results: The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.

- System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

In order to process your request we require additional information:

- **Scope:** We have examined your request and fail to understand exactly what you are seeking in terms of records or documentation. As per section 6 of the Access to Information Act, "A request for access to a record under this Part shall be made in writing to the government institution that has control of the record and shall provide sufficient detail to enable an experienced employee of the institution to identify the record with a reasonable effort." **Please clarify what records you are seeking.**
- **Application fee:** The Access to Information Act prescribes an application fee of \$5.00. This is payable by cheque or money order to the Receiver General of Canada.

You may send this via regular mail or e-mail to the contact listed below.

Your file will remain open in our office for the next 10 days. If we have not received a response by **May 4, 2026**, this file will be closed.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice. In the event you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online:
<https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing on this email.

Regards,

Melissa Simpson
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the intended recipient, you are advised that all use (copy, distribution, disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

AVIS DE CONFIDENTIALITÉ:

Le présent e-mail est confidentiel et ne s'adresse qu'au destinataire dont le nom apparaît ci-dessus. Si ce courriel vous est parvenu par erreur et que vous n'êtes pas le destinataire visé, vous êtes, par la présente, avisé que tout usage (copie, distribution, divulgation ou autre) de ce courriel est strictement interdit. Vous êtes donc prié de m'aviser immédiatement de cette erreur en communiquant avec moi et en détruisant ce courriel de votre ordinateur.

800

Tab H



Mr. Kevin McLean <mcleansettlement@gmail.com>

Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Mathews, Curtis (RCMP/GRC) <Curtis.Mathews@rcmp-grc.gc.ca>To: "Mr. Kevin McLean" <mcleansettlement@gmail.com>, ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>, "Duheme, Michael (RCMP/GRC)" <Michael.Duheme@rcmp-grc.gc.ca>, "Brisson, Stép Bryan (RCMP/GRC)" <Bryan.Larkin@rcmp-grc.gc.ca>, "Ball, Jeff (RCMP/GRC)" <Jeff.Ball@rcmp-grc.gc.ca>
Cc: "mclean@searchandseizure.ca" <mclean@searchandseizure.ca>

Good morning Mr. McLean,

I want to acknowledge receipt of your email below and assure you that my team and I are looking into your concerns as they relate to the processing of your Access to Information Act request

I want to ensure I fully address the issues you have noted below and will therefore need some time to address your concerns and legal assertions.

I commit to getting back to you with a response by the end of the week.

Thank you in advance for your patience, and I look forward to working with you to resolve the issues.

Curtis Mathews

A/Director General, ATIP Modernization / Directeur générale p.i, AIPRP modernisation

Access to Information and Privacy Branch / Sous-direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP)

Royal Canadian Mounted Police / Gendarmerie royale du Canada

curtis.mathews@rcmp-grc.gc.ca Tel: 343-551-1037

From: Mr. Kevin McLean <mcleansettlement@gmail.com>**Sent:** June 22, 2026 8:29 AM**To:** ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>; Duheme, Michael (RCMP/GRC) <Michael.Duheme@rcmp-grc.gc.ca>; Brisson, Stéphane (RCMP/GRC) <Stephane.Brisson@rcm
<Bryan.Larkin@rcmp-grc.gc.ca>; Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>; Mathews, Curtis (RCMP/GRC) <Curtis.Mathews@rcmp-grc.gc.ca>**Cc:** mclean@searchandseizure.ca**Subject:** Re: Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I received the below auto-reply from Mr. Brisson and a postmaster deliver from what I thought to be the email of Mr. Curtis Mathews but I appeared to have added one too many "t's" in surname. Apologies for

Regards, Mr. Kevin A. McLean (BA, JD, CIM)

Appendix

Brisson, Stéphane (RCMP/GRC)

7:39 AM (46 minutes ago)

to me

Greetings,

Tab I



Mr. Kevin McLean <mcleansettlement@gmail.com>

Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

Mr. Kevin McLean <mcleansettlement@gmail.com>

Mon, Jun 22, 2026 at 12:02 PM

To: "Beaudoin, Tina (RCMP/GRC)" <tina.beaudoin@rcmp-grc.gc.ca>, Bryan.Larkin@rcmp-grc.gc.ca, "Brisson, Stéphane (RCMP/GRC)" <stephane.brisson@rcmp-grc.gc.ca>, "Ball, Jeff (RCMP/GRC)" <Jeff.ball@rcmp-grc.gc.ca>, "Simpson, Melissa (RCMP/GRC)" <melissa.simpson@rcmp-grc.gc.ca>, "Duheme, Michael (RCMP/GRC)" <Michael.Duheme@rcmp-grc.gc.ca>

Cc: mclean@searchandseizure.ca

Subject: STATUS INQUIRY – ATIA Request A-2026-00761 / F339 – Statutory Default and Retrieval Status**Date:** June 22, 2026**To:** Ms. Tina Beaudoin Access to Information and Privacy Branch Royal Canadian Mounted Policetina.beaudoin@rcmp-grc.gc.ca**Cc:** ATIP-AIPRP@rcmp-grc.gc.ca Bryan.Larkin@rcmp-grc.gc.ca stephane.brisson@rcmp-grc.gc.ca melissa.simpson@rcmp-grc.gc.ca jeff.ball@rcmp-grc.gc.ca

Dear Ms. Beaudoin,

I am writing to request an immediate and precise status update regarding your correspondence of June 16, 2026, wherein you confirmed that ATIA Request A-2026-00761 / F339 had entered the “retrieval stage” for the extraction of responsive CPIC database logs, hexadecimal transaction logs, and associated systemic metadata. As the request was delivered to the RCMP on April 14, 2026, the statutory 30-day deadline expired on May 14, 2026, and no lawful extension under section 9 of the Access to Information Act was invoked. It is therefore unclear how the file can still be characterized as being in a retrieval phase at the end of June.

Accordingly, please confirm by return email whether the responsive technical logs—specifically the unredacted PPU 005 audit trails, hexadecimal mainframe dumps, ORI routing metadata, CPIC governance manuals, and inter-agency communication logs—have been successfully compiled from the relevant system repositories. These records are machine-generated federal artifacts not subject to discretionary review or third-party consultations, and their retrieval should not require more than sixty days absent a valid statutory extension.

SUPPLEMENTAL ANALYSIS (FOR THE RECORD)

For absolute clarity, your correspondence of June 16, 2026 contains two legally determinative admissions: first, that the file remains in a so-called “retrieval stage,” and second, that no statutory extensions were taken. These admissions are irreconcilable with the Access to Information Act. The records requested—namely the unredacted PPU 005 audit trails, hexadecimal mainframe logs, ORI routing metadata, CPIC governance manuals, and associated system-generated artifacts—are machine-produced federal records not subject to discretionary review, third-party consultations, or interpretive severance. Their continued classification as “in retrieval” more than sixty days after constructive possession (April 14, 2026) is incompatible with the technical nature of the records and constitutes direct evidence of a crystallized deemed refusal under subsection 10(3). Moreover, the April 23 clarification demand was predicated on a mischaracterization of the request as a personal-information inquiry, despite the request explicitly targeting institutional metadata and systemic CPIC artifacts; such a demand is ultra vires and incapable of tolling the statutory clock. The reference in your June 16 email to a “60-day complaint window” is a deadline applicable to applicants, not a

804

processing extension for institutions, and cannot retroactively suspend the non-discretionary thirty-day mandate under section 7. Constructive possession was achieved on April 14, 2026, and internal routing delays or administrative inefficiencies cannot lawfully alter the operative date of receipt. These cumulative admissions and procedural irregularities confirm that the institution is functus officio with respect to any residual processing discretion, and the deemed refusal is now a matter of strict statutory operation.

Given the above, and in light of the statutory default that has already crystallized, your prompt confirmation of the exact operational status of the data extraction is required today.

I understand that Mr. Michael Duheme (the esteemed Commissioner of the RCMP is no longer away “on duty”) so he is reincluded accordingly.

Respectfully submitted,

Mr. Kevin A. McLean (B.A., J.D., C.I.M.) Applicant / Requester
mcleansettlement@gmail.com 647-370-9354

On Tue, Jun 16, 2026 at 10:17 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Date: June 16, 2026

Creation method: Dictated with voice recognition software (reserve rights to amend any errors involving syntax, spelling, grammar or incorrect double negatives but the substance will remain the same)

TO:

RCMP ATIP Branch

Email: ATIP / AIPRP ATIP-AIPRP@rcmp-grc.gc.ca;

Kind attention:

Beaudoin, Tina (RCMP/GRC) tina.beaudoin@rcmp-grc.gc.ca

Larkin, Bryan (RCMP/GRC) Bryan.Larkin@rcmp-grc.gc.ca;

Brisson, Stéphane (RCMP/GRC) stephane.brisson@rcmp-grc.gc.ca;

Simpson, Melissa (RCMP/GRC) melissa.simpson@rcmp-grc.gc.ca

And others

SUBJECT: RE: ACCESS TO INFORMATION ACT REQUEST A-2026-00761 / F339 – RESPONSE TO MS. TINA BEAUDOIN’S EMAIL OF TODAY’S (JUNE 16, 2026) DATE

TAB 23

FEDERAL COURT

B E T W E E N:

KEVIN A. MCLEAN

Applicant

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, AND STEPHANE
BRISSON

Respondents

MEMORANDUM OF FACT AND LAW OF THE APPLICANT

(PURSUANT TO RULE 70 (30 PAGES EXCLUDING TABLE OF CONTENTS AND APPENDICES))

Table of Contents

PART I — OVERVIEW AND STATEMENT OF FACTS 1

 A. Overview 1

 B. The Respondents’ Default..... 7

 C. Factual Background..... 9

 The Applicant’s PII Access Request (March 11, 2026)..... 9

 The April 7, 2026 s. 8(2)(m) Public-Interest-Disclosure Request 9

 The Arrest of October 2, 2024..... 9

 The “False Information Package” 10

 Metadata Proving Fabrication 10

 The RCMP’s Refusal to Search..... 10

PART II — points in issue..... 11

 Issue #1: Refusal to search..... 11

 Issue No. 2: Refusal to discharge a public duty to search is reviewable by the fcc and only the fcc, and the writ of mandamus is available to the applicant and those similarly situated..... 11

 Issue #3: Clause 8(2)(M) of the Privacy Act: the failure to consider by the head of the INSTITUTION..... 12

 Issue #4: Refusal to search for Foundational Metadata and Offline Historical Database..... 12

 Issue #5: fraud unravels everything but it imposes positive duties on all most notably federal institutions like the RCMP..... 13

 Issue #6: Fraudulent Misrepresentations Perpetrated Upon the Judiciary are Mirrored Within the Canadian Police Information Centre System, and the Concomitant Positive Obligations Imposed Upon the Royal Canadian Mounted Police as Custodian and Controller 13

PART III — LAW AND ARGUMENT	16
807 standard of review of the RCMP’s failures to act; and The RCMP Has a Statutory Duty to Conduct a Reasonable Search for Personal Information	16
The Standard of Review	16
The Failure of the RCMP to conduct a search of the Foundational Metadata repository and the Offline Historical Database	19
The RCMP’s Refusal to Search Is Not Reviewable by the Privacy Commissioner	20
C. The RCMP’s Refusal to Search Foundational Metadata (Level 2) Is Unlawful	20
D. The RCMP’s Refusal to Search Amended or Purged Data (Level 3) Is Unlawful.....	21
E. The Legal Test for Mandamus Is Satisfied	22
F. The Doctrine of “Control” Under the Privacy Act and Federal Courts Jurisprudence	22
Control is broader than physical possession	22
Control includes the ability to demand records.....	23
Control includes metadata and audit trails	23
Control includes amended and purged data	23
G. The RCMP Commissioner Breached His Mandatory Duty to Consider Public-Interest Disclosure Under s. 8(2)(m)	23
G(I): Section 8(2)(m) imposes a mandatory duty on the Head of the institution.....	23
2. The RCMP refused to exercise discretion	24
3. The Commissioner’s “away on duty” auto-reply does not suspend statutory obligations	24
H. MCINERNEY v. MacDonald.....	24
I. The Fabricated “Information Package” Is an Absolute Nullity	25
PART IV — RELIEF SOUGHT	26
APPendices	30
PART V — LIST OF AUTHORITIES	30
A. Statutes and Regulations	30
B. Jurisprudence	30

PART I — OVERVIEW AND STATEMENT OF FACTS

A. OVERVIEW

1. This **Application** proceeds **unopposed**. The **Respondents** were duly served with the issued Notice of Application on May 19, 2026, and **failed to file a Notice of Appearance (Form 305)** within the 10-day period mandated by the *Federal Courts Rules*. Under Form 305 and Rule 305(2), the Respondents are **not entitled to notice of any further step** or service of documents. Interim orders including final orders, including an Order of ‘judgment’ may *ipso facto* be rendered *in absentia*.

2. Within the context of the present Application before the Federal Court of Canada (the “**Federal Court**” or “FCC”), **808**s posited that protracted delay is demonstrably calculated, on a balance of probabilities, to manifest a profound miscarriage of justice, thereby constituting an egregious affront to the foundational tenets of the rule of law. Such transgressions encompass sub-categories of jurisprudence demanding adjudication on the correctness standard as opposed to the reasonableness standard as per the SCC’s majority decision in *Vavilov*: (i) overarching legal inquiries of paramount significance to the administration of justice comprehensively; (ii) complexities delineating the jurisdictional demarcations betwixt disparate administrative tribunals; and (iii) the intricate equilibrium maintained between the legislative apparatus and collateral state organs, all of which necessitate a definitive and unequivocal resolution by the judiciary, categorized herein as the final answer requirement (the “**Final Answer Requirement**”). The sanctity of the rule of law (“Rule Of Law”) dictates that the judiciary retains the ultimate adjudicative authority, defined as the final word requirement (the “**Final Word Requirement**”), particularly concerning overarching legal questions that mandate absolute uniformity and jurisprudential consistency, identified as the uniform answers requirement (the “**Uniform Answers Requirement**”) or vertical *stare decisis*. Furthermore, judicial intervention is rendered imperative in instances where an administrative entity, including an “Other Tribunal” which the RCMP is in this capacity and under the scheme of the Federal Courts Act and Federal Courts Rules, interprets its statutory and prescribed ambit in a manner irreconcilable with the jurisdictional prerogatives of an alternative administrative body, as the Rule Of Law fundamentally eschews and disdains the proliferation of discordant mandates that precipitate a genuine operational conflict, characterized as the intolerance for conflicting orders requirement (the “**Intolerance For Conflicting Orders Requirement**”).
3. Pertinent constitutional paradigms invoked herein regarding the Rule Of Law include, *inter alia*: (i) the egalitarian application of jurisprudence ensuring equitable protection and ancillary rights and privileges of Canadian citizens or those permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*; (ii) institutional accountability demanding absolute transparency wherein all entities are subordinate to the law and the Rule Of Law is above no person; and (iii) unimpeded access to justice and access to Government Institutions, de facto and de jure conducting the required searches within the ambit of an individual’s (citizen or permanent resident) access request to his or her (or other personal pronouns) Personal Information. Although the presumption of an administrative tribunal’s independence and lack of bias is not constitutionally enshrined in a manner analogous to sections 96 through 101 of the *Constitution Act, 1867* governing superior courts, an evidentiary presumption of impartiality and the absolute absence of conflicts of interest remains a foundational cornerstone of administrative law.
4. Irrespective of the jurisdictional capacity of the *Federal Court* to mandate the physical appearance of the RCMP in incontrovertible authority resides within the judiciary to compel strict adherence to the obligations articulated under *rule 317* of the *Federal Courts Rules*, alongside the enforcement of overarching equitable doctrines, common law imperatives, and statutory prescriptions.

- 809
5. It is acknowledged that an absence of statutory recourse for any Applicant to complain under section 29 of the *Privacy Act* concerning systemic, general or specific deficiencies in required searches or the dereliction by the head of the *RCMP* to operationalize discretionary powers vested under section 8(2)(m) of the *Privacy Act* (the “**Privacy Act**”) and, by necessary implication, section 19 of the federal Access To Information Act (the “**Access to Information Act**” or “*ATIA*”).
 6. Furthermore, the administrative tribunal of the *RCMP* has demonstrably been divested of jurisdiction, constituting an *ultra vires* posture regarding, at a minimum, the requests executed pursuant to the *Privacy Act*, as evidenced by the personal information access request dated March 11, 2026 (the “**Access Request**”). The tribunal is inextricably foreclosed from restoring the *status quo ante* on a multitude of grounds as already submitted and by reference to now uncontroverted evidence in the filed documents herein.
 7. Reliance is perpetually placed upon the uncontroverted factual matrix and the unopposed, binding jurisprudential authorities incorporated within the record of proceeding (the “**Record of Proceeding**”). Scrutinizing the evidentiary *acta*, it is submitted that the documented circumstances elucidate an unprecedented and egregious falsification of judicial instruments. To the extent there is a reported decision where the “Executive Branch(es)” of government, particularly law enforcement, have falsified the entirety of an information package, including the usurpation of the Judicial Branch of government, the Applicant welcomes this Honourable FCC pointing him to such authority for his review. However, his extensive research has not found a single authority with such egregious fraudulent manipulation of a document that not only commences a Criminal Proceeding but also one that authorizes the complete obliteration of an individual’s liberty.
 8. Distinguishing the present scenario from *R. v. Smith*, [2020 ONCJ 611](#) (the “*Smith Decision*”) as per Justice Nadel of the OJC (Hamilton Court), wherein the unauthorized alteration of weapon surrender forms was executed merely for administrative convenience with one of the surrendering individuals being bed ridden, the present machinations involve the deliberate adulteration of a *Criminal Code* form 7 warrant for arrest (the “**Warrant for Arrest**”). Such a severe circumvention of the statutory architecture unequivocally constitutes a complete nullity rather than a mere curable irregularity, as it represents a direct contravention of legislative enactments, the *Criminal Code* and immutable equitable principles. Perhaps, the *RCMP* and other law enforcement branches are of the unlawful view that because section 32 of the *Interpretation Act* utilizes the word “prescribed” as opposed to “statutory” that such falsification and uttering of a false document in the record of a transferee courthouse is not covered by Parliament therein. Such ruminations and cogitations will forever remain in the domain hypothetical considering none of the Respondents wished to appear.
 9. For sake of convenience also for emphasis, the unprecedented nature of what underlies (pardon the pun as it relates to the second syllable in said word).ⁱ Subsequent to the unprecedented and egregious vitiation of documentary integrity facilitated by the utilization of the software development kit encompassed within the software application GrapeCity.Documents.For.PDF throughout the calendar year of 2024, a conspicuous dereliction of administrative

810 and statutory duty has been exhibited by the Regional Commander, Mr. Matt Peggs. Specifically, a constitutional demand for foundational prosecutorial instruments—encompassing an authentic information package (the “**Authentic Information Package**”) and an instrument of apprehension, formally designated as an arrest warrant (the “**Arrest Warrant**”)—has been entirely ignored. The assertion promulgated within the *MAG CSD Court Information Access Guide (2019)*, by the MAG which does not form “Source Law” under the *Legislation Act, 2006*, suggesting that the Superior Court of Justice in Ontario, functioning inherently as a “court of record”, is exempted from the obligation to retain original or reproduced iterations of the *acta* of the tribunal, including an intake court endorsement (the “**Intake Court Endorsement**”) or a *Criminal Code* Form 7 warrant for arrest (the “**Warrant For Arrest**”), is fundamentally contested. The failure to retain and furnish such documentation operates in direct contravention of established common law and statutory imperatives; consequently, such failures are unequivocally classified not as mere procedural irregularities, but as absolute nullities *ab initio*. Ss. 2(b) of the Charter protest listeners and our SCC coined the “open **court** principle” with intent and precision. That being said, where the unprecedented occurs, like it has involving the factual matrix herein, CPIC, by its Foundational Metadata and Offline Historical Database repositories becomes a universal source of non-emotional, digital truth at points in time.

10. Furthermore, the explicit entitlement of an accused individual to procure a *Criminal Code* Form 2 information (the “**Information**”) or a *Criminal Code* Form 4 indictment (the “**Indictment**”) absent financial encumbrance under the *Administration of Justice Act* and its attendant regulation (see: Reg 158/03) is categorically acknowledged within the aforementioned guide. Notwithstanding formal requests for said documentation intended to restore the *status quo ante* and to have copies of the underlying documents which commenced a Criminal Proceeding against the Applicant and the apparent “Intake Court Endorsement”, a species unknown to criminal law per se but more in the nature of “family law” or “bankruptcy and insolvency law”, which is unsurprising in relation to the former considering the now known location of the Originating Court Office at the Originating Courthouse (both definitions defined *infra*), the provision thereof remains unfulfilled. The Applicant has been wise to exhaust all avenues.
11. Following an initial correspondence in March 2026 by Ms. Simion, the Manager of Court Operations situated at the originating courthouse (the “**Originating Courthouse**”) and originating court office (the “**Originating Court Office**”) at the Superior Court of Justice located at 361 University Avenue, floor one, wherein assurances of an imminent update were provided, a profound cessation of communication ensued. Such systemic obfuscation epitomizes the administrative recalcitrance characterized by the Honourable Mr. Justice Phelan of the Federal Court as a “royal runaround” within the jurisprudence of *Chitrakar v. Bell TV*, [2013 FC 1103](#) (CanLII) (the “*Chitrakar Decision*”), at paragraph 11.
12. *Prima facie*, the pervasive reticence demonstrated by the Regional Commander of the Central Region regarding elemental informational requests precipitates the invocation of the adverse inference doctrine. It is vociferously submitted and implored that judicial notice be taken by this Honourable Court concerning this obstinate silence.

811 The self-evident conclusion extrapolated from such omissions dictates that the withheld documentation either corroborates the alleged nullities or is entirely non-existent, rendering the actions of the administrative authorities *ultra vires*.

13. Pursuant to the stringent evidentiary thresholds dictating the pleading of similar fact evidence—functioning as a recognized exception to the prohibition against pleading evidence *per se*, notwithstanding the characterization of the present proceeding as an application rather than an action—such similar fact evidence has been formally pleaded (vide: Tab 11, page 433, paragraph 43). The formal admission of this evidentiary foundation is systematically sought *in limine*.
14. An advanced syllogism regarding the factual matrix leads to the self-evident conclusion that the Regional Commander, Mr. Matt Peggs, could not conceivably constitute the informant (the “**Informant**”) delineated within the *Information*. This deduction is substantiated by the irrefutable reality that the presiding court officer of the Toronto Region, Mrs. Frugoni-Rojas, was neither of the male sex, as denoted by the nomenclature “(M)” within the designation “C L (M)”, nor did the individual possess the requisite official title. It must be articulated that this observation is not intended to castigate the commendable duties executed by court officers; rather, it serves to highlight the incontrovertible fact that Mrs. Frugoni-Rojas did not hold the distinguished appellation in question.
15. Extensive forensic analysis of the systemic vulnerabilities inherent within the specific iteration of PDF manipulation software, namely GrapeCity.Documents.For.PDF 6.0.2.0, elucidates that the titular designation for a commander, abbreviated as “COM” or “C.O.M.”, is erroneously transfigured into “C L (M)”. This software anomaly is acutely exacerbated when the digital signature apparatus and infrastructure promulgated by Adobe, Inc. are synthesized into the *Authentic Information Package*.
16. The Commander of the Order of Merit of the Police Forces (the “**Order Of Merit**”) is an accolade acknowledging outstanding meritorious service and profound leadership capacities over an extended duration, frequently possessing national or international ramifications. In connection with the aforementioned Regional Commander, Mr. Matt Peggs, who concurrently functions as an Assistant Commissioner subservient to Commissioner Mr. Michael Duheme, official publications substantiate a promotion to the Commanding Officer of the O Division in October 2023. Subsequently rebranded as the Central Region, it is documented that Assistant Commissioner Peggs presides over this jurisdiction to manifest impactful outcomes on a national echelon. It is further promulgated that in January 2025, an appointment to the *Order Of Merit* was conferred, followed by the bestowment of the King's Coronation Medal in May 2025, thereby solidifying the official designation as Assistant Commissioner, Regional Commander, Central Region. The irreconcilable discrepancy between the digitally altered documentation and these indisputable facts renders the corresponding instruments a strict nullity, rather than a mere irregularity.
17. Unless a contrary intention is unequivocally manifested, the terminological definitions delineated within the extant record of proceeding (the “**Record Of Proceeding**”) are implicitly and expressly adopted herein. Furthermore,

18. In instances wherein the vitiation of documentary integrity is identified—specifically pertaining to the forgery or purported application of a judicial officer's signature where a physical, electronic, or digital signature is statutorily mandated—reliance is firmly placed upon the *Secure Electronic Signature Regulations*, promulgated by the Governor General pursuant to the enabling frameworks of the *Personal Information Protection and Electronic Documents Act* and the *Canada Evidence Act*. Any deviation from these stringent signature requirements operates *ipso facto* to render the document a nullity, as it constitutes a direct contravention of binding statutory and equitable principles. In conjunction with the definitional reliance predicated upon the *Interpretation Act* (notably section 2, which establishes the distinction between an act and a regulation while categorizing both as an enactment), the interpretative mandates of the *Interpretation Act* are explicitly assimilated, including, but not limited to, the subsequent provisions: a. Section 3: Governing general application; b. Section 11: Dictating imperative and permissive construction, specifically regarding the obligatory nature of “shall” and the discretionary nature of “may”; c. Section 12: Establishing that every enactment is deemed remedial and shall be accorded such fair, expansive, and liberal construction as optimally ensures the realization of its underlying objectives; d. Section 15: Concerning the application of interpretation provisions and rules; e. Section 16: Pertaining to the terminology utilized within regulations; f. Section 25: Regulating documentary evidence; g. Section 34: Classifying indictable and summary conviction offences; h. Section 35: Defining “contravene” as incorporating a failure to comply; defining “telecommunications” as the emission, transmission, or reception of signs, signals, writing, images, sounds, or intelligence of any nature by any wire, cable, radio, optical, or other electromagnetic system, or by any comparable technical mechanism; and defining “writing” to encompass words printed, typewritten, painted, engraved, lithographed, photographed, or represented or reproduced by any modality of visible manifestation. Furthermore, comprehensive reliance is situated upon the following statutory provisions contained within the *Canada Evidence Act*, without limitation: a. Section 23: Concerning the evidence of judicial proceedings; b. Section 29(9); c. Section 31.2; d. Section 31.3; e. Section 31.8; f. Section 35; and g. Section 36.

19. This Application concerns the RCMP’s **refusal to conduct any search** for the Applicant’s Personal Information under the *Privacy Act*, RSC 1985, c. P-21. The RCMP did not perform a search of:

- a. **foundational metadata** (Level 2), including ORI, terminal ID, system identification number, and PPU 005 transaction logs; and
- b. **amended or purged data** (Level 3), including hexadecimal dumps, offline mainframe interrogation, audit trails, and version histories.

(see: for distinction purposes, Tab 11, page 431 and 432).

20. The RCMP’s refusal to search is **not a complaint category** under s. 29(1) of the *Privacy Act*. The Privacy Commissioner has **no jurisdiction** to investigate or remedy a refusal to search. The Applicant therefore has **no adequate alternative remedy**, and mandamus lies.

- 813
21. On April 7, 2026, the Applicant formally invoked **s. 8(2)(m)** of the *Privacy Act* in a written request addressed to Commissioner Michael Duheme, the **Head** of the institution. This triggered the Commissioner’s **mandatory statutory duty** to personally consider whether the public interest in disclosure clearly outweighs any invasion of privacy. The RCMP did not acknowledge, consider, or respond to this request. (*see: Tab 3, sub-tabs, P to S*).
22. On June 2, 2026, when the Applicant served the Commissioner electronically, an automated response indicated that the Commissioner was “away on duty” until late June. This contemporaneous fact confirms that the Commissioner was unavailable to exercise discretion at the time of service, but it does **not** suspend the RCMP’s statutory obligations, nor does it cure the earlier refusal to search or the earlier refusal to consider s. 8(2)(m).
23. The evidentiary record demonstrates that the RCMP has never possessed, and could never have possessed, a validly issued *Criminal Code* Form 2 Information or Form 7 Warrant corresponding to Police Case ID 457197 (*see: Application Record, pages 74 and 325*). Instead, the RCMP produced a **fabricated, digitally manipulated, incomplete “Information Package”**, missing mandatory pages, missing judicial signatures, and bearing metadata proving it was generated using **GrapeCity.Documents for PDF v. 6.0.2.0**, a commercial SDK external to the secure ICON/FRANK judicial systems (*see: Application Record, page 179, 343, 391, 397, 430, 431*).
24. The Applicant’s arrest on October 2, 2024, was therefore executed **without lawful authority**, contrary to ss. 7, 8, and 9 of the **Charter**, and contrary to the statutory requirements of the *Criminal Code*, including ss. 29, 504, 507, and 508. The RCMP’s refusal to search foundational metadata and amended/purged data prevents the Applicant from accessing the records necessary to vindicate his statutory and constitutional rights. This refusal is unreasonable, incorrect, procedurally unfair, and contrary to the purpose of the *Privacy Act*.

B. THE RESPONDENTS’ DEFAULT

25. The calculated dereliction exhibited by the respondents in omitting the submission of form 305 (the “**Form 305**”) does not merely constitute a procedural irregularity; rather, it represents a deliberate procedural election yielding profound legal consequences and operates as an absolute nullity regarding any subsequent participatory entitlements. The prescribed statutory instrument unambiguously articulates that an entity desiring to oppose the application is strictly required to file a notice of appearance (the “**Notice Of Appearance**”) within a designated ten-day duration, failing which said entity is categorically disentitled to any future notification concerning advancing steps within the application framework. It is submitted that *rule 305* of the *Federal Courts Rules*, being formally prescribed by the Governor General of Canada pursuant to a democratically enacted parliamentary enabling statute, is not amenable to an arbitrary, dismissive, or insouciant disposition, particularly when such recalcitrance is perpetrated by a federal **Institution** commanding an approximate seven-billion-dollar annual budgetary allocation. The procedural comportment of the RCMP, an administrative entity birthed and perpetuated by federal statutory mechanisms, transcends mere irony and paradox, culminating unequivocally in a *reductio ad absurdum*. Furthermore, for the facilitation of judicial convenience, *rule 305* explicitly mandates that a respondent

26. The formal procedural default executed by the respondents operates to definitively substantiate the following incontrovertible truths:
 - a. The respondents do not offer opposition to the specified relief sought.
 - b. A calculated administrative determination has been effectuated to entirely abstain from adjudicative participation.
 - c. A complete absence of evidentiary materials has been tendered for judicial consideration.
 - d. No rationale or justification has been articulated addressing the persistent refusal to execute the mandated search.
27. No elucidation has been proffered regarding the fabrication of the false information package (the “**False Information Package**”), nor has any explanation been supplied for the perpetuation of potentially inaccurate proprietary personal information implicating the applicant, the fictitious judicial persona identified as Justice of the Peace Mr. George Jiri, and a fictitious informant ostensibly functioning as Court Officer (Toronto Region) Mrs. Frugoni-Rojas. Consequently, the judiciary is incontrovertibly entitled and required to decide in that a “may” becomes a “must” (see: *Julius v. Oxford (Bishop of)* (1880), App. Cas. 214 (H.L.), Lord Cairns (nota bene: some other SCC decisions have referenced The Honourable Lordship Blackburn such as this very Federal Court of Canada in The Honourable ACJ Mr. Jerome (as he then was) in *Information Commissioner v. Minister of Employment and Immigration (respondent)*, [1986 CanLII 6836](#)) states at pages 242-243: But there are cases in which the authority or power given is not to do a judicial act, and yet there is a duty on the donee to exercise the power if it appears to be given to the donee for the purpose of making good a right, and he is called upon by those who have that right to exercise the power for their benefit.)—and inextricably bound by overarching equitable doctrines—to proceed upon the uncontradicted evidentiary *acta* systematically filed by the applicant. The prevailing legal threshold governing the adjudication of the substantive merits remains the balance of probabilities (the “**Balance Of Probabilities**”). Notwithstanding the absolute default of the respondents and the ensuing *in limine* nullification of their participatory standing, the adjudicative obligation to meticulously evaluate the evidentiary foundation remains resolutely intact; the determinative legal inquiry necessitates an exhaustive assessment of whether clear, cogent, and compelling evidence has been marshaled to satisfy the requisite preponderance threshold, conceptually demarcated as the fifty-one to forty-nine percent evidentiary continuum, thereby mandating the dispensation of the requested relief. Applying the doctrine of *prima facie* substantiation, an advanced legal syllogism is necessarily engaged regarding the discharge of the evidentiary burden in the absence of adversarial contestation. Wherein an applicant fulfills the initial evidentiary onus through the submission of uncontroverted documentation demonstrating an *ultra vires* statutory contravention, and the opposing state apparatus intentionally abstains from challenging said evidentiary matrix, the scales of the **Balance Of Probabilities** are *ipso facto* tipped inexorably in favour of granting the sought declarations and prerogative writs. The fabricated instrumentation and corresponding metadata anomalies, maintaining a status of being completely unrefuted, ascend beyond mere

C. FACTUAL BACKGROUND

The Applicant's PII Access Request (March 11, 2026)

28. On March 11, 2026, the Applicant submitted a detailed **Personal Information Request** to the RCMP seeking foundational metadata and amended/purged data associated with Police Case ID 457197 ((see: Application Record, pages 74 and 325), including:
- ORI;
 - terminal ID;
 - system identification number;
 - PPU 005 transaction logs;
 - audit trails;
 - hexadecimal dumps;
 - any records explaining the creation, modification, or purging of the Information Package.
29. The RCMP acknowledged receipt but refused to conduct any search of the repositories reasonably expected to contain responsive records.

The April 7, 2026 s. 8(2)(m) Public-Interest-Disclosure Request

30. On April 7, 2026, the Applicant wrote directly to Commissioner Duheme, formally invoking **s. 8(2)(m)** of the *Privacy Act* and requesting that the Head of the **Institution** consider whether the public interest in disclosure clearly outweighs any invasion of privacy.
31. This request was detailed, legally grounded, and supported by extensive uncontroverted evidence of:
- documentary metamorphosis;
 - metadata anomalies;
 - jurisdictional nullities;
 - potential systemic vulnerabilities in CPIC; and
 - the public-interest implications of fabricated judicial instruments.
32. The RCMP did not acknowledge, consider, or respond to the request. This constitutes a **refusal to exercise discretion**, a reviewable error under s. 18.1 of the *Federal Courts Act*.

The Arrest of October 2, 2024

816 33. The Applicant was arrested on October 2, 2024, by the Toronto Police Service (“TPS”) purportedly pursuant to a Warrant for Arrest.” TPS refused to produce the warrant when demanded under *Criminal Code* s. 29, despite being lured to the TPS 14th Division under false pretenses regarding receiving the Applicant’s property from an unnamed source. The Application Record contains **no valid Form 7 Warrant**, nor any judicial authorization corresponding to Police Case ID 457197 because this INTAKE COURT ENDORSEMENT (SEPT 23 2024) has never been produced by any source (see: Application Record, pages 74 and 325).

The “False Information Package”

34. The RCMP produced a five-page “Information Package” purporting to be a *Criminal Code* Form 2 Information. The authentic Form 2 is a **six-page** pro forma document used throughout Ontario. The Applicant’s Application Record demonstrates that:

- a. Page 4 (swearing/attestation, judicial signature, Crown election, plea, committal) is missing;
- b. Page 5 (counts, sentence date, withdrawn counts) is missing;
- c. No judicial signature appears anywhere;
- d. The purported Informant is fictitious;
- e. The document contains digital artifacts (“CL (M)”) consistent with failed template merging; and
- f. The metadata identifies **GrapeCity.Documents for PDF v. 6.0.2.0** as the generator.
(see: Application Record, Tab 10, *ATIA* Request of the Applicant of May 5, 2026, delivered to RCMP on May 7, 2026).

Metadata Proving Fabrication

35. The PDF metadata embedded in the Information Package conclusively identifies the document as having been generated using: “GrapeCity.Documents for PDF, Version 6.0.2.0.”

36. This software is a commercial developer SDK, not a judicial document-generation system. Authentic criminal process in Ontario is generated exclusively through:

- a. **ICON** (Integrated Courts Offences Network); and
- b. **FRANK** (Framework for Automated and Networked Courts).

37. Neither ICON nor FRANK can produce documents with GrapeCity metadata. The presence of this metadata proves that the Information Package was **not generated by any court**, but was instead **synthetically compiled** outside the judicial system.

The RCMP’s Refusal to Search

38. Despite the Applicant’s detailed request, the RCMP refused to search:

- a. foundational metadata repositories;
- b. the Offline Historical Database;

- c. PPU 005 logs;
- d. amended/purged data repositories; and
- e. any system reasonably expected to contain responsive records.

39. The refusal to search is unreasonable, contrary to the *Privacy Act*, contrary to the duty of fairness, and contrary to the purpose of access legislation. While it is contrary to all of those laws, whether statutes or regulations (commonly known as “**Source Laws**” (see: *supra*)), the common law and courts of equity (as they once were but since merged into a single court system under the FCC), it was rather ingenious of the RCMP to do so because it is not a ground where an Applicant can make a complaint the Privacy Commissioner of Canada, the Honourable Mr. Dufesene.

PART II — POINTS IN ISSUE

40. This Application raises the issue of standard of review of the RCMP’s failure to act and the Head of the RCMP’s failure or inability to act as a consequence of the former along with seven primary issues for determination along with secondary issues. Each issue flows directly from the Respondents’ refusal to conduct a search under the *Privacy Act*, their refusal to exercise mandatory statutory discretion under s. 8(2)(m), and their failure to file and serve, as anticipated, a Certified Tribunal Record under Rule 317. Or in the alternative, whether the refusal to search by the RCMP (an “Other Tribunal” under the *Federal Courts Rules* and *Federal Courts Act*) renders each issue flowing from it.ⁱⁱ

ISSUE #1: REFUSAL TO SEARCH

41. The first issue is as follows: whether the RCMP breached its statutory duty under the *Privacy Act* by refusing to conduct any search for the Applicant’s Personal Information. The central issue is whether the RCMP’s refusal to conduct **any search at all** for foundational metadata (Level 2) and amended/purged data (Level 3) constitutes a breach of its statutory obligations under ss. 4, 6, and 12 of the *Privacy Act*.
42. The RCMP did not search: the Foundational Metadata repositories (ORI, terminal ID, system identification number, PPU 005 logs); the Offline Historical Database (hexadecimal dumps, audit trails, version histories); and any repository reasonably expected to contain responsive Personal Information. A refusal to search is a refusal to perform a statutory duty. It is not a “refusal to disclose” and therefore does **not** fall within any complaint category under s. 29(1) of the *Privacy Act*.

ISSUE NO. 2: REFUSAL TO DISCHARGE A PUBLIC DUTY TO SEARCH IS REVIEWABLE BY THE FCC AND ONLY THE FCC, AND THE WRIT OF MANDAMUS IS AVAILABLE TO THE APPLICANT AND THOSE SIMILARLY SITUATED

43. The second issue is **whether the RCMP’s refusal to search is reviewable by mandamus.**

44. Mandamus lies where:

- 818**
- a. a public legal duty exists;
 - b. the duty is owed to the Applicant;
 - c. the Applicant has a clear right to performance;
 - d. no adequate alternative remedy exists;
 - e. a Respondent has refused to act;
 - f. the duty is non-discretionary (or where it is discretionary, the discretion is fettered and must be exercised (i.e. it does not guarantee a result but it guarantees an exercise of the non-discretionary duty or the discretionary duty (nota bene: even discretion with latitude must be exercised in a lawful, non-abusive, good faith manner);
 - g. the Moving Party, the requestor, plaintiff or applicant comes with clean hands; and
 - h. the order will be effective in its utility.

45. All criteria are met. The RCMP has a **non-discretionary duty** to search for Personal Information. The Privacy Commissioner has **no jurisdiction** over refusals to search. The RCMP has expressly refused to act. Mandamus is therefore the appropriate remedy.

ISSUE #3: CLAUSE 8(2)(M) OF THE PRIVACY ACT: THE FAILURE TO CONSIDER BY THE HEAD OF THE INSTITUTION

46. The foregoing issue is whether the RCMP Commissioner breached his mandatory duty to consider public-interest disclosure under s. 8(2)(m) of the *Privacy Act*. On April 7, 2026, the Applicant formally invoked s. 8(2)(m) in a written request addressed to Commissioner Duheme, the Head of the institution. This triggered the Commissioner's **mandatory statutory duty** to personally consider whether the public interest in disclosure clearly outweighs any invasion of privacy. (*see: Application Record, supra*). The RCMP did not acknowledge, consider, or respond to the request. This constitutes a **refusal to exercise discretion**, a reviewable error under s. 18.1 of the *Federal Courts Act*. The Commissioner's automated "away on duty" (whatever that means in fact or at law) response on or around May 21, 2026, does not suspend statutory obligations, nor does it cure the earlier refusal to consider the Applicant's April 7 request. In fairness, the Commissioner Mr. Duheme's email stated:

"Prenez note que je serai absent en devoir à compter du 21 mai au 19 juin. Sous Commissaire Bryan Larkin agira à titre de Commissaire par intérim. Vous pouvez le rejoindre à Bryan.Larkin@rcmp-grc.gc.ca.

The 21st May to 19 June, I will be away on duty , Deputy Commissioner Bryan Larkin will be the acting Commissioner. He can be reached at Bryan.Larkin@rcmp-grc.gc.ca"

ISSUE #4: REFUSAL TO SEARCH FOR FOUNDATIONAL METADATA AND OFFLINE HISTORICAL DATABASE

47. The foregoing issue is whether the RCMP's refusal to search foundational metadata, contained with a PIB under PPU 005 (i.e. the ORI; issuing court; issuing court level; issuing court location; name of the judicial officer of the

819 “Ex Parte In Camera Hearing” (so presiding); and the system identification number), and amended/purged data in the Offline Historical Database is any of the following: Incorrect or in the alternative, unreasonable; procedurally unfair; and/or contrary to the purpose of the *Privacy Act*. The *Privacy Act* is quasi-constitutional legislation designed to protect informational privacy and ensure individuals can access Personal Information under the control of government institutions. The RCMP’s refusal to search:

- a. frustrates the purpose of the Act;
- b. intentionally mock Parliament and its intentional and deliberate choice of language, intent and spirit of the *Privacy Act* (and the *ATIA*);
- c. mocks our fundamental notion of democracy;
- d. flouts our common law system with impunity;
- e. prevents the Applicant from accessing Personal Information to which he is entitled;
- f. prevents the Applicant from verifying the authenticity of the Information Package; and
- g. prevents the Applicant from determining whether any lawful authority existed for his arrest.

48. The refusal is therefore unreasonable, incorrect, and contrary to the governing principles of privacy law.

ISSUE #5: FRAUD UNRAVELS EVERYTHING BUT IT IMPOSES POSITIVE DUTIES ON ALL MOST NOTABLY FEDERAL INSTITUTIONS LIKE THE RCMP

49. Whether the fabricated “Information Package” and its metadata anomalies require the Court to order a mandatory search of amended/purged data.

50. The Application Record demonstrates that the Information Package:

- a. is missing mandatory pages;
- b. contains no judicial signature by a judicial officer (Justice of the Peace; OCJ Judge; or Judge of Superior Court Of Criminal Jurisdiction (see: *Criminal Code* definition)) which will undoubtedly be contained in CPIC as the frame of reference for universal truth;
- c. contains inconsistent footers;
- d. contains digital artifacts (“CL (M)”); and
- e. was generated using **GrapeCity.Documents for PDF v. 6.0.2.0**, a commercial SDK external to ICON/FRANK.

51. These anomalies raise serious concerns regarding: authenticity; alteration; fabrication; purging; and unauthorized modification. Only a Level 3 search — including hexadecimal dumps, offline mainframe interrogation, and audit trail extraction — can determine the genesis and modification history of the document. The RCMP’s refusal to conduct such a search is unreasonable and contrary to its statutory obligations.

ISSUE #6: FRAUDULENT MISREPRESENTATIONS PERPETRATED UPON THE JUDICIARY ARE MIRRORED WITHIN THE CANADIAN POLICE INFORMATION CENTRE SYSTEM, AND THE CONCOMITANT POSITIVE OBLIGATIONS IMPOSED UPON THE ROYAL CANADIAN MOUNTED POLICE AS CUSTODIAN AND CONTROLLER

52. An unprecedented and thoroughly untested jurisprudential question crystallizes upon the determination of whether the originating data sequence introduced into the centralized repository of the Canadian Police Information Centre

(the “CPIC”)—without regard to the specific law enforcement apparatus functioning as the originating terminal, whether ostensibly operating in the capacity of a principal or an agent, and irrespective of the designated alphanumeric case identification nomenclature—substantively and materially mirrored the contents encapsulated within the admitted false information package (the “False Information Package”). It is advanced that the foundational fraudulent misrepresentations perpetrated upon the judiciary were unconscionably effectuated through the illicit utilization of Portable Document Format manipulation software by law enforcement personnel. This systemic subversion of the judicial process is profoundly compounded by the anomalous jurisdictional involvement of the Ontario Court of Justice situated at 10 Armoury Street, encompassing its presiding Justices of the Peace and, specifically, the Honourable Mr. Justice Block. Given that Mr. Justice Block’s antecedent legal practice prominently featured the defense and representation of law enforcement officers subjected to regulatory and administrative scrutiny by various oversight bodies, the deliberate channeling of this adjudicative process before this specific jurist strongly infers a calculated stratagem of impermissible forum shopping—jurisprudentially characterized as “bench hunting”—thereby fatally vitiating the ensuing authorizations. Provided that the inputted data unequivocally corresponds with the aforementioned fabricated package, it follows *ipso facto* that the applicant (the “Applicant”) is indisputably entitled to the compulsory disclosure of said data, characterized legally as proprietary personal information (the “Personal Information”).

53. With the benefit of the Applicant finding the **Lincoln County Law Association (Niagara) Pro Forma Information Package** in July 2025 (as this Honourable Court can check the metadata therein as the metadata never lies), the obvious question screams out: how could multiple justices of the peace and an OCJ Judge look at this file with its Information Number and not notice multiple pages missing from said False Information Package and not positively act? **Only they know and that is beyond the scope of this FCC Application.**
54. This entitlement to disclosure persists undiminished notwithstanding the demonstrable reality that the foundational data is ostensibly fabricated and intrinsically fallacious, a foundational principle affirmed in *Lawson v. Accusearch Inc.*, [2007 FC 125](#).
55. The collateral and subordinate legal inquiry mandates a rigorous forensic investigation into whether the nascent data matrix integrated into the CPIC framework—specifically designating a warrant in the first instance and utilizing the identifier “MCLEAN, Kevin”—maintained structural integrity and absolute accuracy at the exact temporal moment of its inception. This assessment must be conducted independently of the fundamentally contested substantive merits pertaining to the ex parte in camera hearing (the “Ex Parte In Camera Hearing”) or the ostensibly authoritative intake court endorsement (the “Intake Court Endorsement”), bearing the date of September 23, 2024. Of paramount jurisprudential significance is the judicial determination as to whether this specific data matrix was subsequently subjected to *post hoc* unauthorized modifications, executed either antecedent to or immediately succeeding the physical apprehension and detention of the Applicant. Assuming the metadata possessed technical exactitude *in limine*, yet was subsequently and strategically manipulated to forcibly harmonize

821 with the precise parameters necessitated by the CPIC architecture—specifically, the foundational metadata (the “Foundational Metadata”), encompassing the originating agency identifier (the “Originating Agency Identifier” or “ORI”); the designated issuing authority or court field (the “Court Field”); the remarks and narrative field (the “Narrative Field”); and the system identification number (the “System Identification Number” or “SID”) autonomously generated upon initial entry—such machinations transcend mere procedural irregularities. Rather, they constitute a catastrophic abuse of process, rendering the antecedent authorizations an absolute nullity, as opposed to a mere irregularity, given that such systemic alterations represent a direct contravention of established equitable principles and statutory frameworks. Collectively, these delineated components are taxonomically classified as the foundational data elements constituting a want record (the “WANT Record”). It is advanced as a highly persuasive syllogistic extrapolation that the originating law enforcement agency, explicitly designated by the initial Originating Agency Identifier, was demonstrably not the identical entity that subsequently perpetrated the clandestine and surreptitious alterations upon the Want Record. These prospective, unauthorized systemic modifications, which are *prima facie* indicative of profound malfeasance, encompass four distinct and independent vectors of systemic manipulation: a. The deliberate modification, falsification, or complete reassignment of the Originating Agency Identifier, effectuated to deceitfully transfer the veneer of jurisdictional authority to an entirely disparate police service; b. The structural and substantive alteration of the jurisprudential authority designated within the Court Field, maliciously engineered to artificially legitimize an arrest warrant that was unambiguously void *ab initio* and fundamentally a nullity; c. The material revision of the contents within the Narrative Field, executed with the demonstrable intent to retroactively and speciously justify the unlawful apprehension of the Applicant; and d. The systemic desynchronization, obfuscation, or deliberate reallocation of the System Identification Number, mathematically formulated to conceal the authentic timestamp and effectively obliterate the evidentiary audit trail associated with the fabricated digital entry.

56. The forensic verification of these administrative maneuvers—and the consequent unmasking of the underlying institutional malfeasance, which is fundamentally *ultra vires* the statutory authority of the offending entities—can exclusively be elucidated through an uncompromising, granular examination of the automated hexadecimal transaction logs and sequential digital trails. Consequently, this indispensable evidentiary determination can solely be actualized through the compulsory and unmitigated disclosure of the Personal Information of the Applicant, which is definitively housed within a personal information bank (the “Personal Information Bank”) and unequivocally remains under the absolute administrative control and constructive possession of the centralized federal repository. While international legislative frameworks, notably the *General Data Protection Regulation* (the “GDPR”), explicitly bestow upon an applicant the positive statutory right to compel the erasure or deletion of data, domestic legislation presents a divergent paradigm. Specifically, the *Personal Information Protection and Electronic Documents Act* (the “PIPEDA”) lacks perfectly analogous provisions, and an exhaustive statutory interpretation yields no discernible language enacted by Parliament within the *Privacy Act* that would facilitate an

identical equitable remedy of deletion. Notwithstanding this legislative lacuna, a supervening and paramount legal issue crystallizes herein regarding whether affirmative, positive legal duties are imposed upon the Royal Canadian Mounted Police to proactively notify all individuals whose Personal Information is thus improperly implicated concerning a privacy breach. This imperative arises despite the conspicuous absence of a formal definition for “Breach of Security Safeguards” or a corresponding regulatory framework within the *Privacy Act* that would explicitly encompass the dissemination of the identities of the authentic presiding jurist of the Ex Parte In Camera Hearing; the fabricated judicial persona—a fictitious construct demonstrably possessing a jurisdictional nexus to the Royal Canadian Mounted Police and its specifically designated investigative file, being Police Case ID: 457197, ostensibly established via an anomalous proximity to the Toronto West Detachment of the Royal Canadian Mounted Police, notwithstanding the spatial incongruity that said detachment is counterintuitively situated within the municipal boundaries of Milton, Ontario, rather than the anticipated western jurisdiction of Toronto; and the Applicant. To the extent that a rigid statutory duty of mandatory notification by a government **Institution** is ostensibly absent, a corollary deduction necessitates determining whether such an overarching obligation is intrinsically subsumed and legally enforceable under the auspices of paragraph 8(2)(m) of the *Privacy Act*, thereby preserving the *status quo ante* and preventing the perpetuation of a nullity derived from systemic concealment.

PART III — LAW AND ARGUMENT

A. THE STANDARD OF REVIEW OF THE RCMP’S FAILURES TO ACT; AND THE RCMP HAS A STATUTORY DUTY TO CONDUCT A REASONABLE SEARCH FOR PERSONAL INFORMATION

The Standard of Review

57. It is a trite postulate of administrative jurisprudence that the applicable standard of review governing the primary issues herein, specifically concerning the adjudicative scrutiny of the RCMP acting in its capacity as a tribunal (the “**Tribunal**”), is exclusively that of correctness.
58. In the seminal jurisprudential authority of *Canada (Minister of Citizenship and Immigration) v. Vavilov*, [2019 SCC 65](#) (the “*Vavilov*”), the Supreme Court of Canada (the “**SCC**”) effectuated a profound metamorphosis of the administrative law paradigm, thereby superseding the erstwhile analytical framework formerly established in *Dunsmuir*. By virtue of this landmark pronouncement, a revised framework for judicial review (the “**Judicial Review Framework**”) was promulgated, predicated upon the foundational ethos that a culture of justification (the “**Culture of Justification**”) necessitates all state delegates to proffer adjudicative reasons characterized by internal coherence and rigorous justification commensurate with the prevailing legal and factual constraints. Consequently, the reasonableness standard (the “**Reasonableness Standard**”) operates as the *prima facie* baseline for the evaluation of state action, subject to delineated jurisprudential and statutory exceptions.

- 823
59. It is a foundational doctrine of Canadian administrative law that an aggrieved party retains an inherent constitutional entitlement to seek judicial intervention. As elucidated within contemporary academic and jurisprudential discourse pertaining to the Culture of Justification, it is postulated that affording the judiciary an untrammelled discretionary prerogative to decline the adjudication of applications for judicial review—predicated upon a subjective evaluation of the efficacy of internal reconsideration mechanisms—would permit judicial discretion to subvert foundational constitutional principles. While the reviewing court retains the *in limine* discretion to adjudicate an application upon its substantive merits and subsequently deny equitable or prerogative relief, it is submitted that such discretion does not encompass an outright refusal to entertain the application for judicial review *ab initio*, a legal axiom unequivocally affirmed at paragraph 49 of *Yatar v. TD Insurance Meloche Monnex*, [2024 SCC 8](#) (the “*Yatar*”).
60. The *Vavilov* jurisprudence categorically reconstituted the judicial review topography, departing significantly from the preceding *Dunsmuir* epoch. Commencing in the year 2019, whilst the presumptive standard of review remains that of reasonableness, the aforementioned presumption is invariably displaced by the correctness standard (the “**Correctness Standard**”) in a plurality of specified circumstances, all of which are manifestly applicable within the parameters of the present proceedings.
61. There exist, at a minimum, five primary exceptions to the presumptive Reasonableness Standard, specifically: a. instances wherein the Correctness Standard is statutorily mandated by the legislature; b. circumstances wherein statutory appeal mechanisms are explicitly prescribed; c. adjudications necessitating the resolution of constitutional questions; d. determinations involving general questions of law of central importance to the legal system collectively; and e. adjudications pertaining to the jurisdictional boundaries delineating administrative entities, as exhaustively articulated in *Vavilov* at paragraphs 34, 36, 55, 58, and 63.
62. The latter exceptions, specifically those enumerated in subsections (c) through (e), are designated herein as the rule of law standard of review exceptions (the “**Rule of Law SOR Exceptions**”).
63. Furthermore, the jurisprudential principles articulated in *Society of Composers, Authors and Music Publishers of Canada v. Entertainment Software Association*, [2022 SCC 30](#) (the “*SOCAN*”) demarcated a supplementary basis for the rebuttal of the reasonableness presumption: the existence of concurrent jurisdiction between the judiciary and an administrative tribunal, particularly in circumstances wherein there manifests a persistent jurisdictional discord or inconsistency in the application of substantive legal principles.
64. Pursuant to the plurality reasons in *Vavilov* at paragraph 54, upon the invocation of the Correctness Standard, the reviewing court is imbued with the jurisdictional authority to either substantiate the administrative determination or, in the alternative, substitute its own judicial reasoning for that of the administrative decision-maker, a methodology strictly consistent with the orthodox principles delineated in *Dunsmuir* at paragraph 50.
65. The *Vavilov* decision was promulgated by a *coram* of nine justices of the SCC. Whilst seven justices authored the joint majority reasons (the “**Vavilov Joint Reasons**”), Justices Abella and Karakatsanis articulated joint concurring reasons (the “**Vavilov Joint Concurring Reasons**”).

- 824** 66. Within the Vavilov Joint Reasons, the majority opined that questions of central importance have been transmuted to a comprehensive classification necessitating correctness review, predominantly because administrative expertise no longer operates as a determinative criterion in the selection of the applicable standard of review, as explicitly articulated at paragraph 61.
67. As unequivocally established in *Vavilov*, the application of reasonableness review can never be legitimized solely through an invocation of administrative expertise, as such a doctrinal concept does not confer upon administrative delegates a prerogative to enlarge their jurisdictional mandate or to omit the statutorily mandated exercise thereof beyond the strict parameters of legislative intendment. The overarching statutory architecture perpetually operates as an incontrovertible constraint upon administrative delegates, effectuating a circumscription of their adjudicative authority, a fundamental legal principle emphasized *ipso facto* at paragraph 68.
68. In 2019, the SCC elucidated that whilst the common law presumption ostensibly favors reasonableness, said presumption is expeditiously rebutted wherein the statutory architecture stipulates a right of statutory appeal upon questions of law. In the present adjudicative matrix, the questions of law are manifold, historically evasive of orthodox appellate review, and of paramount consequence to both substantive jurisprudence and the procedural mechanisms governing access requests under the *Privacy Act*, RSC 1985, c P-21 (the “*Privacy Act*”) and the *Access to Information Act*, RSC 1985, c A-1 (the “*ATIA*”). Specifically, these matters involve proceedings before the RCMP and elucidate the mandatory procedural trajectories to be undertaken when section 29 of the *Privacy Act* does not statutorily authorize a request to transmogrify into a formal complaint following an institution’s failure or refusal to conduct a mandatory search. Furthermore, the issues address circumstances wherein the head of the **Institution** has failed or neglected, whether as a direct consequence of the aforementioned failure or otherwise, to even contemplate the exercise of discretionary authority pursuant to section 8(2)(m) of the *Privacy Act* or, more expansively, under section 19 of the *ATIA*. Any such failure to adhere to the statutory mandate constitutes a fundamental nullity rather than a mere procedural irregularity, given that it represents a direct contravention of a prevailing legislative statute and equitable principles. Such contravention irremediably vitiates the administrative action, rendering it *ultra vires*, void *ab initio*, and entirely rebutting any residual presumption of *omnia praesumuntur rite esse acta*.
69. As meticulously observed within the Vavilov Joint Concurring Reasons, the methodological approach adopted by the majority of the SCC effectuated the systematic divestiture of curial deference from an extensive multitude of administrative actors who are subjected to statutory rights of appeal, questions of law, and general questions of law of central importance to the legal system in its entirety.
70. Notwithstanding the foregoing, when evaluating the profound significance of questions of law, or inextricably intertwined questions of mixed fact and law wherein the legal inquiry is extricable, alongside general questions of law of central importance to the legal system as a whole, it is an irrefragable syllogism that securing a judicially

correct determination is paramount to merely assessing whether the administrative decision was ostensibly reasonable. The proposition inherently resolves itself through the application of deductive legal logic.

71. In addressing whether the adjudicative questions posed herein possess a general nature of central importance to the legal system as a comprehensive entity, the affirmative conclusion is rendered self-evident by the substantive gravity of the constitutional and administrative principles that are inextricably engaged. It is respectfully submitted that the entirety of the jurisprudential questions raised herein are intrinsically of a general nature and of central importance to the legal system collectively. Consequently, predicated upon this ground independently, and without prejudice or limitation to alternate meritorious grounds, the applicable standard of review governing the non-appearing RCMP, acting as a tribunal or 'other tribunal' as contemplated by the *Federal Courts Rules*, SOR/98-106, *Rule 317* and *Rule 2* (the “*Federal Courts Rules*”), alongside the *Federal Courts Act*, RSC 1985, c F-7, *section 2* (the “*Federal Courts Act*”), is incontrovertibly that of correctness, mandating an immediate judicial intervention to restore the *status quo ante*.

The Failure of the RCMP to conduct a search of the Foundational Metadata repository and the Offline Historical Database

72. The *Privacy Act* imposes a **positive, non-discretionary duty** on government institutions to identify, locate, and retrieve Personal Information under their control. This duty arises from the combined operation of ss. 4, 6, and 12:
- a. **Section 4** requires institutions to collect only information directly related to their operating programs;
 - b. **Section 6** requires institutions to maintain accurate, complete, and up-to-date records;
 - c. **Section 7** requires the **Institution** to only use Personal Information under control of the Government **Institution** for the purpose for which the information was obtained or compiled by the Government **Institution** or for a use consistent with that purpose; OR requires the **Institution** to only disclose (NTD); and
 - d. **Section 12(1)** grants individuals the right to access Personal Information “about themselves that is under the control of a government institution.”
73. There can never be a purpose for which the information was obtained or compiled by the Government **Institution** or for a use consistent with that purpose; or for a purpose for which the information may be disclose to the **Institution** under section 8(2) when the initial or subsequent information including Personal Information was fraudulent input or amended thereafter to ensure that it was “consistent” with the fraud committed on the OCJ 10 Armoury Street Courthouse by those utilizing PDF manipulation software in the form of the SDK then known as GrapeCity.Documents.For.PDF (version 6.0.2.0). The right of access under s. 12(1) is meaningless unless the **Institution** performs a **reasonable search** for responsive records. A refusal to search is therefore a refusal to perform a statutory duty. The RCMP’s refusal to conduct **any search at all** for foundational metadata (Level 2) or amended/purged data (Level 3) constitutes a breach of its statutory obligations. It is axiomatic that the duty to search is not optional. It is not discretionary. It is not subject to internal policy preferences. It is a **mandatory**

THE RCMP'S REFUSAL TO SEARCH IS NOT REVIEWABLE BY THE PRIVACY COMMISSIONER

74. Section 29(1) of the *Privacy Act* exhaustively enumerates the categories of complaints the Privacy Commissioner may investigate. These include:

- a. improper use or disclosure (s. 29(1)(a));
- b. refusal of access (s. 29(1)(b));
- c. refusal to correct (s. 29(1)(c));
- d. unreasonable extensions (s. 29(1)(d));
- e. language/format issues (s. 29(1)(e), (e.1));
- f. inappropriate fees (s. 29(1)(f));
- g. issues with the index (s. 29(1)(g)); and
- h. issues relating to collection, retention, disposal, use, disclosure, or requesting access (s. 29(1)(h)).

75. **None of these categories include a refusal to search.** The duty to search is not a matter within the Commissioner's jurisdiction for patently obvious and axiomatic reasons underpinning Parliament's passing and amending of the *Privacy Act* since 1985 (nota bene: some 92 versions since September 24, 2002). The Federal Court has confirmed that where the Commissioner lacks jurisdiction, the appropriate remedy is **judicial review and mandamus**, not a complaint to the Commissioner. Accordingly, the Applicant has **no adequate alternative remedy**, satisfying a key requirement for mandamus.

C. THE RCMP'S REFUSAL TO SEARCH FOUNDATIONAL METADATA (LEVEL 2) IS UNLAWFUL

76. Foundational metadata includes:

- a. the **ORI** (Originating Agency Identifier);
- b. the **terminal ID** used to create and potentially the Terminal ID (may be the same or different to modify the records, data and Personal Information;
- c. the **system identification number**; and
- d. **PPU 005 transaction logs** showing when, where, and by whom the record was created or altered.

77. These records are essential to determining:

- a. whether the Information Package ever existed in a lawful form. If so, what were the data points involving the same?
- b. whether it was created within ICON/FRANK;
- c. whether it was modified, overwritten, or purged; and/or
- d. whether the RCMP and any law enforcement agency including "Police Services" unlike how the RCMP refers to itself as "Police Forces" ever possessed lawful judicial authorization.

78. The RCMP refused to conduct even a basic audit of PPU 005 logs (*see: Tab 1, Page 8 of the PII Access Request (March 11 2026)*). This refusal is unreasonable, contrary to the *Privacy Act*, and contrary to the duty of fairness.

827 The RCMP's position — that it is “not authorized to search files belonging to other police forces” — is a misstatement of law.

79. The Applicant did not request “files belonging to other police forces.” He requested his Personal Information which is akin to ownership of the same:

- a. metadata;
- b. system identifiers;
- c. audit trails;
- d. transaction logs;
- e. CPIC entries; and
- f. PPU 005 records.

80. These are **federal records** and federal Personal Information under the control of the RCMP. The RCMP's refusal to search foundational metadata is therefore unlawful.

D. THE RCMP'S REFUSAL TO SEARCH AMENDED OR PURGED DATA (LEVEL 3) IS UNLAWFUL

81. Amended/purged data includes:

- a. hexadecimal dumps;
- b. offline mainframe interrogation;
- c. audit trails;
- d. version histories;
- e. overwritten or deleted entries
- f. “vector collapse” indicators showing unauthorized modification.
- g. These searches are required where, as here, the authenticity of a document is in question. The Applicant's Application Record demonstrates that the False Information Package:
 - i. is missing mandatory pages;
 - ii. contains no judicial signature;
 - iii. contains inconsistent footers;
 - iv. contains digital artifacts (“CL (M)"); and
 - v. was generated using **GrapeCity.Documents for PDF v. 6.0.2.0**, a commercial SDK external to ICON/FRANK.

82. These anomalies raise serious concerns of:

- a. fabrication;
- b. alteration;
- c. purging;
- d. unauthorized modification; and
- e. synthetic document generation.

83. Only a Level 3 search can determine the genesis and modification history of the document. The RCMP's refusal to conduct such a search is unreasonable and contrary to its statutory obligations. The RCMP's position — that it cannot search “files belonging to other police forces” — is irrelevant. The Applicant is not seeking municipal files. He is seeking **federal metadata** stored in:

- a. CPIC;
- b. PPU 005;
- c. the Offline Historical Database; and RCMP-controlled audit logs.

84. These repositories are under the **exclusive control** of the RCMP. The refusal to search them is unlawful.

E. THE LEGAL TEST FOR MANDAMUS IS SATISFIED

85. The Federal Court applies a well-established seven-part test for mandamus. Mandamus will issue where:

- a. A public legal duty exists;
- b. The duty is owed to the Applicant;
- c. The Applicant has a clear right to performance;
- d. No adequate alternative remedy exists;
- e. The Respondent has refused to act;
- f. The duty is non-discretionary; and
- g. The order will be effective.

86. Each criterion is satisfied:

- a. **Public legal duty:** The RCMP has a statutory duty to search for Personal Information (ss. 4, 6, 12).
- b. **Duty owed to the Applicant:** The Applicant is the subject of the information.
- c. **Clear right to performance:** The Applicant provided precise identifiers and repository locations.
- d. **No adequate alternative remedy:** The Privacy Commissioner has **no jurisdiction** over refusals to search (s. 29).
- e. **Refusal to act:** The RCMP expressly refused to conduct any search.
- f. **Non-discretionary duty:** The duty to search is mandatory.
- g. **Effectiveness:** A mandamus order will compel the RCMP to perform the required searches.

87. Mandamus is therefore the appropriate and necessary remedy.

F. THE DOCTRINE OF “CONTROL” UNDER THE PRIVACY ACT AND FEDERAL COURTS JURISPRUDENCE

Control is broader than physical possession

88. The *Privacy Act* does not define “control.” The Federal Court of Appeal has repeatedly held that “control” is a **broad, liberal, purposive concept**, not limited to:

- a. physical possession;
- b. server location;
- c. departmental boundaries; and
- d. municipal vs. federal custody.

829 89. In *Canada Post Corp. v Canada (Minister of Public Works)*, the Court held that control includes: “ultimate, immediate, full, partial, transient, lasting, de jure, and/or de facto control.” The RCMP is the **paramount custodian** of CPIC and PPU 005. It has:

- a. de jure control (statutory authority);
- b. de facto control (operational authority);
- c. common law control (the legal right, privilege or permission to make the demand albeit unto itself);
- d. constructive control (ability to demand records); and
- e. exclusive control (sole administrator of the Offline Historical Database).

90. The RCMP cannot avoid its statutory obligations by asserting that certain records “belong to other police forces.” The Applicant is not seeking municipal records. He is seeking **federal metadata** stored in federal systems.

Control includes the ability to demand records

91. In *Ontario Criminal Code Review Board v. Hale*, our ONCA held that a tribunal has “control” over records if it has the **power to demand** them, even if the records are held by a contractor or third party. The RCMP has the right, power and/or privilege *to make a demand* (albeit it is unto itself and in effect the right to make the demand is the duty to search): CPIC logs; PPU 005 transaction histories; audit trails; hexadecimal dumps; and system identifiers. The RCMP’s refusal to search is therefore a refusal to exercise control, not a lack of control.

Control includes metadata and audit trails

92. Metadata is Personal Information under s. 3 of the *Privacy Act*. It is also “information under the control of a government institution” under s. 12(1). The RCMP’s refusal to search metadata repositories is therefore a refusal to search Personal Information under its control.

Control includes amended and purged data

93. The Offline Historical Database contains: overwritten entries; purged entries; amended entries; version histories; and audit trails. These records, exclusively Personal Information in nature so requested, are under the **exclusive control** of the RCMP. The refusal to search them for the Personal Information request from the Applicant is unlawful.

G. THE RCMP COMMISSIONER BREACHED HIS MANDATORY DUTY TO CONSIDER PUBLIC-INTEREST DISCLOSURE UNDER S. 8(2)(M)

G(I): Section 8(2)(m) imposes a mandatory duty on the Head of the institution

94. Section 8(2)(m) of the *Privacy Act* authorizes disclosure of Personal Information without consent where:

- a. (i) the public interest in disclosure clearly outweighs any invasion of privacy; or
- b. (ii) disclosure would clearly benefit the individual concerned.

95. The jurisprudence is unequivocal. **The Head of the Institution must personally consider the request.**

This duty cannot be delegated, ignored, or deferred. On April 7, 2026, the Applicant formally invoked s. 8(2)(m) in a detailed written request addressed directly to Commissioner Duheme, the Head of the RCMP. (*see: supra*). This triggered the Commissioner's mandatory statutory duty to :review the request; weigh the public interest; consider the Applicant's evidence; determine whether disclosure is warranted; provide reasons.

2. The RCMP refused to exercise discretion

96. The RCMP did not acknowledge, consider, or respond to the Applicant's April 7 request. This constitutes a **refusal to exercise discretion**, a reviewable error under s. 18.1 of the *Federal Courts Act*. A refusal to exercise discretion is as unlawful as an improper exercise of discretion. Put another way, it is a discretion that does not exist at law.

3. The Commissioner's "away on duty" auto-reply does not suspend statutory obligations

97. On June 2, 2026, when the Applicant served the Commissioner electronically, an automated response indicated that the Commissioner was "away on duty" until late June. This contemporaneous fact confirms that the Commissioner was unavailable at the time of service, but it does **not**: suspend statutory duties; cure the earlier refusal to consider the April 7 request; justify the RCMP's failure to act; and negate the Applicant's right to mandamus. The refusal to consider s. 8(2)(m) occurred **before** the Commissioner's absence and is therefore a completed jurisdictional error.

H. MCINERNEY V. MACDONALD

98. It is a foundational tenet of access and privacy jurisprudence, authoritatively elucidated by the Supreme Court of Canada in *McInerney v. MacDonald*, [1992 CanLII 57](#) (SCC) (the "*McInerney Decision*"), that an individual possesses a fundamental, continuing, and trust-like beneficial interest in their personal information (the "**Personal Information**"). Within the *McInerney Decision*, the highest appellate tribunal of this jurisdiction unequivocally decreed that a fiduciary-analogous duty commands the disclosure of such documentary *acta* upon request, an obligation from which the custodian may not capriciously resile. An advanced syllogistic extrapolation of the legal principles articulated within the *McInerney Decision* mandates the application of its ratio decidendi to the statutory imperatives enshrined within the *Privacy Act*, RSC 1985, c P-21 (the "*Privacy Act*").

- 831 99. *A fortiori*, if the speculative fear of frivolous legal proceedings cannot ostensibly validate a refusal to disclose recognized documentation, such apprehensions are *ipso facto* and incontrovertibly deficient to legitimize a comprehensive institutional refusal to conduct a mandatory search (i.e. the refusal to search) *in limine*.
100. Furthermore, the *McInerney Decision* recognized the paradoxical reality that the outright denial of access is demonstrably calculated to incentivize the very commencement of litigation it purportedly seeks to avoid. As noted by the Supreme Court of Canada, when an entity refuses disclosure, the aggrieved party is inevitably compelled to commence an action to acquire the requisite records via the rules of civil procedure governing documentary discovery. Applied *mutatis mutandis* to the present factual matrix, the absolute failure of the Royal Canadian Mounted Police to conduct a requisite search of the offline historical database (the “**Offline Historical Database**”) precipitates an identical outcome: the applicant (the “**Applicant**”) is forcibly conscripted into initiating these exact judicial review proceedings, culminating in the pursuit of the prerogative writ of mandamus, to effectuate the compulsory search that ought to have been executed *prima facie*.
101. In direct application of the aforementioned jurisprudence to the uncontroverted evidentiary matrix herein, the Royal Canadian Mounted Police has purportedly refused to search the foundational metadata (the “**Foundational Metadata**”) under the guise that such efforts might yield information over which they disclaim authority or which they baselessly deem extraneous. However, the *McInerney Decision* categorically invalidates the argument that records may be withheld merely because they are perceived as meaningless or subject to misinterpretation. If the documentation housed within the Canadian Police Information Centre (the “**CPIC**”) is genuinely unblemished, its revelation would precipitate no prejudice; conversely, the persistent refusal to search strongly substantiates the adverse inference that said repositories contain indisputable proof of systemic fabrication. The utilized software mechanism, identified as GrapeCity.Documents.For.PDF (version 6.0.2.0), manufactured an ostensibly authoritative instrument that is inextricably devoid of jurisdictional competence, thereby constituting an absolute nullity *ab initio* rather than a curable procedural irregularity, as it was forged in direct contravention of the *Criminal Code*, and immutable equitable principles. Consequently, the institutional posture of the Royal Canadian Mounted Police—characterized by an *ultra vires* refusal to interrogate the hexadecimal dumps and audit trails—is diametrically opposed to the equitable duties of disclosure affirmed in the *McInerney Decision*. By failing to restore the *status quo ante*, the respondents (the “**Respondents**”) have abdicated their positive statutory obligations, utilizing administrative reticence as a clandestine mechanism to perpetuate the concealment of a juridical nullity. It is therefore respectfully advanced that the judicial intervention of this Honourable Court is strictly necessitated to vitiate this obstinate recalcitrance and compel the execution of a comprehensive search, thereby ensuring that the foundational tenets of transparency and the rule of law are unequivocally upheld.
102. In order for the Applicant to be able to exercise his right to request correction, the RCMP must discharge its duty to search at first instance.

I. THE FABRICATED “INFORMATION PACKAGE” IS AN ABSOLUTE NULLITY

103. The Application Record demonstrates that the Information Package:
- 832**
- a. is missing mandatory pages;
 - b. contains no judicial signature (ink; electronic; or “digital signature” although it purports to have been digitally signed by JP Mr. George Jiri of OCJ Brampton in a Toronto Region matter (on its best day), which is unlawful in of itself and, on its face (pardon the pun), would have been impossible considering the full implementation of the Criminal E-Intake Portal in 2022 province wide for the OCJ
 - c. contains inconsistent footers;
 - d. contains digital artifacts (“CL (M)”) which on their face and by lack of controverted evidence or the single appearance by a single Respondent including the failure of the Regional COM of the entire Central Region (formerly the “O” Region” for Ontario) in Regional COM Mr. Matt Peggs (not to be confused with former Fire Commissioner in Mr. Matthew Pegg (nota bene: no “s”); and
 - e. was generated using **GrapeCity.Documents for PDF v. 6.0.2.0**, a commercial SDK external to ICON/FRANK.
104. These anomalies are not “irregularities.” They are **jurisdictional defects** that render the document an **absolute nullity**. A fabricated Information Package cannot:
- a. authorize an arrest;
 - b. be the grounds to lure an individual to a police division that it has received some of the individual’s property only with the motive to falsely arrest him, detain him, imprison him with the threat of indefinite imprisonment at another detention centre;
 - c. support a CPIC entry ab initio or post facto by falsification;
 - d. justify a deprivation of liberty; and
 - e. be relied upon by law enforcement.
105. Only a Level 3 search can determine the genesis and modification history of the document. The RCMP’s refusal to conduct such a search is unreasonable and contrary to law.

PART IV — RELIEF SOUGHT

106. It is imperative, with respect, to recall what is in the Record Of Proceeding by way of Tab 12 in the Applicant’s Rule 317 Request (see: page 457 and onwards). By way of summary and recasting with current temporal relevant, the jurisprudential and administrative determinations promulgated by the Office of the Privacy Commissioner of Canada (the “OPCC”) establish an irrevocable and binding paradigm: the Royal Canadian Mounted Police (the “RCMP”) is strictly precluded from operating as a passive repository or “blind conduit” concerning the proliferation of intelligence contributed by external municipal or provincial law enforcement apparatuses. As the supreme technological administrator and absolute statutory steward of the Canadian Police Information Centre (the “CPIC”) infrastructure, the RCMP exercises paramount, non-delegable control over all multi-jurisdictional entries. Consequently, it is an irrefragable syllogism that the RCMP is encumbered with the ultimate legal responsibility to actively govern, monitor, and ensure that all proprietary data transiting this national framework strictly comports with the rigid parameters of the *Privacy Act*. Invoking the foundational equitable and legal maxims *qui facit per alium facit per se* and *qui non prohibet quod prohibere potest assentire videtur*, the recalcitrant refusal to conduct a mandatory search of the foundational metadata (the “Foundational Metadata”) and

the Offline Historical Database constitutes a direct contravention of statutory obligations. The OPCC has explicitly included that the quantum of control exercised by the RCMP over the CPIC mainframe is unequivocally sufficient to trigger the robust, mandatory protections enshrined within section 8 of the *Privacy Act*. Even in circumstances wherein an ancillary municipal entity ostensibly originated the data upload and maintained nominal carriage of a localized investigative file, the Commissioner of the RCMP remains the ultimate authority accountable for the administration and statutory compliance of the overarching system. Therefore, the attempt by the RCMP to shield itself behind the facade of a decentralized framework to evade an affirmative duty to search is fundamentally *ultra vires*.

107. This absolute architectural stewardship inextricably equates to absolute legal accountability, particularly when confronted with the insidious integration of fabricated or fundamentally inaccurate data. Given the evidentiary record demonstrating the presence of unparalleled subfacial and facial fabrications—amounting to absolute nullities *ab initio* rather than mere curable procedural irregularities—the RCMP is legally bound to exercise an active, governing supremacy over the implicated files. In relation to said implicated files, wherein the personal information (the “Personal Information”) of the applicant (the “Applicant”) is inextricably intertwined, an immutable and infeasible statutory entitlement to said data is possessed by the Applicant. Drawing from binding federal public sector jurisprudence, the taxonomy of what constitutes the Personal Information mandates a profoundly broad and expansive interpretative framework; it encompasses information that is strictly “about” an identifiable individual, signifying that the data not only subjects the individual but substantively relates to or concerns them, as authoritatively articulated in *Dagg v. Canada (Minister of Finance)*, [\[1997\] 2 SCR 403](#), *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, [2006 FCA 157](#), and *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003 SCC 8](#).
108. Furthermore, it is a settled doctrine that a serious possibility of an individual being identified through the utilization of said information, either in isolation or synthesized with external data matrices, strictly satisfies the threshold of an “identifiable individual,” a principle confirmed in *Gordon v. Canada (Health)*, [2008 FC 258](#). The classification transcends mere recorded typologies; the essential nature of information concerning an identifiable subject operates to solidify its status as the Personal Information, irrespective of its physical or unrecorded embodiment, as supported by *Morgan v. Alta Flights Inc.*, [2006 FCA 121](#). The jurisprudential parameters remain utterly undiminished even if the intelligence is shared among multiple identifiable subjects, as established in *Wyndowe v. Rousseau*, [2008 FCA 39](#), or if the data ostensibly exists within the public domain, as affirmed in *Englander v. TELUS Communications Inc.*, [2004 FCA 387](#). Of paramount significance to the present matrix of fabricated instruments, subjective or fundamentally inaccurate intelligence ascribed to an individual unequivocally retains its strict classification as the Personal Information, a doctrine firmly cemented in *Lawson v. Accusearch Inc.*, [2007 FC 125](#).

109. The systemic subversion effectuated through the illicit utilization of Portable Document Format manipulation software demands uncompromising forensic verification via the compulsory disclosure of the requested hexadecimal transaction logs and sequential digital trails. The failure to actively restrict, audit, and expose such unlawful data manipulation renders the RCMP directly culpable for the resultant privacy breaches, thereby entirely destroying any residual presumption of *omnia praesumuntur rite esse acta*. *Ipso facto*, the present application for judicial review is correctly and inescapably predicated upon the egregious dereliction of the RCMP in failing to conduct the requisite search. To achieve compliance with the *Privacy Act*, the prerogative writ of *mandamus* must be issued to actively interrogate the repositories under the sovereign and constructive control of the centralized federal repository. Consequently, immediate judicial intervention *in limine* is strictly necessitated to compel the execution of a comprehensive, multi-level search, thereby restoring the *status quo ante* and ensuring that the foundational tenets of transparency, statutory adherence, and the rule of law are unequivocally upheld.

110. The Applicant seeks the following relief, flowing directly from the Respondents' refusal to search, refusal to exercise statutory discretion, failure to produce a Certified Tribunal Record, and failure to participate in this proceeding. The Applicant seeks all relief set out in this Notice of Application, including but not limited to:

- a. A declaration that the RCMP Tribunal has lost jurisdiction over file 2025-16999 [sic] and the Applicant's two ATIA requests to the RCMP ATIP Branch (Request #1 delivered April 14, 2026, and Request #2 delivered May 7, 2026; Application Record, Tabs 9 and 10). This relief is subject to the passage of time, the date of the judgment hearing, and leave to make further submissions (including seeking directions and enforcement of orders);
- b. The declaratory relief detailed at subparagraphs 1(k) through 1(p), 1(r) through 1(t), 1(v), 1(w), and 1(y) through 1(hh);
- c. The orders detailed at subparagraphs 1(x) and 1(ii); and
- d. Any other relief not expressly encompassed above;
- a. A declaration that the RCMP breached its statutory obligations under ss. 4, 6, and 12 of the *Privacy Act* by:
 - a. refusing to conduct any search for the Applicant's Personal Information;
 - b. refusing to search foundational metadata (Level 2), including ORI, terminal ID, system identification number, and PPU 005 logs;
 - c. refusing to search amended or purged data (Level 3), including hexadecimal dumps, offline mainframe interrogation, audit trails, and version histories; and
 - d. refusing to take any steps reasonably necessary to identify, locate, or retrieve Personal Information under its control;
- c. An order in the nature of *mandamus* compelling the RCMP to conduct a full, complete, and good-faith search for all Personal Information responsive to the Applicant's March 11, 2026 request, specifically including:
 - a. Level 2 (Foundational Metadata): ORI (Originating Agency Identifier), terminal ID, system identification number, PPU 005 transaction logs, and all metadata identifying the genesis, custody, or modification history of Police Case ID 457197; and
 - b. Level 3 (Amended or Purged Data): hexadecimal dumps, offline mainframe interrogation results, audit trails, version histories, records showing overwritten/deleted/purged entries, and any indicators of synthetic document generation or "vector collapse";
- d. An order in the nature of *mandamus* compelling the Head of the RCMP, Commissioner Michael Duheme, to:
 - a. exercise his statutory discretion under s. 8(2)(m) of the *Privacy Act*;
 - b. consider whether the public interest in disclosure clearly outweighs any invasion of privacy, and whether disclosure would benefit the Applicant;
 - c. review the Applicant's April 7, 2026 request; and
 - d. provide written reasons documenting this analysis. (*Note: This relief compels the lawful consideration of disclosure, not the disclosure itself*).
- e. A declaration that the RCMP's refusal to search:
 - a. is incorrect and unreasonable;
 - b. frustrates the purpose of the *Privacy Act* and the ATIA;
 - c. violates the Applicant's right of access under s. 12(1);
 - d. violates the duty to maintain accurate and complete records under s. 6; and
 - e. violates the duty to collect and retain information lawfully under s. 4.

- f. An order requiring the RCMP to file, within a time fixed by the Court, a sworn Affidavit of Compliance setting out: a. the repositories searched and methods used; b. the specific metadata and amended/purged data retrieved; c. the results of all Level 2 and Level 3 searches, including the Applicant's located Personal Information; and d. any records confirmed to have been altered, overwritten, or purged;
- g. An order in the nature of *prohibition* enjoining the RCMP, its delegates, and affiliated bodies from expunging, altering, transferring, sanitizing, migrating, obfuscating, or archiving beyond rapid retrieval any metadata, system logs, or historical audit trails associated with Police Case ID 457197 pending final adjudication and exhaustion of appeals;
- h. An order that the Court remain seized of this matter to oversee compliance with the Orders herein, to address the RCMP's loss of jurisdiction, and to address any subsequent issues arising from the Respondents' execution of these directives;
- i. An order granting immediate interim injunctive relief pending final disposition of this Application;
- j. An order granting permanent injunctive relief to abate ongoing statutory breaches
- k. Such costs as this Honourable Court deems just, including elevated or full indemnity costs if warranted by the Respondents' default and refusal to perform statutory duties; and
- l. Such further and other relief as this Honourable Court deems just and necessary to give full effect to its judgment.

All of which is most respectfully submitted to this Honourable Federal Court of Canada by the Applicant on below date:

Date: June 3, 2026



Mr. Kevin A. McLean (BA, JD, CIM)
Applicant (Self-Represented)
68 Abell Street
(Receptionist desk)
Toronto, Ontario
M6J 0B1
Email: mclean@searchandseizure.ca
Fax: 416.352.0055

PART V — LIST OF AUTHORITIES

(Rule 70(1)(e), *Federal Courts Rules*)

A. Statutes and Regulations

1. ***Federal Courts Act***, RSC 1985, c F-7
2. ***Federal Courts Rules***, SOR/98-106
3. ***Privacy Act***, RSC 1985, c P-21
4. ***Access to Information Act***, RSC 1985, c A-1
5. ***Canadian Charter of Rights and Freedoms***, Part I of the Constitution Act, 1982
6. ***Criminal Code***, RSC 1985, c C-46

*B. Jurisprudence**Supreme Court of Canada*

7. *Lavigne v Canada (Commissioner of Official Languages)*, 2002 SCC 53
8. *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403
9. *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25

2. Federal Court of Appeal / Federal Court

17. *Apotex Inc v Canada (Attorney General)*, [1994] 1 FC 742 (CA)
18. *Dagg v. Canada (Minister of Finance)*, [1997] 2 SCR 403,
19. *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, and
20. *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8.
21. *Morgan v. Alta Flights Inc.*, 2006 FCA 121.
22. *Wyndowe v. Rousseau*, 2008 FCA 39,
23. *Englander v. TELUS Communications Inc.*, 2004 FCA 387. 7

3. Provincial Appellate and Superior Courts

25. *Ontario Criminal Code Review Board v Hale*, [1999 CanLII 3805](#) (ONCA)

C. Secondary Materials

26. Treasury Board Secretariat, Personal Information Banks — RCMP PPU 005

27. GrapeCity.Documents for PDF, Developer Documentation (Version 6.0.2.0)

28. OPC Special Investigation Report (2014) — Mental Health Disclosures to U.S. CBP

ⁱ “[4] To substantiate the gravity of subfacial and facial fabrications, reliance is placed upon *R. v. Schertzer*, 2015 ONCA 259 (the “Schertzer Decision”), and *R. v. Hansen*, 2018 ONCA 46 (the “Hansen Decision”). These appellate authorities adjudicated instances of subfacial fabrication, wherein ostensibly valid judicial authorizations were rendered constitutionally defective due to underlying prevarications promulgated by law enforcement officials regarding the scope of their investigations and the purported existence of reasonable grounds to believe (the “Reasonable Grounds To Believe”).

[5] The Schertzer Decision involved the falsification of police notes designed to conceal an unlawful search, whereas the Hansen Decision addressed the invalidation of search warrants predicated upon misleading information sworn by affiants. Applying the legal principles elucidated therein to the present factual matrix, it is evident that the actions deployed against the Applicant transcend mere subfacial deficiencies; they constitute overt, absolute fabrications of judicial processes ab initio.

[6] A comparative analysis necessitates an examination of *Silva v. R.*, 2021 QCCS 4627, and *Silva v. R.*, 2021 QCCS 4131 (collectively, the “*R. v. Silva Decisions*”). The factual matrix therein involved an officer of the Service de Police de la Ville de Montréal (the “SPVM”), Officer Guillaume Joly-Tessier, who temporarily misappropriated a judicial stamp belonging to a Justice of the Peace to forge an arrest warrant. The target of said fabrication was a highly dangerous, convicted fugitive possessing a documented history of severe, violent criminality, including armed robbery and murder. While the misconduct elucidated in the “*R. v. Silva Decisions*” was undeniably deplorable, it was rationalized internally as a manifestation of noble-cause corruption, undertaken in extremis to apprehend a significant threat to public safety.

[7] Conversely, the circumstances surrounding the Applicant, an individual devoid of any criminal antecedents but for the soundly defeating of the RCMP and former RCMP officers while retained by the soon to be defunct LSBC, stand in stark contrast to the preceding authorities. The fabrication of the Criminal Code Form 2 Information (the “Form Two Information”) within the False Information Package involved the installation of a Toronto Region Court Officer, Mrs. Frugoni-Rojas, as a fabricated informant (the “Fictitious Informant”). Furthermore, the process ostensibly engaged a fictitious Justice of the Peace, Mr. George Jiri, improperly ascribed to the Ontario Court of Justice Brampton Courthouse (the “Brampton Courthouse”). The Applicant maintained no residential or jurisdictional nexus to the Brampton Courthouse. Geographically and jurisdictionally, the Royal Canadian Mounted Police Milton Detachment (the “RCMP Milton Detachment”) operated with proximity and oversight regarding specific federal matters within Toronto West. Simply put, unprecedented fraud on two levels of court involving a fictitious informant and fictitious judicial officer. More colourfully put, Mr. Jeff Ball, Director, Privacy, of the RCMP ATIB Branch has the audacity to represent that he cannot search the Foundational Metadata Repository and Offline Historical Database Repository. The Applicant pleads that the RCMP ATIB Branch must search but it does not want to search for fear of what it will discover.”

(see: Tab 11, pages 425 and 426).

ⁱⁱ Put another way, without the RCMP (ATIP Branch) conducting a search under the PII Access Request (March 11 2026) (and presumably by the time of the “Hearing” (not by conference as that would not be legally possible based on the most expeditiousness under which the Applicant is marshalling this FCC Application forward, then the Head of the **Institution**(Commissioner Mr. Micheal Duheme) cannot exercise a discretion, as fettered as it may be and still subject to the relief of a writ of mandamus, under ss. 8(2)(m). It is trite that this FCC Application raises at the very least general issues which are of central importance to the legal system as a whole.

TAB 24

FEDERAL COURT

BETWEEN:

KEVIN A. McLEAN

Applicant

and

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, and STEPHANE
BRISSON

Respondents

REASONS FOR ORDER or REASONS FOR
JUDGMENT with ORDER at Appendix A

(Issued concurrently with the Order dated _____, 2026)

Table of Contents

Court File No. T-2448-26 1

FEDERAL COURT 1

REASONS FOR ORDER 1

 I. INTRODUCTION 5

 II. PROCEDURAL HISTORY 5

 A. Service of the Notice of Application and Rule 317 Request 5

 B. Failure to Transmit the Certified Tribunal Record 5

 C. Motion in Writing (NOM #1) 6

 D. Requisition for Hearing (Form 314) 6

 E. Supplemental Application Record (June 22, 2026) 6

II. FACTUAL BACKGROUND	6
839 Privacy Act Request (March 11, 2026)	6
B. ATIA Request #1 (April 14, 2026)	7
C. ATIA Request #2 (May 7, 2026)	8
D. The False Information Package	8
E. The Tripartite Contradiction	9
(1) Privacy Act Request	9
(2) ATIA Request #1	9
(3) ATIA Request #2	9
REASONS FOR ORDER — PART III	10
III. ISSUES	10
Issue 1 — Whether the RCMP breached its statutory duty to conduct a reasonable search under the Privacy Act	10
Issue 2 — Whether the RCMP breached its duty to assist and duty to make every reasonable effort to locate records	10
Issue 3 — Whether the RCMP Commissioner failed to exercise his mandatory statutory discretion under s. 8(2)(m) of the Privacy Act	11
Issue 4 — Whether the RCMP’s failure to comply with Rule 318 constitutes a breach of procedural duty warranting judicial intervention	11
Issue 5 — Whether the RCMP’s contradictory positions across the Privacy Act Request, ATIA #1, and ATIA #2 constitute evidence of bad faith, procedural unfairness, or jurisdictional error	11
Issue 6 — Whether the Applicant is entitled to prerogative relief in the nature of mandamus	12
Issue 7 — Whether the Applicant is entitled to prerogative relief in the nature of prohibition	12
Issue 8 — Whether the Applicant is entitled to declaratory relief	12
Issue 9 — Whether the Court should remain seized to supervise compliance	12
Issue 10 — Whether solicitor-client costs are warranted	13
REASONS FOR ORDER — PART IV	13
IV. ANALYSIS	13
Segment 1 — The Duty to Search Under the Privacy Act	13
A. The Statutory Framework	13
B. The RCMP’s “Live Query” Was Not a Search	14
C. The RCMP’s Assertion That It “Cannot Search Files Belonging to Other Police Forces” Is Incorrect in Law	14
(1) The jurisprudence on “control”	14
(2) The Applicant did not request municipal records	15
(3) The RCMP’s own ATIA #1 admission contradicts its Privacy Act position	15
D. The RCMP’s Refusal to Search Constitutes a Reviewable Error	15
E. The Tripartite Contradiction Reinforces the Finding of a Breach	16
REASONS FOR ORDER — PART IV	16

Segment 2 — Duty to Assist & Duty to Make Reasonable Efforts	16
840 Duty to Assist Under the ATIA and Privacy Act.....	17
B. The RCMP’s Contradictory Positions Demonstrate a Breach of the Duty to Assist	17
C. The RCMP’s “Unable to Locate” Notice Is a Breach of the Duty to Assist.....	18
D. The RCMP’s “Retrieval Stage” Admission Confirms a Breach of the Duty to Assist	18
E. The Duty to Assist Requires Technological Competence	19
F. The General Principle of the Federal Courts Rules and the Extraordinary Importance of the Issues.....	19
PART IV — ANALYSIS, Segment 3 (Commissioner’s s. 8(2)(m) Failure) → AFTER that section → a new dedicated subsection:	Error! Bookmark not defined.
“G. Abuse of Process, Inconsistent Positions, and the Binding Nature of Formal Admissions”	Error! Bookmark not defined.
PART IV — ANALYSIS	Error! Bookmark not defined.
Segment 3 (continued).....	Error! Bookmark not defined.
G. Abuse of Process, Inconsistent Positions, and the Binding Nature of Formal Admissions	20
H. Abuse of Process: The RCMP’s Irreconcilable Positions Cannot Stand	21
I. Abuse of Process Applies Even Without a Notice of Appearance.....	21
J. The RCMP Cannot Now Take Any Contrary Position	22
K. Conclusion on Abuse of Process and Admissions	22
REASONS FOR ORDER — PART IV	23
Segment 4 — Rule 318 Breach & Mandamus Test.....	23
A. The Mandatory Nature of Rule 318.....	23
B. Silence Is Not a Lawful Response Under Rule 318.....	23
C. Rule 318 Applies Regardless of Whether the Respondents Filed a Notice of Appearance	24
D. The RCMP’s Written Admissions Confirm the Breach	24
E. The Legal Test for Mandamus	25
F. Application of the Mandamus Test	25
(1) Public legal duty to act	25
(2) Duty owed to the Applicant	25
(3) Clear right to performance.....	25
(4) No adequate alternative remedy	25
(5) Prior demand	26
(6) Refusal	26
G. Mandamus Must Issue.....	26
H. The Court’s Supervisory Jurisdiction Requires Intervention	26
I. Mandamus Must Be Coupled With a Strict Timeline.....	26
J. Conclusion on Rule 318 and Mandamus.....	27
REASONS FOR ORDER — PART IV	27
Segment 5 — Prohibition & Preservation of Metadata (Spoliation Risk)	27

841	A. The Legal Framework for Prohibition	27
	B. The RCMP's Conduct Creates a Real and Substantial Risk of Spoliation	27
	C. The RCMP's Jurisdiction Over the Metadata Is Established	28
	D. The Legal Test for Prohibition Is Satisfied	29
	(1) The RCMP has acted without jurisdiction	29
	(2) The RCMP is about to act in excess of jurisdiction	29
	(3) The risk of irreparable harm is established	29
	(4) No adequate alternative remedy exists	29
	(5) The Court's supervisory jurisdiction is engaged	29
	E. The RCMP's Conduct Demonstrates a Need for Prohibition	29
	F. Prohibition Must Issue to Prevent Spoliation	30
	G. The Court Must Remain Seized to Ensure Compliance	31
	H. Conclusion on Prohibition	31
	PART IV — ANALYSIS	31
	Segment 6 (Expanded) — Declaratory Relief, Elevated Costs, and Final Disposition	31
	B. The RCMP's Conduct Warrants Elevated, Full Indemnity Costs	31
	1. The Legal Standard for Elevated Costs	31
	2. The RCMP's Conduct Meets the Elevated Costs Threshold	32
	Vector 1 — Systemic Bad Faith	32
	Vector 2 — Total Statutory Delinquency	32
	Vector 3 — Compounding ATIA Breaches and a Coordinated Institutional Obstruction	33
	3. The Applicant's Work Was Necessary, Proportionate, and Caused Solely by the RCMP's Conduct	34
	4. Tariff B Is Manifestly Inadequate	34
	5. Full Indemnity Costs Are Required to Uphold the Rule of Law	34
	6. Lump-Sum Award	35
	REASONS FOR ORDER — PART V	35
	V. CONCLUSION	35
	APPENDIX A — ORDER	37
	ORDER	37
	A. DECLARATIONS	37
	B. MANDAMUS	38
	C. PROHIBITION & PRESERVATION OF EVIDENCE	38
	D. COSTS	38
	E. COURT REMAINS SEIZED	38

I. INTRODUCTION

[1] This judicial review concerns a series of profound statutory, procedural, and institutional failures by the Royal Canadian Mounted Police (“RCMP”) in its capacity as a federal institution under the *Privacy Act*, RSC 1985, c P-21, and the *Access to Information Act*, RSC 1985, c A-1 (“ATIA”), and as a “tribunal” within the meaning of Rule 2 of the *Federal Courts Rules* and s. 2(1) of the *Federal Courts Act*.

[2] The Applicant seeks declaratory relief, prerogative remedies in the nature of mandamus and prohibition, and solicitor-client costs. He also seeks enforcement of his Rule 317 Request and compliance with Rule 318, which requires a tribunal to transmit the Certified Tribunal Record (“CTR”) within 20 days of service.

[3] The Respondents were duly served with the Notice of Application and the Rule 317 Request on May 19, 2026. They did not file a Notice of Appearance within the 10-day period mandated by Rule 305. They filed no affidavits, no submissions, and no objections under Rule 318(2). They have therefore elected not to participate in this proceeding.

[4] The absence of a Notice of Appearance does not deprive the Court of jurisdiction to adjudicate the matter. It does, however, mean that the Respondents are not entitled to notice of further steps and that the evidentiary record consists exclusively of the Applicant’s materials.

[5] The issues raised are of broader systemic importance. They concern the integrity of federal access-to-information regimes, the mandatory nature of statutory search obligations, the personal duty of the head of an institution under s. 8(2)(m) of the *Privacy Act*, and the consequences of a tribunal’s failure to comply with Rule 318.

[6] The record also reveals a troubling pattern of contradictory institutional positions taken by the RCMP across three parallel access requests — one under the *Privacy Act* and two under the ATIA — which cannot logically or legally coexist. These contradictions bear directly on the statutory duties at issue and the appropriateness of the extraordinary relief sought.

II. PROCEDURAL HISTORY

A. Service of the Notice of Application and Rule 317 Request

[7] The Applicant served the Notice of Application (Form 301) and the Rule 317 Request on May 19, 2026. The Respondents were required to file a Notice of Appearance within 10 days under Rule 305(1). They did not do so.

[8] Under Rule 305(2), a respondent who fails to file a Notice of Appearance is not entitled to notice of any further step in the proceeding. The Applicant was therefore entitled to proceed ex parte.

B. Failure to Transmit the Certified Tribunal Record

[9] The Rule 317 Request triggered the mandatory obligation under Rule 318(1) to transmit the CTR within 20 days. The deadline expired on June 10, 2026.

[10] The RCMP did not transmit the CTR. It did not file a written objection under Rule 318(2). It did not communicate with the Court or the Applicant. The failure is absolute.

C. Motion in Writing (NOM #1)

843

[11] On June 10, 2026, the Applicant filed a Notice of Motion seeking an order compelling compliance with Rule 318. The Motion Record was filed on June 11, 2026. The Respondents did not oppose the motion.

[12] The motion proceeded in writing on June 17, 2026. No Respondent filed any materials.

D. Requisition for Hearing (Form 314)

[13] The Applicant filed a Requisition for Hearing on June 12, 2026, and again on June 19, 2026, after making minor amendments to ensure strict compliance with Rule 314.

[14] The Registry initially declined to accept the requisition, citing the general flowchart for judicial review applications. The Applicant responded, correctly noting that:

- the Respondents' failure to file a Notice of Appearance extinguished their procedural rights;
- the time for filing a respondent's record never arose;
- Rule 314(1) therefore required the requisition to be filed within 10 days after the expiration of the time for the respondent's record — which, in a default scenario, is immediate.

[15] The Applicant's position is consistent with the text and structure of the Rules.

E. Supplemental Application Record (June 22, 2026)

[16] On June 22, 2026, the Applicant filed a Supplemental Application Record containing:

- fresh evidence of contradictory RCMP ATIP positions;
- the June 16, 2026 "retrieval stage" admission;
- the June 18, 2026 "unable to locate" notice;
- the Applicant's Research Dossier analyzing the tripartite contradiction;
- additional correspondence with the Registry.

[17] These materials are admissible and relevant to the issues before the Court.

II. FACTUAL BACKGROUND

A. The Privacy Act Request (March 11, 2026)

[18] On March 11, 2026, the Applicant submitted a highly particularized request under the *Privacy Act* seeking access to his personal information contained within the Canadian Police Information Centre ("CPIC") architecture, including:

- foundational metadata (ORI codes, terminal IDs, system identifiers);
- raw CPIC Offline Historical Database entries;
- ADD/MODIFY/CLEAR/CANCEL command logs;
- hexadecimal dumps;
- amended or purged data;
- cryptographic audit trails; and

- operator-level logs.

844

[19] These categories correspond to the Personal Information Bank RCMP PPU 005 and are central to the Applicant's allegations that the "False Information Package" underlying his October 2, 2024 arrest was digitally manipulated using GrapeCity.Documents for PDF v.6.0.2.0.

[20] On April 27, 2026, the RCMP issued a three-page response that:

- did **not** search the Offline Historical Database;
- did **not** search PPU 005;
- did **not** search for amended or purged data;
- did **not** search for hexadecimal dumps;
- did **not** search for audit trails;
- did **not** search for operator logs;
- did **not** search for foundational metadata.

[21] Instead, the RCMP executed a **live CPIC query** ("Q PERS+" and "Q CNI") on April 14, 2026 — a method that, by design, cannot retrieve historical, purged, or amended records. The RCMP then asserted that the Privacy Act "does not authorize the RCMP to search files belonging to other police forces."

[22] This position is inconsistent with:

- the statutory definition of "personal information";
- the jurisprudence on "control" (Canada Post, Hale, MO-4542);
- the RCMP's role as custodian of CPIC;
- the architecture of PPU 005;
- the Applicant's explicit request for federal-level metadata.

[23] The Privacy Act response therefore constitutes a **refusal to search**, not a search that yielded no results.

B. ATIA Request #1 (April 14, 2026)

[24] On April 14, 2026, the Applicant submitted a request under the ATIA seeking:

- Investigative Data Bank audit trails;
- raw hexadecimal mainframe dumps;
- terminal metadata (ORI, MAC, IP logs);
- inter-agency communications;
- GrapeCity PDF vector anomaly logs;
- Offline Historical Database search results;
- CPIC governance manuals.

[25] These are the **same categories of records** the RCMP refused to search under the Privacy Act.

[26] On June 16, 2026, RCMP ATIP Team Leader **Tina Beaudoin** emailed the Applicant stating:

"Kindly note that no extensions were taken on your file... the file remains in the retrieval stage."

[27] This admission is legally and factually significant:

- It confirms the RCMP **can** search the Offline Historical Database.
- It confirms the RCMP **is** searching the Offline Historical Database.
- It contradicts the RCMP's Privacy Act position that such records are "unsearchable."
- It confirms the existence of the very records the RCMP refused to search for.
- It confirms the RCMP did not take a valid extension under s. 9 of the ATIA.
- It confirms the file entered a **deemed refusal** on May 14, 2026.

[28] The "retrieval stage" admission is a **binding institutional concession** that the RCMP possesses the technological capacity, jurisdictional authority, and systemic access to the records sought.

C. ATIA Request #2 (May 7, 2026)

[29] On May 7, 2026, the Applicant submitted a second ATIA request seeking:

- procurement records;
- licensing agreements;
- NTOP onboarding logs;
- Azure cloud integration logs;
- security matrices;
- lifecycle tickets

for **GrapeCity.Documents for PDF v.6.0.2.0**, the SDK whose metadata appears in the "False Information Package."

[30] On June 18, 2026, RCMP Director **Curtis Mathews** issued a notice stating:

"The RCMP is unable to locate records."

[31] This notice is defective under s. 10(1)(a) of the ATIA, which requires the institution to state:

"that the record does not exist."

[32] The phrase "unable to locate" is not a statutory ground. It is an admission of a **failed search**, not a declaration of non-existence.

[33] The defective notice triggers an **automatic deemed refusal** under s. 10(3).

[34] The notice is also contradicted by:

- the forensic metadata showing GrapeCity v.6.0.2.0 was used to generate the "False Information Package";
- the DOC-6507 vector collapse anomaly;
- the presence of GrapeCity XMP toolkits in the PDF;
- the RCMP's own "retrieval stage" admission for ATIA #1.

[35] It is not credible that a federal institution with a multi-billion-dollar budget cannot locate **any** procurement or licensing records for enterprise-level software actively used in its document-generation pipeline.

D. The False Information Package

[36] The Applicant's arrest on October 2, 2024 was executed pursuant to a "False Information Package" that:

- contains only 5 pages instead of the mandatory 6;
- omits the statutory attestation page (Page 4);
- omits the sentencing/disposition page (Page 5);
- contains no judicial signature;
- contains no digital signature;
- contains no wet signature;
- contains no valid JP authorization;
- contains inconsistent footers;
- contains metadata proving it was generated using GrapeCity.Documents for PDF v.6.0.2.0.

[37] The missing attestation page renders the Information a **nullity ab initio** under ss. 504–508 of the *Criminal Code*.

[38] The GrapeCity metadata — including the DOC-6507 vector collapse anomaly — demonstrates that the document was generated **outside** the secure ICON/FRANK judicial systems.

[39] This explains why the Applicant sought hexadecimal dumps and audit trails: only raw mainframe data can reveal the true provenance of the document.

E. The Tripartite Contradiction

[40] The Applicant’s Research Dossier identifies a **three-way institutional contradiction**:

(1) Privacy Act Request

RCMP and Respondent Mr. Ball’s position:

“We cannot search these records.”

(2) ATIA Request #1

RCMP and Ms. Beaudoin’s position:

“We are actively retrieving these records.”

(3) ATIA Request #2

RCMP and Mr. Mathew’s position:

“We are unable to locate records.”

[41] These positions cannot simultaneously be true.

[42] The contradictions demonstrate:

- inconsistent statutory interpretations;
- inconsistent technological claims;
- inconsistent representations of control;
- inconsistent representations of searchability;
- inconsistent representations of record existence;
- inconsistent representations of institutional capacity.

[43] The contradictions also demonstrate:

847

- a refusal to search under the Privacy Act;
- a defective statutory notice under the ATIA;
- a crystallized deemed refusal under both statutes;
- a breach of the duty to assist;
- a breach of the duty to search;
- a breach of the duty to exercise statutory discretion;
- a breach of Rule 318.

[44] The contradictions are central to the Court’s analysis and the appropriateness of the extraordinary relief sought.

REASONS FOR ORDER — PART III

III. ISSUES

[45] The Applicant raises a series of interrelated statutory, procedural, and institutional failures. The evidentiary record — which is entirely uncontested due to the Respondents’ failure to appear — gives rise to the following determinative issues:

Issue 1 — Whether the RCMP breached its statutory duty to conduct a reasonable search under the Privacy Act

[46] The first issue is whether the RCMP’s refusal to search the Offline Historical Database, foundational metadata repositories, amended/purged data, and hexadecimal logs constitutes a breach of its mandatory duty under ss. 12 and 14 of the *Privacy Act*.

[47] This includes consideration of:

- the RCMP’s reliance on a “live query” incapable of retrieving historical or purged data;
- the RCMP’s assertion that it cannot search “files belonging to other police forces”;
- the jurisprudence on “control” (Canada Post, Hale, MO-4542);
- the Applicant’s explicit request for federal-level metadata;
- the RCMP’s contradictory admission under ATIA #1 that the same records are in the “retrieval stage.”

Issue 2 — Whether the RCMP breached its duty to assist and duty to make every reasonable effort to locate records

[48] The second issue is whether the RCMP’s conduct — including its refusal to search, its reliance on an inadequate search method, and its contradictory positions across three access requests — constitutes a breach of the duty to assist under s. 4(2.1) of the ATIA and the equivalent principles under the *Privacy Act*.

Issue 3 — Whether the RCMP Commissioner failed to exercise his mandatory statutory discretion under s. 8(2)(m) of the Privacy Act

[49] The third issue is whether the Commissioner’s failure to respond to, acknowledge, or consider the Applicant’s April 7, 2026 request under s. 8(2)(m) constitutes a jurisdictional error.

[50] This includes whether:

- the duty under s. 8(2)(m) is personal and non-delegable;
- the Commissioner’s “away on duty” autoreply affects the statutory obligation;
- the failure to consider the request warrants mandamus.

Issue 4 — Whether the RCMP’s failure to comply with Rule 318 constitutes a breach of procedural duty warranting judicial intervention

[51] The fourth issue is whether the RCMP’s failure to transmit the Certified Tribunal Record within 20 days — and its failure to file a written objection — constitutes a breach of Rule 318 requiring the Court to compel production.

[52] This includes whether:

- Rule 318 is mandatory;
- silence is a lawful response;
- the RCMP’s default impedes the Court’s superintending jurisdiction;
- mandamus is appropriate to enforce Rule 318.

Issue 5 — Whether the RCMP’s contradictory positions across the Privacy Act Request, ATIA #1, and ATIA #2 constitute evidence of bad faith, procedural unfairness, or jurisdictional error

[53] The fifth issue concerns the Applicant’s Research Dossier and the “tripartite contradiction”:

1. Privacy Act: “We cannot search these records.”
2. ATIA #1: “We are retrieving these records.”
3. ATIA #2: “We are unable to locate records.”

[54] The Court must determine whether these contradictions:

- undermine the credibility of the RCMP’s representations;
- demonstrate a refusal to search;
- demonstrate a defective statutory notice;
- crystallize deemed refusals under both statutes;

Issue 6 — Whether the Applicant is entitled to prerogative relief in the nature of mandamus

[55] The sixth issue is whether the legal test for mandamus is satisfied, including:

- the existence of a public legal duty;
 - the Applicant’s clear right to performance;
 - the absence of an adequate alternative remedy;
 - a prior demand;
 - a refusal;
 - the absence of equitable bars.
-

Issue 7 — Whether the Applicant is entitled to prerogative relief in the nature of prohibition

[56] The seventh issue is whether the RCMP’s conduct — including its refusal to search, its contradictory positions, and the risk of spoliation — warrants an order prohibiting the deletion, alteration, or archiving of relevant metadata, logs, and audit trails.

Issue 8 — Whether the Applicant is entitled to declaratory relief

[57] The eighth issue is whether the Applicant is entitled to declarations concerning:

- the RCMP’s loss of jurisdiction;
 - the defective statutory notice under s. 10(1)(a) of the ATIA;
 - the deemed refusals under s. 10(3);
 - the RCMP’s contradictory positions;
 - the existence and searchability of the requested records;
 - the structural defects in the “False Information Package.”
-

Issue 9 — Whether the Court should remain seized to supervise compliance

[58] The ninth issue is whether, given the Respondents’ procedural default and the nature of the relief ordered, the Court should remain seized to supervise compliance with its orders.

Issue 10 — Whether solicitor-client costs are warranted

850

[59] The final issue is whether the Respondents' conduct — including:

- failure to appear;
- failure to comply with Rule 318;
- failure to discharge statutory duties;
- contradictory institutional positions;
- defective statutory notices;
- crystallized deemed refusals —

warrants an award of solicitor-client costs.

REASONS FOR ORDER — PART IV

IV. ANALYSIS

Segment 1 — The Duty to Search Under the Privacy Act

A. The Statutory Framework

[60] The *Privacy Act* imposes a mandatory duty on federal institutions to conduct a reasonable search for personal information responsive to a request. Section 12(1) grants individuals the right to access their personal information, and s. 14 requires the head of the institution to respond within 30 days unless a valid extension is taken.

[61] The jurisprudence is unequivocal: a federal institution must make **every reasonable effort** to identify and locate responsive records. A refusal to search is a reviewable error. A search that is superficial, incomplete, or technologically inadequate is also a reviewable error.

[62] The duty to search is not satisfied by a cursory or methodologically defective inquiry. It requires a search that is:

- **thorough;**
- **technically competent;**
- **directed to the repositories where responsive records are likely to be found;**
- **conducted by personnel with the requisite access and expertise; and**
- **responsive to the specific parameters articulated by the requester.**

851
[63] The Applicant’s request was not vague. It was not broad. It was not ambiguous. It was surgical, precise, and technically specific. It identified:

- the exact Personal Information Bank (PPU 005);
- the exact repositories (Offline Historical Database);
- the exact metadata fields (ORI, terminal ID, system ID);
- the exact transaction types (ADD/MODIFY/CLEAR/CANCEL);
- the exact forensic artifacts (hexadecimal dumps);
- the exact temporal window (Sept. 15–Dec. 31, 2024).

[64] The RCMP was therefore required to search these repositories. It did not.

B. The RCMP’s “Live Query” Was Not a Search

[65] The RCMP’s April 27, 2026 response relied exclusively on a **live CPIC query** (“Q PERS+” and “Q CN1”) executed on April 14, 2026.

[66] A live query searches only the **active, front-facing GUI** of CPIC. It does not — and cannot — retrieve:

- historical records;
- purged records;
- amended records;
- cancelled warrants;
- audit trails;
- hexadecimal logs;
- Offline Historical Database entries;
- PPU 005 metadata.

[67] The RCMP’s reliance on a live query is therefore **not a search** within the meaning of the *Privacy Act*. It is the functional equivalent of searching the surface of a database while refusing to interrogate the underlying mainframe.

[68] The Applicant expressly requested the **offline** repositories. The RCMP refused to search them.

C. The RCMP’s Assertion That It “Cannot Search Files Belonging to Other Police Forces” Is Incorrect in Law

[69] The RCMP asserted that the Privacy Act “does not authorize the RCMP to search files belonging to other police forces.”

[70] This position is legally incorrect.

(1) The jurisprudence on “control”

[71] The Federal Court of Appeal in *Canada Post Corp. v. Canada (Minister of Public Works)* held that “control” is broad, liberal, and purposive. It includes:

- 852**
- de facto control;
 - de jure control;
 - constructive control;
 - the ability to demand records;
 - the ability to retrieve records;
 - the ability to access records stored in a shared or federated system.

[72] The Ontario Court of Appeal in *Hale* applied this principle to tribunal records.

[73] The Information and Privacy Commissioner of Ontario in Order MO-4542 applied this principle **directly to CPIC**, holding that:

Municipal police services do not control CPIC audit trails, routing logs, or offline metadata.

Control rests exclusively with the RCMP as the federal host.

[74] The RCMP therefore **cannot** disclaim control over CPIC metadata by invoking “originator control.”

(2) The Applicant did not request municipal records

[75] The Applicant did not request:

- Toronto Police Service files;
- municipal investigative files;
- provincial court files.

[76] He requested **federal-level metadata** stored in **federal repositories** controlled by the RCMP.

(3) The RCMP’s own ATIA #1 admission contradicts its Privacy Act position

[77] On June 16, 2026, the RCMP admitted that the same records were in the “**retrieval stage**” under ATIA #1.

[78] This admission is incompatible with the RCMP’s Privacy Act position that the records are “unsearchable.”

D. The RCMP’s Refusal to Search Constitutes a Reviewable Error

[79] The RCMP did not search:

- the Offline Historical Database;
- PPU 005;
- amended/purged data;
- hexadecimal logs;
- audit trails;
- operator logs;
- foundational metadata.

[80] It relied on a methodologically defective “live query.”

[81] It asserted a legally incorrect jurisdictional limitation.

853
[82] It ignored the Applicant's explicit parameters.

[83] It contradicted its own ATIA #1 admission.

[84] It failed to discharge its statutory duty.

[85] The refusal to search is therefore:

- **incorrect;**
 - **unreasonable;**
 - **procedurally unfair;**
 - **contrary to the purpose of the Privacy Act;**
 - **a breach of the duty to assist;**
 - **a jurisdictional error.**
-

E. The Tripartite Contradiction Reinforces the Finding of a Breach

[86] The RCMP's three contradictory positions — refusal to search (Privacy Act), retrieval stage (ATIA #1), and unable to locate (ATIA #2) — reinforce the conclusion that the Privacy Act search was not conducted.

[87] These contradictions demonstrate:

- inconsistent statutory interpretations;
- inconsistent technological claims;
- inconsistent representations of control;
- inconsistent representations of searchability;
- inconsistent representations of record existence.

[88] The contradictions also demonstrate:

- a refusal to search;
- a defective statutory notice;
- crystallized deemed refusals;
- a breach of the duty to assist;
- a breach of the duty to search.

[89] The Privacy Act search was not merely inadequate — it was **never conducted**.

REASONS FOR ORDER — PART IV

Segment 2 — Duty to Assist & Duty to Make Reasonable Efforts

A. The Duty to Assist Under the ATIA and Privacy Act

854

[90] Section 4(2.1) of the *Access to Information Act* imposes a mandatory “duty to assist” on federal institutions. This duty requires institutions to make **every reasonable effort** to:

- assist the requester,
- respond accurately and completely, and
- conduct a search that is adequate, good-faith, and technologically competent.

[91] Although the *Privacy Act* does not contain an identically worded provision, the Federal Court has repeatedly held that the same principles apply. The duty to assist is inherent in the statutory right of access and the right of correction under s. 12(2). A refusal to search, or a search that is methodologically defective, constitutes a breach of this duty.

[92] The RCMP’s conduct in this case falls far short of the statutory standard. The Applicant provided:

- precise repositories (PPU 005, Offline Historical Database),
- precise metadata fields (ORI, terminal ID, system ID),
- precise forensic artifacts (hexadecimal dumps),
- precise transaction types (ADD/MODIFY/CLEAR/CANCEL), and
- a precise temporal window.

[93] The RCMP ignored these parameters entirely. It did not attempt to search the repositories identified. It did not consult technical personnel capable of extracting hexadecimal logs. It did not interrogate the mainframe. It did not retrieve audit trails. It did not search amended or purged data. It did not search the Offline Historical Database.

[94] Instead, it executed a **live query** — a method incapable of retrieving the very categories of records requested — and then asserted that the Privacy Act “does not authorize” the RCMP to search files belonging to other police forces.

[95] This is not a reasonable effort. It is not an effort at all. It is a refusal to assist.

B. The RCMP’s Contradictory Positions Demonstrate a Breach of the Duty to Assist

[96] The RCMP’s contradictory positions across the three access requests — refusal to search (Privacy Act), retrieval stage (ATIA #1), and unable to locate (ATIA #2) — demonstrate a systemic failure to assist.

[97] These contradictions reveal:

- inconsistent interpretations of statutory obligations;
- inconsistent representations of technological capacity;
- inconsistent representations of record existence;
- inconsistent representations of control;
- inconsistent representations of searchability.

[98] The contradictions also reveal that the RCMP:

- did not conduct a reasonable search;

- did not make every reasonable effort;
- did not assist the Applicant;
- did not provide accurate or complete responses;
- did not comply with the statutory timelines;
- did not issue valid statutory notices.

[99] The duty to assist requires candour, diligence, and good faith. The RCMP's conduct demonstrates none of these qualities.

C. The RCMP's "Unable to Locate" Notice Is a Breach of the Duty to Assist

[100] The June 18, 2026 notice issued by Director Mathews stated that the RCMP was "unable to locate records" relating to the procurement and licensing of GrapeCity.Documents for PDF v.6.0.2.0.

[101] This notice is defective under s. 10(1)(a) of the ATIA, which requires the institution to state:

"that the record does not exist."

[102] The phrase "unable to locate" is not a statutory ground. It is an admission of a **failed search**, not a declaration of non-existence.

[103] A failed search is, by definition, a breach of the duty to assist. It indicates that the institution did not:

- search the correct repositories;
- consult the correct personnel;
- deploy the correct tools;
- interpret the request correctly;
- make every reasonable effort.

[104] The forensic metadata embedded in the "False Information Package" — including the DOC-6507 vector collapse anomaly and the GrapeCity XMP toolkits — proves that the software was used. The RCMP's inability to locate procurement records for software that leaves an indelible cryptographic footprint is not credible.

[105] The only reasonable inference is that the RCMP did not conduct a reasonable search.

D. The RCMP's "Retrieval Stage" Admission Confirms a Breach of the Duty to Assist

[106] On June 16, 2026, RCMP ATIP Team Leader Tina Beaudoin confirmed that ATIA Request #1 was in the "retrieval stage" and that **no extensions were taken**.

[107] This admission is fatal to the RCMP's Privacy Act position. It confirms that:

- the RCMP **can** search the Offline Historical Database;
- the RCMP **is** searching the Offline Historical Database;

- 856**
- the RCMP’s Privacy Act refusal to search was incorrect;
 - the RCMP’s Privacy Act refusal to search was unreasonable;
 - the RCMP’s Privacy Act refusal to search was a breach of the duty to assist.

[108] The RCMP cannot simultaneously claim that records are “unsearchable” under the Privacy Act and “in retrieval” under the ATIA.

[109] The contradiction is evidence of a systemic failure to assist.

E. The Duty to Assist Requires Technological Competence

[110] The duty to assist requires institutions to deploy the tools, personnel, and technical expertise necessary to retrieve the records requested.

[111] When an applicant requests:

- hexadecimal dumps,
- audit trails,
- amended/purged data,
- Offline Historical Database entries,
- PPU 005 metadata,
- terminal logs,
- ORI codes,
- system identifiers,

the institution must assign personnel capable of retrieving these records.

[112] The RCMP did not do so. It relied on a GUI-level query incapable of retrieving the requested records. This is a breach of the duty to assist.

F. The General Principle of the Federal Courts Rules and the Extraordinary Importance of the Issues

[113] The Court is guided by the General Principle codified in Rule 3 of the *Federal Courts Rules*, which mandates that the Rules:

“shall be interpreted and applied so as to secure the just, most expeditious and least expensive outcome of every proceeding,”

and that proportionality must be assessed “having regard to the proceeding’s complexity, the importance of the issues involved and the amount in dispute.”

[114] The issues raised in this judicial review are not merely important — they are unprecedented. The evidentiary record discloses, for the first time in any reported Canadian decision, a wholesale manipulation of a Criminal Code Form 2 Information Package (CCO-2-000-1), including:

- the apparent alteration of judicial signatures;
- the omission of mandatory statutory pages;
- the embedding of commercial PDF-generation metadata foreign to the secure ICON/FRANK judicial systems.

[115] These allegations, supported by uncontroverted forensic evidence, strike at the heart of the administration of justice in Ontario and raise systemic questions extending far beyond the Applicant’s individual circumstances.

[116] The Court cannot ignore the broader context. Recent public reporting concerning “Project South” and other investigations into document integrity within Ontario’s justice system underscores the possibility that the issues raised here may not be isolated. The Applicant’s experience — involving a falsified Information Package, contradictory federal ATIP responses, and the RCMP’s refusal to search the very repositories that would confirm or refute the authenticity of the underlying judicial instruments — raises the troubling question of whether other individuals may be similarly affected, including persons currently detained pre-trial or serving custodial sentences.

[117] The RCMP’s conduct in this proceeding, including its internally inconsistent factual assertions, contradictory statutory positions, and refusal to comply with mandatory procedural obligations under Rule 318, further amplifies the systemic significance of the matter. The RCMP bears the title “Royal,” a designation that carries with it a heightened expectation of institutional integrity, transparency, and fidelity to the rule of law. When a federal law-enforcement institution adopts mutually incompatible positions across three statutory regimes — asserting that records are “unsearchable” under the *Privacy Act*, “in retrieval” under ATIA #1, and “unable to be located” under ATIA #2 — the Court is entitled to scrutinize whether these inconsistencies reflect mere administrative error or a deeper structural problem.

[118] In these circumstances, proportionality under Rule 3 weighs heavily in favour of decisive judicial intervention. The complexity of the issues, the unprecedented nature of the alleged document manipulation, the potential systemic implications for other affected individuals, and the Respondents’ complete procedural default all support the conclusion that the extraordinary remedies sought — including mandamus, prohibition, and declaratory relief — are not only appropriate but necessary to secure a just and expeditious outcome.

G. Abuse of Process, Inconsistent Positions, and the Binding Nature of Formal Admissions

[119] Even if the Respondents had filed a Notice of Appearance — which they did not — the RCMP’s own written statements, made by senior officials in three separate statutory regimes, would bind them in this proceeding. These statements were made:

- by Director **Jeffrey Ball** under the *Privacy Act* (PII Access Request, March 11, 2026);
- by Team Leader **Tina Beaudoin** under **ATIA Request #1** (June 16, 2026 “retrieval stage” admission);
- by Director **Curtis Mathews** under **ATIA Request #2** (June 18, 2026 “unable to locate” notice).

[120] These written representations — many of them made **after** the Form 301 Judicial Review Application was filed — constitute **formal admissions**. They cannot be withdrawn, contradicted, or re-characterized without leave of the Court, which has not been sought and would not be granted in the circumstances.

[121] The law of formal admissions is well-settled. A formal admission is:

“an express and intentional waiver... a powerful instrument of speedier justice... conclusive of the matter admitted.” — *Patterson v. Scherloski*; *McWilliams Canadian Criminal Evidence*; *Sopinka, Lederman & Bryant, The Law of Evidence in Canada*

[122] A formal admission:

858

is not evidence;

- is **stronger than evidence**;
- **dispenses with the need for proof**;
- **binds the party making it**;
- **cannot be contradicted by later evidence**;
- **cannot be withdrawn without leave** (and only on strict terms).

[123] The RCMP's written statements therefore conclusively establish:

- that the Privacy Act search was not conducted;
- that the Offline Historical Database is searchable;
- that the records exist and are in "retrieval";
- that the ATIA #2 notice was defective;
- that the RCMP's positions are mutually irreconcilable.

H. Abuse of Process: The RCMP's Irreconcilable Positions Cannot Stand

[124] The doctrine of abuse of process prevents a party from advancing **diametrically inconsistent factual positions** in related proceedings. The jurisprudence is clear:

- *Toronto (City) v. CUPE, Local 79*, 2003 SCC 63 — courts have inherent power to prevent misuse of their process.
- *First Majestic Silver Corp. v. Davila Santos*, 2012 BCCA 5 — abuse of process includes inconsistent factual positions.
- *Glover v. Leakey*, 2024 BCSC — a party cannot assert contradictory facts in parallel proceedings.
- *Mystar Holdings Ltd. v. 247037 Alberta Ltd.*, 2009 ABQB 480 — irreconcilable factual positions are impermissible.
- *Pepper's Produce Ltd. v. Medallion Realty Ltd.*, 2012 BCCA 247 — inconsistent positions undermine the integrity of the court's process.
- *Halagan v. Reifel*, 1997 BCSC — "saying something to one judge and the opposite to another will not be countenanced."

[125] The RCMP's conduct falls squarely within this doctrine. It has taken **three mutually exclusive positions**:

1. **Privacy Act**: "We cannot search these records."
2. **ATIA #1**: "We are retrieving these records."
3. **ATIA #2**: "We are unable to locate records."

[126] These positions cannot coexist. They are not alternative pleadings. They are **irreconcilable factual assertions** made by the same institution concerning the same repositories, the same metadata, and the same subject matter.

[127] Under *Glover*, *Mystar*, *Pepper's Produce*, and *First Majestic*, this constitutes an abuse of process.

I. Abuse of Process Applies Even Without a Notice of Appearance

859 [128] The RCMP's failure to file a Notice of Appearance does not insulate it from the consequences of its own written admissions. Rule 305 removes the Respondents' entitlement to notice — it does not erase their prior statements.

[129] Rule 318 treats the RCMP as a **tribunal**, and the access requests under the *Privacy Act* and ATIA as **proceedings**. The RCMP's written responses in those proceedings are therefore **formal admissions** in this judicial review.

[130] The Court is entitled — indeed required — to rely on these admissions as dispositive of the issues to which they relate.

J. The RCMP Cannot Now Take Any Contrary Position

[131] The jurisprudence is unequivocal:

- A party **cannot approbate and reprobate** (*Halagan*).
- A party **cannot advance diametrically inconsistent facts** (*Mystar*).
- A party **cannot contradict its own admissions** (*Marchand*; *Azevedo*).
- A party **cannot withdraw an admission without leave** (*Patterson*; *Falco*).
- A party **cannot escape the consequences of its own statements by silence** (*Seal Tech*; *National Utility Service*).
- Even the Crown is bound by its admissions, **even if contradicted by evidence** (*R v Robertson*, 2021 SKCA 125).

[132] The RCMP has made:

- a formal admission that it refused to search;
- a formal admission that the records are in retrieval;
- a formal admission that it could not locate procurement records;
- a formal admission that no extensions were taken;
- a formal admission that the Privacy Act search was not conducted.

[133] These admissions are **binding**. They are **conclusive**. They are **dispositive**.

[134] The RCMP cannot now assert:

- that it conducted a reasonable search;
- that the records do not exist;
- that the repositories are unsearchable;
- that the ATIA notices were valid;
- that the Privacy Act response was lawful.

[135] To permit such a reversal would undermine the integrity of the Court's process and violate the principles articulated in *CUPE*, *Glover*, *Mystar*, *Pepper's Produce*, and *First Majestic*.

K. Conclusion on Abuse of Process and Admissions

[136] The RCMP's contradictory positions constitute:

- a breach of the duty to assist;
- a breach of the duty to search;
- a breach of procedural fairness;
- a breach of Rule 318;
- a crystallized deemed refusal under both statutes;
- a formal admission that the Privacy Act search was not conducted;
- an abuse of process under the jurisprudence.

[137] These findings independently justify:

- declaratory relief;
- mandamus;
- prohibition;
- solicitor-client costs;
- and the Court remaining seized with leave to the Applicant alone to tender, transmit and file further submissions arising out of the RCMP and various Respondents' delinquency.

REASONS FOR ORDER — PART IV

Segment 4 — Rule 318 Breach & Mandamus Test

A. The Mandatory Nature of Rule 318

[138] Rule 318(1) of the *Federal Courts Rules* imposes a **mandatory**, non-discretionary obligation on a tribunal to transmit the requested material within 20 days of receiving a Rule 317 request. The Rule provides:

“The tribunal **shall transmit** the material to the Registry within 20 days after being served with the request.”

[139] The use of the word “**shall**” is determinative. Under s. 11 of the *Interpretation Act*, “shall” is imperative. It removes discretion. It imposes a public legal duty.

[140] The RCMP, acting as a “tribunal” under Rule 2 and s. 2(1) of the *Federal Courts Act*, was therefore required to:

1. **transmit** the Certified Tribunal Record (CTR) within 20 days; or
2. **file a written objection** under Rule 318(2) within the same period.

[141] The RCMP did neither. It did not transmit the CTR. It did not file an objection. It did not seek an extension. It did not communicate with the Registry. It did not appear. It did not respond.

[142] The 20-day deadline expired on **June 10, 2026**. The RCMP has been in continuous breach since that date.

B. Silence Is Not a Lawful Response Under Rule 318

[143] The jurisprudence is unequivocal: a tribunal cannot ignore a Rule 317 request. Silence is not compliance. Silence is **not** an objection. Silence is not a lawful response.

861

[144] In *Rémillard v. Canada (National Revenue)*, 2020 FC 1061, the Court held that Rule 317/318 is not exploratory discovery — it is a **mandatory transmission mechanism** essential to the Court’s superintending jurisdiction.

[145] In *Lill v. Canada*, 2023 FC 1364, the Court held that where allegations of bias, procedural unfairness, or jurisdictional error are raised, the scope of the CTR expands, and the tribunal’s duty to transmit becomes even more critical.

[146] The RCMP’s refusal to transmit the CTR therefore:

- impedes the Court’s ability to conduct judicial review;
- obstructs the Applicant’s right to a fair process;
- undermines the open court principle;
- constitutes a breach of a public legal duty;
- constitutes a jurisdictional error.

C. Rule 318 Applies Regardless of Whether the Respondents Filed a Notice of Appearance

[147] Rule 305 governs the Respondents’ entitlement to notice. It does **not** govern their obligations under Rule 318.

[148] Even when a respondent is in default of appearance, Rule 318 continues to apply with full force. A tribunal cannot avoid its statutory duty by refusing to appear.

[149] The RCMP’s failure to file a Notice of Appearance therefore:

- removes their entitlement to notice;
- removes their entitlement to service;
- **does not** remove their obligation to transmit the CTR.

[150] The RCMP’s default under Rule 305 and its breach of Rule 318 are parallel, independent failures.

D. The RCMP’s Written Admissions Confirm the Breach

[151] The RCMP’s own written statements — including those of Director Ball, Team Leader Beaudoin, and Director Mathews — confirm that:

- the CTR was not transmitted;
- the CTR was not prepared;
- the CTR was not assembled;
- the CTR was not searched for;
- no objection was filed;
- no extension was sought.

[152] These statements constitute **formal admissions**, binding on the Respondents. They cannot now be contradicted.

862
[153] The breach of Rule 318 is therefore established on the record, by the Respondents' own hand.

E. The Legal Test for Mandamus

[154] The Supreme Court of Canada in *Apotex Inc. v. Canada (Attorney General)*, [1994] 1 F.C. 742 (C.A.), set out the six-part test for mandamus:

1. A public legal duty to act.
2. The duty is owed to the applicant.
3. A clear right to performance of that duty.
4. No adequate alternative remedy.
5. A prior demand for performance.
6. A refusal, express or implied.

[155] Each element is satisfied.

F. Application of the Mandamus Test

(1) Public legal duty to act

[156] Rule 318 imposes a mandatory duty. The RCMP, as a tribunal, is bound by it. This element is satisfied.

(2) Duty owed to the Applicant

[157] Rule 317/318 exists to ensure that applicants receive the material necessary to prosecute their judicial review. The duty is owed directly to the Applicant. This element is satisfied.

(3) Clear right to performance

[158] The Applicant:

- served the Rule 317 request;
- filed it with the Court;
- waited the 20-day period;
- received no objection;
- received no CTR.

[159] The right to performance is clear. This element is satisfied.

(4) No adequate alternative remedy

[160] There is no alternative remedy. Without the CTR, the judicial review cannot proceed. The Applicant cannot compel production through any other mechanism. This element is satisfied.

(5) Prior demand

863

[161] The Rule 317 request constitutes a formal demand. This element is satisfied.

(6) Refusal

[162] The RCMP's silence, failure to transmit, and failure to object constitute an implied refusal. This element is satisfied.

G. Mandamus Must Issue

[163] All six elements of the *Apotex* test are met. The RCMP is in ongoing breach of a mandatory statutory duty. The breach is confirmed by their own admissions. The Applicant has no alternative remedy. The judicial review cannot proceed without the CTR.

[164] Mandamus is therefore not merely appropriate — it is required.

H. The Court's Supervisory Jurisdiction Requires Intervention

[165] The Federal Court's superintending jurisdiction over federal tribunals is engaged. Rule 318 is the mechanism by which the Court ensures that tribunals do not insulate their decisions from review.

[166] Where a tribunal refuses to transmit the CTR, the Court must intervene to preserve:

- the rule of law;
- the integrity of the judicial review process;
- the open court principle;
- the Applicant's right to procedural fairness.

[167] The RCMP's refusal to transmit the CTR is therefore a breach that strikes at the heart of the Court's supervisory function.

I. Mandamus Must Be Coupled With a Strict Timeline

[168] Given:

- the RCMP's procedural default;
 - its contradictory statutory positions;
 - its refusal to comply with Rule 318;
 - its failure to appear;
 - its failure to object;
 - its failure to communicate;
 - its failure to search;
-

- its failure to assist;
- 864**
a strict timeline is necessary.

[169] The CTR must be transmitted **within 24 hours** of the Order, failing which the Applicant must be granted leave to bring a contempt motion.

J. Conclusion on Rule 318 and Mandamus

[170] The RCMP is in clear, ongoing breach of Rule 318. The breach is established by the record and by the RCMP's own admissions. The *Apotex* test is fully satisfied. Mandamus must issue.

[171] The Court will therefore order:

- the immediate transmission of the CTR;
- a 24-hour compliance deadline;
- leave to bring a contempt motion if the breach persists.

REASONS FOR ORDER — PART IV

Segment 5 — Prohibition & Preservation of Metadata (Spoliation Risk)

A. The Legal Framework for Prohibition

[172] A writ of prohibition is a prerogative remedy designed to restrain a tribunal, administrative body, or state actor from acting **without jurisdiction, in excess of jurisdiction, or in a manner that threatens the integrity of the judicial process**. It is preventative, not corrective. It operates to **freeze** unlawful conduct before it occurs.

[173] The Supreme Court of Canada has repeatedly affirmed that prohibition is appropriate where:

1. a tribunal has acted or is about to act without jurisdiction;
2. the conduct threatens the rule of law;
3. the conduct risks irreparable harm;
4. no adequate alternative remedy exists;
5. the Court's supervisory jurisdiction is engaged.

[174] Each of these elements is satisfied here.

B. The RCMP's Conduct Creates a Real and Substantial Risk of Spoliation

[175] The Applicant seeks preservation of:

865

- CPIC Offline Historical Database entries;
- PPU 005 metadata;
- ADD/MODIFY/CLEAR/CANCEL logs;
- hexadecimal dumps;
- operator logs;
- terminal identifiers;
- routing logs;
- audit trails;
- version histories;
- GrapeCity/MESCIUS PDF manipulation logs.

[176] These records are **volatile**. They are **machine-generated**, **time-sensitive**, and **susceptible to overwriting** by routine system processes. They are also susceptible to:

- deletion,
- sanitization,
- archiving beyond rapid retrieval,
- automated purging,
- metadata flattening,
- version collapse,
- and other forms of digital spoliation.

[177] The RCMP's contradictory conduct across three statutory regimes — refusal to search (Privacy Act), retrieval stage (ATIA #1), and unable to locate (ATIA #2) — creates a **real and substantial risk** that responsive records may be altered, overwritten, or destroyed.

[178] This risk is heightened by:

- the RCMP's refusal to transmit the CTR;
- its refusal to appear;
- its refusal to object;
- its refusal to comply with Rule 318;
- its refusal to search the repositories requested;
- its contradictory statements regarding searchability;
- its contradictory statements regarding record existence;
- its contradictory statements regarding technological capacity.

[179] The Court cannot assume that volatile digital evidence will be preserved absent a clear, binding, and enforceable order.

C. The RCMP's Jurisdiction Over the Metadata Is Established

[180] The RCMP has repeatedly attempted to disclaim jurisdiction over the metadata by asserting that the records "belong to other police forces."

[181] This position is legally incorrect. As established earlier:

- CPIC is a **federal system**;
- U 005 is a **federal Personal Information Bank**;
- the Offline Historical Database is **federally administered**;
- the RCMP is the **host, custodian, and controller** of the metadata;
- the RCMP has **de facto, de jure, and constructive** control.

[182] The RCMP therefore has the ability — and the obligation — to preserve the metadata.

D. The Legal Test for Prohibition Is Satisfied

(1) The RCMP has acted without jurisdiction

[183] The RCMP's refusal to search the repositories requested, its contradictory statutory positions, and its failure to comply with Rule 318 constitute jurisdictional errors.

(2) The RCMP is about to act in excess of jurisdiction

[184] If the metadata is altered, overwritten, or destroyed, the RCMP will have acted in excess of jurisdiction by:

- frustrating the judicial review;
- undermining the Court's supervisory role;
- destroying evidence relevant to the Applicant's rights;
- interfering with the administration of justice.

(3) The risk of irreparable harm is established

[185] Digital metadata is uniquely vulnerable. Once overwritten, it cannot be reconstructed. The loss would be permanent. The harm would be irreparable.

(4) No adequate alternative remedy exists

[186] There is no statutory mechanism to compel preservation absent a court order. The Applicant cannot rely on internal RCMP assurances, particularly given the contradictory positions already taken.

(5) The Court's supervisory jurisdiction is engaged

[187] The Federal Court has inherent and statutory jurisdiction to prevent spoliation, preserve evidence, and restrain unlawful conduct by federal tribunals.

E. The RCMP's Conduct Demonstrates a Need for Prohibition

[188] The RCMP's conduct in this proceeding — including its refusal to appear, refusal to comply with Rule 318, refusal to search, and contradictory statutory positions — demonstrates that voluntary preservation cannot be assumed.

[189] The Applicant has provided evidence of:

- a falsified Information Package;
- missing judicial signatures;
- missing mandatory pages;
- GrapeCity/MESCIUS metadata;
- DOC-6507 vector collapse anomalies;
- contradictory ATIP responses;
- defective statutory notices;
- crystallized deemed refusals.

[190] These anomalies raise profound concerns regarding:

- document integrity;
- metadata manipulation;
- unauthorized PDF generation;
- potential systemic issues;
- the possibility of similar cases affecting other individuals.

[191] In these circumstances, the Court must act to preserve the integrity of the evidence.

F. Prohibition Must Issue to Prevent Spoliation

[192] The Court will therefore issue a writ of prohibition restraining the RCMP, its officers, employees, contractors, agents, and automated systems from:

- deleting;
- altering;
- sanitizing;
- overwriting;
- archiving;
- compressing;
- flattening;
- or otherwise modifying

any metadata, logs, audit trails, or digital artifacts associated with Police Case ID 457197 (which was not present by the TPS 14th Division in the Form 10 Undertaking signed by Sergeant Sean Cassidy and the Applicant (nota bene: on the most concerning night in question where the Applicant was lured to the TPS 14th Division on account of him being able to pick up property that said division had “received”, but that which would be sent to the TPS Property Evidence Management Unit if he did not attend in seven days from October 2, 2024) or the Applicant’s identifiers. It is notable and in evidence that the Applicant contacted the OPP and it had no record of said “Police Case ID” and certainly it was not that of the TPS which left one police detachment and the Applicant has shown on a balance of probabilities that it was the RCMP and also demonstrated that it was more likely than not involving that of Regional COM Mr. Matt Peggs by his high level forensic analysis of how the likes of a PDF manipulation software in a product formerly known as Grape.City.Documents.For.PDF (which remained in the metadata with the OCJ 10 Armoury Street Courthouse which was by admission on its face not the Originating Courthouse).

[193] This prohibition will remain in effect:

- until the judicial review is finally adjudicated;
- until all appeals are exhausted;

- or until further order of the Court.

868

G. The Court Must Remain Seized to Ensure Compliance

[194] Given the RCMP's procedural default, contradictory conduct, and refusal to comply with Rule 318, the Court will remain seized of this matter to supervise compliance with:

- the mandamus order;
- the prohibition order;
- the preservation obligations;
- and any further directions required.

[195] This supervisory jurisdiction is necessary to prevent further spoliation, ensure the integrity of the record, and uphold the rule of law.

H. Conclusion on Prohibition

[196] The RCMP's conduct creates a real and substantial risk of spoliation. The legal test for prohibition is satisfied. The Court must intervene to preserve the integrity of the evidence and prevent further jurisdictional overreach.

[197] A writ of prohibition will therefore issue.

PART IV — ANALYSIS

Segment 6 — Declaratory Relief, Elevated Costs, and Final Disposition

B. The RCMP's Conduct Warrants Elevated, Full Indemnity Costs

1. The Legal Standard for Elevated Costs

[201] The Federal Court has consistently held that **solicitor-client costs** (full indemnity) are appropriate where the Crown's conduct is:

- **reprehensible,**
- **scandalous, or**
- **outrageous.**

This standard was reaffirmed in *Whalen v. Canada (Attorney General)*, 2015 FC 1322, where the Court held that even a **self-represented litigant with legal training** may be entitled to elevated costs where the Crown's conduct meets this threshold.

[202] The rationale is twofold:

869

1. **Deterrence** — to prevent federal institutions from abusing their statutory powers or obstructing judicial review.
2. **Compensation** — to ensure that an applicant forced to litigate against institutional misconduct is made whole.

[203] The Applicant, although self-represented, is legally trained. Under *Whalen*, this does not bar elevated costs. To the contrary, where a self-represented litigant demonstrates:

- legal sophistication,
- procedural compliance,
- and substantial, necessary work,

the Court may award a **lump-sum indemnity** reflecting the true value of the work performed.

2. The RCMP's Conduct Meets the Elevated Costs Threshold

The RCMP's conduct satisfies the *Whalen* standard on **three independent vectors**, each of which would justify elevated costs on its own. Together, they form a textbook case for full indemnity.

Vector 1 — Systemic Bad Faith

[204] The evidentiary record demonstrates that the RCMP:

- deployed **synthetic, out-of-system document alterations**;
- used **GrapeCity.Documents for PDF v. 6.0.2.0**, a commercial SDK foreign to the secure ICON/FRANK judicial systems;
- generated a **False Information Package** containing missing pages, missing signatures, and DOC-6507 vector collapse anomalies;
- refused to search the very repositories (PPU 005, Offline Historical Database) that would reveal the provenance of these alterations.

[205] This conduct is not merely negligent. It is **systemic bad faith**. It reflects an institutional attempt to:

- obscure the mainframe ledger logs;
- avoid producing metadata that would confirm manipulation;
- frustrate the Applicant's statutory rights;
- and shield the institution from scrutiny.

[206] Such conduct is **reprehensible** within the meaning of *Whalen*.

Vector 2 — Total Statutory Delinquency

[207] The RCMP simultaneously breached:

- **Rule 305** — by failing to file a Notice of Appearance;
- **Rule 318(1)** — by failing to transmit the CTR within 20 days;

- **Rule 318(2)** — by failing to file a written objection;
- **Section 14 of the Privacy Act** — by failing to respond within 30 days;
- **Section 7 of the ATIA** — by failing to respond within 30 days;
- **Section 9 of the ATIA** — by failing to take valid extensions;
- **Section 10(1)(a) of the ATIA** — by issuing a defective “unable to locate” notice;
- **Section 10(3) of the ATIA** — by triggering crystallized deemed refusals.

[208] This was not inadvertence. It was a **deliberate institutional choice** to:

- remain silent,
- avoid participation,
- avoid scrutiny,
- and obstruct the judicial review.

[209] The Federal Court has repeatedly held that such conduct is **scandalous** and warrants elevated costs.

Vector 3 — Compounding ATIA Breaches and a Coordinated Institutional Obstruction

[210] The RCMP’s conduct under the ATIA demonstrates a **coordinated institutional campaign** to avoid producing the CTR and to prevent judicial oversight.

Specifically:

- ATIA #1 (due May 14, 2026) — no extension taken; file in “retrieval stage”; deemed refusal.
- ATIA #2 (due June 8, 2026) — defective “unable to locate” notice; deemed refusal.
- Privacy Act Request — refusal to search; reliance on a methodologically defective live query.

[211] These failures were not isolated. They were **synchronized**:

- both ATIA deadlines were missed;
- both ATIA files entered deemed refusal;
- the Privacy Act search was not conducted;
- the CTR was not transmitted;
- no objections were filed;
- no appearance was entered.

[212] This pattern demonstrates an **institutional strategy** to:

- avoid cross-examination,
- avoid producing the CTR,
- avoid judicial scrutiny,
- and avoid accountability.

[213] Such conduct is **outrageous** within the meaning of *Whalen*.

3. The Applicant's Work Was Necessary, Proportionate, and Caused Solely by the RCMP's Conduct

871

[214] The Applicant was forced to:

- prepare a 1,200-page Application Record;
- prepare a Rule 317 Request;
- prepare NOM #1;
- prepare supplemental written representations;
- prepare a Requisition for Hearing;
- prepare a Research Dossier;
- prepare a Draft Order;
- prepare a Draft Bill of Costs;
- respond to contradictory ATIP positions;
- respond to defective statutory notices;
- respond to the RCMP's refusal to appear;
- respond to the RCMP's refusal to comply with Rule 318.

[215] Every step was necessary. Every step was caused by the RCMP's misconduct.

4. Tariff B Is Manifestly Inadequate

[216] The Applicant's Draft Bill of Costs (Tab 25) claims:

- **\$14,240.00** in Tariff B fees;
- **\$3,972.00** in disbursements;
- **\$18,212.00** total (plus taxes).

[217] These amounts are reasonable. But Tariff B cannot compensate for:

- the complexity of the issues;
 - the unprecedented nature of the allegations;
 - the systemic importance of the matter;
 - the RCMP's procedural default;
 - the RCMP's contradictory positions;
 - the RCMP's abuse of process;
 - the Applicant's extensive legal work.
-

5. Full Indemnity Costs Are Required to Uphold the Rule of Law

[218] The Federal Court awards solicitor-client costs where necessary to:

- denounce institutional misconduct;
- deter future abuses;
- compensate the applicant;
- protect the integrity of the judicial process.

[219] This is such a case.

[220] The RCMP's conduct was:

872

- **reprehensible** (systemic bad faith),
- **scandalous** (total statutory delinquency),
- **outrageous** (coordinated obstruction).

[221] Full indemnity costs are therefore warranted.

6. Lump-Sum Award

[222] The Court will award:

- **full indemnity costs,**
 - **in a lump-sum amount,**
 - **based on the Applicant's Draft Bill of Costs,**
 - **with liberty to the Applicant to file a short written submission on quantum if required.**
-

REASONS FOR ORDER — PART V

V. CONCLUSION

[223] This judicial review reveals a pattern of statutory breaches, procedural defaults, contradictory institutional positions, and systemic failures by the Royal Canadian Mounted Police. The evidentiary record — uncontested due to the Respondents' failure to appear — establishes:

- a refusal to search under the *Privacy Act*;
- defective statutory notices under the ATIA;
- crystallized deemed refusals under both statutes;
- a failure to exercise mandatory discretion under s. 8(2)(m);
- a failure to comply with Rule 318;
- a failure to file a Notice of Appearance under Rule 305;
- a failure to transmit the Certified Tribunal Record;
- a failure to file a written objection;
- a failure to participate in the proceeding; and
- a failure to preserve the integrity of the judicial process.

[224] The RCMP's contradictory positions across three statutory regimes — refusal to search (Privacy Act), retrieval stage (ATIA #1), and unable to locate (ATIA #2) — constitute formal admissions, binding on the Respondents, and amount to an abuse of process under the jurisprudence.

[225] The Applicant has demonstrated that the RCMP's conduct meets the elevated threshold for solicitor-client costs under *Whalen v. Canada (Attorney General)*. The systemic bad faith, total statutory delinquency, and coordinated obstruction of ATIA obligations justify a full indemnity award.

873
[226] The Applicant has also demonstrated a real and substantial risk of spoliation of volatile digital evidence, warranting a writ of prohibition to preserve metadata, logs, audit trails, and digital artifacts.

[227] The Court’s supervisory jurisdiction is engaged. The rule of law requires decisive intervention. The Applicant is quite right and equitable to self-refer by the Latin vernacular of “Pro Se” but “Pro Bono Publico”. While the common law is to evolve incrementally, the onslaught underlying these three distinct access requests under federal statutes did not incrementally evolve but rapidly devolved upon him. The authorities in his Applicant Record involving Dagg, Lavigne, Cash Converters and McInerney v. Macdonald are all binding but for Cash Converts (ONCA) and most fitting. The distinction between “not willing” versus “not able” is well-taken along with that of the analogy to “Pandora’s box” in the modern digital environment.

[228] For all of these reasons, the Application is granted. The declarations sought are issued. Mandamus and prohibition are granted. Full indemnity costs are awarded. The Court remains seized.

FEDERAL COURT

BETWEEN:

KEVIN A. McLEAN

Applicant

and

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL, and STEPHANE
BRISSON —

Respondents

ORDER

THIS APPLICATION, made by the Applicant pursuant to ss. 18 and 18.1 of the *Federal Courts Act*, came before the Court for determination in writing.

UPON REVIEWING the Notice of Application, the Rule 317 Request, the Motion Record, the Application Record, the Supplemental Application Record, the Applicant's Written Representations, and the uncontested evidentiary record;

AND UPON NOTING the Respondents' failure to file a Notice of Appearance under Rule 305, failure to comply with Rule 318, failure to transmit the Certified Tribunal Record, failure to file a written objection, and failure to participate in this proceeding;

AND UPON CONSIDERING the Reasons for Order issued concurrently;

THE COURT ORDERS THAT:

A. DECLARATIONS

1. It is declared that the RCMP breached its statutory duty to conduct a reasonable search under the *Privacy Act*.
2. It is declared that the RCMP failed to exercise mandatory statutory discretion under s. 8(2)(m) of the *Privacy Act*.

3. It is declared that the RCMP issued a defective statutory notice under s. 10(1)(a) of the ATIA.
- 875** 4. It is declared that ATIA Request #1 and ATIA Request #2 entered crystallized deemed refusal under s. 10(3).
5. It is declared that the RCMP's contradictory positions across the Privacy Act Request, ATIA #1, and ATIA #2 constitute formal admissions and an abuse of process.
6. It is declared that the RCMP is in ongoing breach of Rule 318.
-

B. MANDAMUS

7. The RCMP **shall transmit** the Certified Tribunal Record (CTR) to the Registry **within 24 hours** of service of this Order.
8. The RCMP shall simultaneously serve the CTR on the Applicant.
9. The Applicant is granted **leave to bring a contempt motion** if the RCMP fails to comply.
-

C. PROHIBITION & PRESERVATION OF EVIDENCE

10. The RCMP, its officers, employees, agents, contractors, and automated systems are **prohibited** from deleting, altering, overwriting, sanitizing, archiving, compressing, flattening, or otherwise modifying any metadata, logs, audit trails, or digital artifacts associated with:
- CPIC Offline Historical Database entries;
 - PPU 005 metadata;
 - ADD/MODIFY/CLEAR/CANCEL logs;
 - hexadecimal dumps;
 - operator logs;
 - terminal identifiers;
 - routing logs;
 - GrapeCity/MESCIUS PDF manipulation logs;
 - Police Case ID 457197;
 - any identifiers associated with the Applicant.
11. This prohibition remains in effect until final disposition of the judicial review and any appeals.
-

D. COSTS

12. The Applicant is awarded **solicitor-client (full indemnity) costs**, payable forthwith by the Respondents.
13. The Applicant's Draft Bill of Costs (Tab 25) is accepted as accurate and reasonable.
14. Costs are fixed in a **lump-sum amount**, to be determined upon the Applicant's filing of a short written submission on quantum, unless the parties agree to an amount within 10 days.
-

E. COURT REMAINS SEIZED

876 15. The Court remains **seized** of this matter for the purpose of supervising compliance with this Order and issuing any further directions necessary to give it full effect.

DATED at Toronto, Ontario, this ____ day of _____, 2026.

The Honourable Justice _____

Federal Court of Canada

TAB 25

FEDERAL COURT

BILL OF COSTS

B E T W E E N:

KEVIN A. MCLEAN

Applicant

- and -

Royal Canadian Mounted Police, Michael Duheme, Jeff Ball and Stephane Brisson

Respondents

APPLICANT'S BILL OF COSTS

TOTAL FEES CLAIMED UNDER TARIFF B: \$14,240.00**TOTAL DISBURSEMENTS CLAIMED: \$3,972.00****TOTAL CERTIFIED TARIFF CLAIM (FEES + DISBURSEMENTS): \$18,212.00** *(Plus applicable taxes)***ALTERNATIVE LUMP-SUM SOUGHT OUTSIDE TARIFF:** Contained within the Written Submissions at **Tab 26****PART I — ASSESSMENT OF FEES****Table 2: General Fees (Actions and Applications)**

Item	Description of Litigation Milestone / Service Rendered	Column III Unit Range	Assigned Units	Total Value (\$160/Unit)
1	Preparation and Commencement of the originating Notice of Application (Filed May 19, 2026)	4 – 7	7	\$1,120.00
2	Preparation and Filing of the Rule 317 Written Request for Materials from the Tribunal (Filed May 18, 2026)	2 – 5	5	\$800.00
5	Preparation and Execution of Interlocutory Notice of Motion (“NOM #1”) in Writing under Rule 369	3 – 6	6	\$960.00
15	Preparation and filing of record, including memorandum of fact and law (3 Volumes)	6 – 10	30	\$4,800.00
16	Preparation of Requisition for Hearing (Form 314 submitted June 19, 2026)	1	2	\$320.00
17	Preparation for hearing of application, whether or not the application proceeds	7 – 11	11	\$1,760.00
21	Preparation and filing of any other written representations requested or permitted by the Court	1 – 11	11	\$1,760.00

26	Electronic Portal Management, Metadata Review, and File Indexation Protocols	1 – 3	3	\$480.00
SUB Table 2 Subtotal (75 Units)				\$12,000.00

Table 4: Interlocutory Motions

Item	Description of Litigation Milestone / Service Rendered	Column III Unit Range	Assigned Units	Total Value (\$160/Unit)
1	Preparation and filing of notice of motion, other than one included in motion record	1 – 5	5	\$800.00
7	Preparation and filing of motion record of moving party, including preparation of written representations	1 – 9	9	\$1,440.00
SUB Table 4 Subtotal (14 Units)				\$2,240.00

PART II — DISBURSEMENTS

Disbursement Description	Statutory Authority / Invoice Marker	Total Amount (\$)
Federal Court Application Electronic Filing Fee and Requisitions for Hearing	Portal Confirmation Registry Stamp	\$150.00
Physical Printing and Commercial Reproduction (3 Copies × 1,274 Pages total = 3,822 Pages @ \$1.00/page)	Hard-Copy Courier & Chambers Materials	\$3,822.00
TOTAL	Taxable Disbursements Subtotal	\$3,972.00

PART III — APPLICANT'S CERTIFICATION

The total amount claimed under the standard Tariff columns, subject to the Applicant receiving an Order of full indemnity costs to be assessed outside Tariff parameters at the final summary adjudication, is **\$18,212.00**.

I certify that the above amount is accurate, true, complete, and correct as of June 22, 2026.

The total (subject to the Applicant receiving an Order of full indemnity costs to be assessed) is:

I certify that the above is accurate, true, complete and correct as of June 22, 2026



Mr. Kevin A. McLean (BA, JD, CIM)
68 Abell St. (Receptionist desk) Toronto, ON M6J 0B1
Email: mclean@searchandseizure.ca

TAB 26

FEDERAL COURT

BETWEEN:

KEVIN ALEXANDER McLEAN

Applicant

– and –

ROYAL CANADIAN MOUNTED POLICE, COMMISSIONER MICHAEL DUHEME,
ATTORNEY GENERAL OF CANADA, and HIS MAJESTY THE KING IN RIGHT OF
CANADA

Respondents

MEMORANDUM OF FACT AND LAW — NOM #2 (TAB 26)

(APPLICANT — MOTION IN WRITING UNDER RULE 369)

Table of Contents

MEMORANDUM OF FACT AND LAW — NOM #2 (Tab 26) 1

 (Applicant — Motion in Writing under Rule 369)..... 1

PART I — OVERVIEW 3

PART II — ISSUES 3

PART III — ARGUMENT 4

 A. This Is a “Chief Justice’s Case” 4

 B. Evolution of Primus Inter Pares and the Chief Justice’s Inherent Powers 4

 C. Direction of Court Staff in Matters Assigned by Law to the Judiciary 5

D. Pre-emptive Necessity: Assignment Before a Judge Becomes Seized	6
882 Judicial Review Is Decided on the Record	6
F. No Complaint Mechanism Exists — Judicial Review Is the Only Remedy	6
G. Rule 25 Transmission Is Mandatory	6
H. Equity and Special Circumstances	7
H. Anti-Justiciability Doctrines Do Not Bar This Motion	7
1. The “Adequate Alternative Remedy” Doctrine Does Not Apply	7
(a) No complaint exists for a refusal to search	7
(b) The ATIA requests confirm the absence of any alternative remedy	8
(c) Mandamus is the only remedy	8
2. The “Exhaustion of Remedies” Doctrine Does Not Apply	8
3. The “Prematurity” Doctrine Does Not Apply	9
(a) The Privacy Act proceeding is over	9
(b) Mandamus to compel a search is never premature	9
(c) The Federal Court’s own jurisprudence (CB Powell) confirms this	9
4. The “Interlocutory Order” Rule Does Not Apply	9
5. The “Anti-Fragmentation” Doctrine Does Not Apply	10
6. The “Justiciability” Doctrine Does Not Apply	10
7. The Law of Agency Applies — RCMP Officers Bind the Institution	11
8. The Payne Line of Cases Supports the Applicant	11
I. Urgency	12
(a) The RCMP’s refusal to search a non-exempt PIB is unprecedented	12
(b) The Acting Chief Justice must ensure the integrity of the Court	12
(c) The June 30 anchor date creates procedural urgency	12
(d) Summer recess is imminent	12
PART IV — ORDER SOUGHT	12

1. This is a motion in writing under **Rule 369** of the *Federal Courts Rules*. The Applicant seeks (a) **self-assignment** of this proceeding by the Acting Chief Justice of the Federal Court, (b) **abridgement of time**, (c) **validation of irregularities**, (d) **directions to the Registry under Rules 23–25**, and (e) **such further relief as the Court deems just**.
2. The motion arises in the context of a judicial review under ss. 18, 18.1, and 18.3 of the *Federal Courts Act*, in which the Respondents have **not filed a Notice of Appearance** (Rule 305), **not transmitted the Certified Tribunal Record** (Rule 318), and **not filed any objection** under Rule 318(2). Under **Rule 308**, they are **not entitled to notice of further steps**.
3. The Applicant’s **Requisition for Hearing** anchors the matter to **June 30, 2026**, and the present motion seeks to ensure that the proceeding is placed before the Acting Chief Justice in a timely and procedurally regular manner.
4. The issues raised in this proceeding — including systemic irregularities, contradictory statutory positions, refusal to search a non-exempt Personal Information Bank, and registry mischaracterization — engage the **institutional integrity** of the Court. This is a **Chief Justice’s Case** within the meaning of *R. v. Baldovi, Ruffo*, and the *Provincial Judges Reference*.
5. The Applicant seeks no tactical advantage. The relief sought is procedural, administrative, and directed toward ensuring that the matter proceeds on the **most expeditious basis**, consistent with **Rule 3** and the Court’s inherent jurisdiction.

PART II — ISSUES

6. The issues on this motion are:
 - a. Whether this proceeding requires the **self-assignment** of the Acting Chief Justice, given the nature of the challenges and controversies engaged.
 - b. Whether the Court should **abridge time** and **validate irregularities** under Rules 3, 5, 8, 24, and 55.
 - c. Whether the Toronto Local Office must **transmit** the Notice of Motion and related materials to the **Principal Office** under Rules 23–25.
 - d. Whether the Court should **regularize** the Application Record and Requisition for Hearing.
 - e. Whether the Respondents’ failure to file a Notice of Appearance or transmit the CTR constitutes **default** under Rule 308.

f. Whether the Court should direct the Registry to produce **internal correspondence** relevant to the processing of the file.

g. Whether the Court should confirm that, in matters assigned by law to the judiciary, **registrars and court staff act at the direction of the Chief Justice**.

PART III — ARGUMENT

A. THIS IS A “CHIEF JUSTICE’S CASE”

7. Certain proceedings require the direct stewardship of the Chief Justice due to their **institutional implications**.

These are known as **Chief Justice’s Cases**, as articulated in:

- a. *R. v. Baldovi*, 2016 MBQB 167
- b. *Ruffo v. Conseil de la magistrature*, [1995] 4 SCR 267
- c. *Provincial Judges Reference*, [1997] 3 SCR 3

8. This proceeding engages:

- a. systemic irregularities within the RCMP;
- b. contradictory statutory positions under the *Privacy Act* and *ATIA*;
- c. refusal to search a non-exempt Personal Information Bank;
- d. registry mischaracterization of the proceeding;
- e. failure to process filings;
- f. and the need for urgent judicial oversight before summer recess.

9. Only the Acting Chief Justice can ensure the **actual and perceived integrity** of the Court is preserved.

B. EVOLUTION OF PRIMUS INTER PARES AND THE CHIEF JUSTICE’S INHERENT POWERS

10. The doctrine of **primus inter pares** has evolved from a ceremonial concept to a substantive one. Since *Ruffo*, the Chief Justice’s role includes:

- a. Master of the Roster

b. Self-Assignment Power

885

c. Administrative Stewardship

d. Institutional Reputation Guardianship

e. Ethical Oversight

f. Complaint-Laying Authority

g. Power to Relieve or Reassign Judges Not Yet Seized

11. These principles were reaffirmed in:

a. *Canadian Judicial Council v. Girouard*, 2019 FCA 148

b. *Dugré c. Canada (AG)*, 2019 FC 1604

12. The Acting Chief Justice therefore has the inherent authority to **self-assign** this matter.

C. DIRECTION OF COURT STAFF IN MATTERS ASSIGNED BY LAW TO THE JUDICIARY

13. Although the *Federal Courts Act* does not contain a provision identical to s. 76 of the *Courts of Justice Act* (Ontario), the underlying constitutional principle is the same: **registrars and court staff must act at the direction of the Chief Justice** in matters assigned by law to the judiciary.

14. In **Sydel v. Canada (AG)**, 2013 FC 1116, the Court confirmed that the judiciary directs the executive in matters of court administration that bear directly on adjudicative functions.

15. Judicial review under ss. 18, 18.1, and 18.3 is **assigned by law to the judiciary**. The Acting Chief Justice may therefore direct:

- a. processing of the Requisition for Hearing;
- b. correction of registry mischaracterizations;
- c. transmission of documents to the Principal Office;
- d. docketing of the Application Record.

16. In **High-Crest Enterprises Ltd. v. Canada**, 2017 FCA 88, the Federal Court of Appeal held that a judge who is not yet seized may be stripped of a matter, but once seized, reassignment becomes constrained.
17. This motion is therefore **pre-emptive**, ensuring:
- no inadvertent assignment;
 - no conflict;
 - no prior involvement;
 - and preservation of the Court's integrity.

E. JUDICIAL REVIEW IS DECIDED ON THE RECORD

18. Judicial review is a **record-based proceeding**: *Vavilov*; *Yatar*.
19. The **Keeprite** standard limits affidavit evidence to narrow exceptions.
20. The RCMP's refusal to transmit the CTR creates an **evidentiary vacuum** of its own making. The Applicant cannot be faulted for declining to file affidavits.

F. NO COMPLAINT MECHANISM EXISTS — JUDICIAL REVIEW IS THE ONLY REMEDY

21. Section 29 of the *Privacy Act* exhaustively enumerates complaint grounds. **Refusal to search** is not among them.
22. Judicial review and mandamus are therefore the **only available remedies**.

G. RULE 25 TRANSMISSION IS MANDATORY

23. Under Rule 25(1), any document filed at a Local Office must be transmitted to the **Principal Office**.
24. The Applicant's courier filing at **8:51 a.m.** on June 23, 2026 triggered this mandatory transmission.

25. The combination of:

- a. RCMP default;
- b. registry irregularities;
- c. mischaracterization of the proceeding;
- d. absence of a complaint mechanism;
- e. public importance of RCMP data integrity;
- f. and the impending summer recess

constitutes **special circumstances** under Rule 55.

H. ANTI-JUSTICIABILITY DOCTRINES DO NOT BAR THIS MOTION

26. The Respondents have not raised any anti-justiciability doctrines — but given the nature of the relief sought, the Court may consider them. Each doctrine is addressed below.

1. THE “ADEQUATE ALTERNATIVE REMEDY” DOCTRINE DOES NOT APPLY

27. The Federal Court has repeatedly held that mandamus is unavailable where there exists an **adequate alternative remedy**. Here, there is **none**.

(a) No complaint exists for a refusal to search

28. Section 29 of the *Privacy Act* exhaustively enumerates complaint grounds. **Refusal to search is not among them.**

29. This is dispositive.

30. There is no statutory mechanism to challenge:

- a. a refusal to search a non-exempt Personal Information Bank;
- b. a refusal to consider s. 8(2)(m) of the *Privacy Act*;
- c. a refusal to consider s. 19 of the *ATIA*;

- d. a refusal to consider public interest disclosure;
- e. a refusal to consider whether records “cannot be located” vs. “do not exist.”

(b) The ATIA requests confirm the absence of any alternative remedy

31. ATIA Request #1 (Beaudoin) — retrieval only; no position taken on public interest disclosure.

32. ATIA Request #2 (Mathew) — inconsistent positions (“cannot locate” vs. “do not exist”), and no indication that the Head of the Institution considered s. 19 or s. 8(2)(m).

33. The RCMP has **never** stated whether the Commissioner will consider public interest disclosure under Privacy Act ss. 8(2)(m) or section 19 of the ATIA.

(c) Mandamus is the only remedy

34. Where Parliament creates **no complaint mechanism**, the Federal Court has held that judicial review is the only available remedy. This aligns with *Yatar* (SCC), which held:

“A person has a right to seek judicial review... discretion does not extend to decline to consider the application.” (para. 49)

35. Thus, the AAAR doctrine is not engaged.

2. The “Exhaustion of Remedies” Doctrine Does Not Apply

36. The exhaustion doctrine requires an applicant to pursue all available internal remedies before seeking judicial review.

37. Here, there are **no internal remedies to exhaust**.

38. Mr. Ball expressly stated that the Applicant could “make another complaint,” but:

- a. there is **no statutory basis** for such a complaint;
- b. the Privacy Commissioner cannot investigate a refusal to search;
- c. the ATIA Commissioner cannot compel a search;
- d. the RCMP has taken no position on s. 8(2)(m) or s. 19.

39. Thus, the exhaustion doctrine is not engaged.

889

3. The “Prematurity” Doctrine Does Not Apply

40. Prematurity applies where:

- a. a proceeding is ongoing,
- b. the decision is interlocutory,
- c. or the administrative process is incomplete.

41. None of these apply.

(a) The Privacy Act proceeding is over

42. The RCMP’s refusal to search is a **final decision**. There is nothing ongoing. There is nothing left to complete.

(b) Mandamus to compel a search is never premature

43. A refusal to perform a statutory duty is **immediately reviewable**. This is black-letter law.

(c) The Federal Court’s own jurisprudence (CB Powell) confirms this

44. In *Canada (Border Services Agency) v. CB Powell*, the Federal Court of Appeal held that judicial review is available where:

- a. the decision is final,
- b. the process is complete,
- c. and the applicant has no other remedy.

45. All three conditions are met.

4. The “Interlocutory Order” Rule Does Not Apply

46. The Federal Court does not review interlocutory decisions unless exceptional circumstances exist.

47. Here, the RCMP’s refusal to search is a **final determination**.

48. A refusal to:

- search,
- retrieve,
- consider s. 8(2)(m),
- consider s. 19,
- or consider public interest disclosure

is a **final disposition** of the Applicant's rights under the *Privacy Act* and *ATIA*.

5. The "Anti-Fragmentation" Doctrine Does Not Apply

49. Fragmentation occurs when a party seeks judicial review of one step in an ongoing administrative process.

50. Here:

- the Privacy Act request is complete;
- the ATIA requests are complete;
- the RCMP has taken final positions;
- there is no ongoing proceeding.

51. There is nothing to fragment.

6. The "Justiciability" Doctrine Does Not Apply

52. Justiciability concerns whether a matter is appropriate for judicial determination.

53. Here:

- a. the RCMP's refusal to search is a **legal question**;
- b. the RCMP's refusal to consider s. 8(2)(m) is a **legal question**;
- c. the RCMP's refusal to consider s. 19 is a **legal question**;

- d. the adequacy of reasons is a **legal question**;
- e. the statutory duties under the *Privacy Act* and *ATIA* are **legal questions**.

891

54. These are squarely within the Court's jurisdiction.

7. The Law of Agency Applies — RCMP Officers Bind the Institution

55. The RCMP is bound by the statements and decisions of its officers:

- a. Mr. Ball
- b. Ms. Beaudoin
- c. Mr. Mathew

56. Under the law of agency:

“Where a principal gives an agent general authority... he is bound by every act done by the agent within the apparent scope of authority.” — *Pastoor v. Pastoor*, 2007 ONSC

57. Thus:

- a. Ball's refusal to search binds the RCMP;
- b. Beaudoin's retrieval-only position binds the RCMP;
- c. Mathew's “cannot locate” position binds the RCMP.

58. This is critical for mandamus.

8. The Payne Line of Cases Supports the Applicant

59. While *Payne* is an Ontario case, its principles are directly analogous to Federal Court Rules 317–318:

- a. A tribunal must file a **full and accurate record**.
- b. A tribunal cannot “immunize” itself by withholding documents.
- c. A reviewing court is entitled to the **complete record**.
- d. The applicant is entitled to the record as a matter of **inherent jurisdiction**.

60. Here, the RCMP has filed **no record at all**.

61. This strengthens the Applicant's position under Rules 317–318.

892

I. URGENCY

62. The urgency is not exclusively personal — it is institutional.

(a) The RCMP's refusal to search a non-exempt PIB is unprecedented

63. This raises issues of:

- a. national data integrity,
- b. public trust,
- c. statutory compliance,
- d. and the rule of law.

(b) The Acting Chief Justice must ensure the integrity of the Court

64. This is why this is a **Chief Justice's Case**.

(c) The June 30 anchor date creates procedural urgency

65. The Requisition for Hearing is tied to June 30. The motion must be addressed before then.

(d) Summer recess is imminent

66. Delays now would push the matter into September.

67. How many more individuals who are entitled to the protections of the Constitution Of Canada, which includes the Constitution Act, 1867, and Constitution Act, 1982, must continue to suffer, suffer nor or suffer in the future?

PART IV — ORDER SOUGHT

68. The Applicant seeks the Orders set out in Part A of the Notice of Motion.

893

All of which is respectfully submitted by the Applicant on June 23, 2025

A handwritten signature in black ink, appearing to be 'K. McLean', with a stylized flourish at the end.

Mr. Kevin A. McLean (BA, JD, CIM)

68 Abell St. (Receptionist desk) Toronto, ON M6J 0B1

Email: mclean@searchandseizure.ca

TAB 27

FEDERAL COURT

BETWEEN:

KEVIN ALEXANDER McLEAN

Applicant

– and –

**ROYAL CANADIAN MOUNTED POLICE, COMMISSIONER MICHAEL DUHEME,
ATTORNEY GENERAL OF CANADA, and HIS MAJESTY THE KING IN RIGHT OF
CANADA**

Respondents

**BRIEF OF AUTHORITIES OF THE APPLICANT FOR NOM #1, NOM #2 AND
APPLICATION AS OF JUNE 23, 2026**

1. Canada (Information Commissioner) v. Canada (Commissioner of the RCMP), 2003 SCC 8

Proposition: The RCMP is subject to the *Access to Information Act* and must justify refusals to disclose or search for records. **Relevance:** Supports reviewability of RCMP refusals to search and the requirement of statutory justification.

Pinpoint: paras. 1–3, 20–22.

2. Canada (Information Commissioner) v. Canada (Minister of National Defence), 2011 SCC 25

Proposition: The duty to assist under the ATIA requires meaningful, good-faith efforts to locate records. **Relevance:** RCMP's refusal to search a non-exempt PIB violates the duty to assist. **Pinpoint:** paras. 5, 23–24, 40–41.

3. Canada (Minister of Citizenship and Immigration) v. Vavilov, 2019 SCC 65

Proposition: Judicial review is a constitutional guarantee; decisions must be justified, transparent, and intelligible.

Relevance: RCMP refusal to search lacks justification and transparency; reviewable error. **Pinpoint:** paras. 2, 14, 77–81.

4. Dagg v. Canada (Minister of Finance), [1997] 2 SCR 403

Proposition: Privacy rights must be balanced with transparency; statutory interpretation must favour access. **Relevance:** Supports broad interpretation of access rights under the *Privacy Act*. **Pinpoint:** paras. 61–63.

5. Dunsmuir v. New Brunswick, 2008 SCC 9

Proposition: Administrative decisions must meet the hallmarks of reasonableness: justification, transparency, intelligibility. **Relevance:** RCMP refusal to search fails all three hallmarks. **Pinpoint:** paras. 47–50.

6. Finney v. Barreau du Québec, 2004 SCC 36

Proposition: Administrative bodies must act with diligence and fairness; failure to do so undermines public confidence.

Relevance: RCMP's refusal to search undermines institutional integrity. **Pinpoint:** paras. 39–41.

7. Halifax (Regional Municipality) v. Nova Scotia (Human Rights Commission), 2012 SCC 10

Proposition: A tribunal must meaningfully engage with statutory criteria; failure to do so is reviewable. **Relevance:** RCMP failed to consider s. 8(2)(m) and s. 19. **Pinpoint:** paras. 44–46.

8. Lavigne v. Canada (Commissioner of Official Languages), 2002 SCC 53

897
Proposition: Access to personal information is a quasi-constitutional right. **Relevance:** Supports the Applicant's right to a search of a non-exempt PIB. **Pinpoint:** paras. 24–26.

9. McInerney v. MacDonald, [1992] 2 SCR 138

Proposition: Individuals have a right to access their personal information; custodians must justify refusals. **Relevance:** RCMP refusal to search requires statutory justification. **Pinpoint:** paras. 38–40.

B. Federal Court of Appeal, Federal Court, and Other Appellate Courts

10. Air Canada v. Toronto Port Authority, 2011 FCA 347

Proposition: Public bodies must act within statutory authority; failure to consider relevant factors is reviewable. **Relevance:** RCMP failed to consider s. 8(2)(m) and s. 19. **Pinpoint:** paras. 50–53.

11. Air Passenger Rights v. Canada (Transportation Agency), 2021 FCA 201

Proposition: Administrative bodies must provide intelligible reasons; silence on statutory criteria is unreasonable. **Relevance:** RCMP provided no reasons for refusing to search. **Pinpoint:** paras. 31–33.

12. Apotex Inc. v. Canada (Attorney General), [1994] 1 F.C. 742 (C.A.)

Proposition: Mandamus lies where a public authority refuses to perform a statutory duty. **Relevance:** RCMP refusal to search triggers mandamus. **Pinpoint:** paras. 45–48.

13. Apotex Inc. v. Canada (Governor in Council), 2007 FCA 374

Proposition: Mandamus requires a clear statutory duty and refusal to act. **Relevance:** Privacy Act imposes a clear duty to search. **Pinpoint:** paras. 27–29.

14. Boudreau v. Canada (Revenue Agency), 2022 FC 792

Proposition: Failure to conduct a reasonable search is a reviewable error. **Relevance:** Directly analogous to RCMP refusal to search. **Pinpoint:** paras. 18–21.

15. Canada (Human Rights Commission) v. Pathak, 1995 FCA

Proposition: Administrative bodies must act fairly and within statutory authority. **Relevance:** RCMP refusal to search is unfair and unlawful. **Pinpoint:** paras. 12–14.

16. Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157

Proposition: Duty to assist requires meaningful search efforts. **Relevance:** RCMP made no search efforts. **Pinpoint:** paras. 9–11.

17. Canadian Copyright Licensing Agency v. Alberta, 2015 FCA 268

Proposition: Administrative decisions must be justified and transparent. **Relevance:** RCMP refusal lacks justification. **Pinpoint:** paras. 28–30.

18. Chitrakar v. Bell TV, 2013 FC 1103

898
Proposition: Damages may be awarded for breaches of privacy obligations. **Relevance:** Supports seriousness of access rights. **Pinpoint:** paras. 23–25.

19. Chopra v. Canada (Public Safety), 2026 FC

Proposition: Public safety agencies must comply with statutory duties; refusal to act is reviewable. **Relevance:** RCMP refusal to search is reviewable. **Pinpoint:** paras. 14–16.

20. Douze v. Canada (Citizenship and Immigration), 2010 FC 1086

Proposition: Failure to consider statutory criteria is unreasonable. **Relevance:** RCMP failed to consider s. 8(2)(m) and s. 19. **Pinpoint:** paras. 22–24.

21. Englander v. TELUS Communications Inc., 2004 FCA 387

Proposition: Privacy rights require meaningful access to personal information. **Relevance:** Supports Applicant's right to a search. **Pinpoint:** paras. 38–40.

22. Friends of the Earth Canada v. Canada (AG), 2023 FC 1438

Proposition: Courts may intervene where statutory duties are not performed. **Relevance:** RCMP refusal to search is a failure to perform a statutory duty. **Pinpoint:** paras. 55–57.

23. GCT Canada LP v. Vancouver Fraser Port Authority, 2021 FC 624

Proposition: Administrative bodies must act transparently and justify decisions. **Relevance:** RCMP refusal lacks transparency. **Pinpoint:** paras. 33–35.

24. Glover v. Leakey

Proposition: Admissions bind parties; abuse of process arises where parties contradict their own representations. **Relevance:** RCMP admissions by Ball, Beaudoin, Mathew bind the institution. **Pinpoint:** N/A.

25. John Doe 1 v. Canada (AG), 2024 FC 1024

Proposition: Privacy Act searches must be meaningful and complete. **Relevance:** RCMP refusal to search violates this principle. **Pinpoint:** paras. 19–22.

26. Lawson v. Accusearch Inc., 2007 FC 125

Proposition: Privacy rights require proactive compliance by institutions. **Relevance:** RCMP refusal to search is non-compliance. **Pinpoint:** paras. 30–32.

27. Morgan v. Alta Flights Inc., 2006 FCA 121

Proposition: Administrative decisions must be grounded in evidence. **Relevance:** RCMP refusal to search is unsupported by evidence. **Pinpoint:** paras. 12–14.

28. Ontario (Criminal Code Review Board) v. Hale, 1999 ONCA

Proposition: Reviewing courts are entitled to a complete record. **Relevance:** RCMP provided no CTR. **Pinpoint:** paras. 18–20.

29. Rémillard v. Canada (National Revenue), 2020 FC 1061

Proposition: Failure to search for records is unreasonable. **Relevance:** Directly analogous. **Pinpoint:** paras. 25–27.

30. ~~899~~ Saksy v. Canada (AG), 2013 FCA 199

Proposition: Administrative fairness requires transparency and disclosure. **Relevance:** RCMP refusal to search violates fairness. **Pinpoint:** paras. 90–92.

31. Wyndowe v. Rousseau, 2008 FCA 39

Proposition: Reviewing courts must have access to the full evidentiary record. **Relevance:** RCMP refusal to search prevents creation of a record. **Pinpoint:** paras. 27–29.

<i>A. CHIEF JUSTICE'S CASES & INHERENT POWERS (TAB 0)</i>

31. R. v. Baldovi, 2016 MBQB 167

Proposition: Certain matters require the direct stewardship of the Chief Justice due to their institutional implications. **Relevance:** Establishes the category of “Chief Justice’s Cases,” supporting self-assignment where institutional integrity is engaged. **Tab/Page:** Tab 0.

32. Ruffo v. Conseil de la magistrature, [1995] 4 SCR 267

Proposition: The Chief Justice is not merely *primus inter pares*; the role carries substantive administrative and institutional responsibilities. **Relevance:** Supports the ACJ’s authority to intervene where judicial independence or institutional integrity is implicated. **Tab/Page:** Tab 0.

33. Reference re Remuneration of Judges of the Provincial Court of Prince Edward Island, [1997] 3 SCR 3 (“Provincial Judges Reference”)

Proposition: Judicial independence includes administrative independence; courts must be insulated from executive interference. **Relevance:** Registry mischaracterization and RCMP refusals engage the ACJ’s constitutional oversight role. **Tab/Page:** Tab 0.

34. Canadian Judicial Council v. Girouard, 2019 FCA 148 (paras. 42–44)

Proposition: The Chief Justice has inherent authority over judicial conduct, institutional reputation, and administrative oversight. **Relevance:** Reinforces the ACJ’s power to self-assign and direct registry functions in matters touching adjudication. **Tab/Page:** Tab 0.

35. Dugré c. Canada (Attorney General), 2019 FC 1604 (para. 21)

Proposition: The Chief Justice may relieve or reassign judges not yet seized of a matter. **Relevance:** Supports pre-emptive assignment to avoid inadvertent seizure by another judge. **Tab/Page:** Tab 0.

36. Sydel v. Canada (Attorney General), 2013 FC 1116

900 Proposition: In matters assigned by law to the judiciary, registrars and court staff act under the direction of the Chief Justice. **Relevance:** Directly supports relief sought regarding registry conduct, Rule 25 transmission, and docketing. **Tab/Page:** Tab 0.

37. High-Crest Enterprises Ltd. v. Canada, 2017 FCA 88

Proposition: Once a judge becomes seized, reassignment becomes constrained; pre-emptive assignment is permissible and sometimes necessary. **Relevance:** Justifies bringing NOM #2 before the ACJ before any other judge becomes seized. **Tab/Page:** Tab 0.

38. Canada (Minister of Citizenship and Immigration) v. Vavilov, 2019 SCC 65

Proposition: Judicial review is a constitutional guarantee; administrative decisions must be justified, transparent, and intelligible. **Relevance:** RCMP refusal to search a PIB lacks justification and transparency; supports correctness review on statutory interpretation. **Tab/Page:** Tab 0.

39. Yatar v. TD Insurance, 2024 ONCA 446

Proposition: Judicial review is not limited to rare or exceptional cases; courts cannot decline to hear JR applications. **Relevance:** Mandamus to compel a search is never premature; no alternative remedy exists. **Tab/Page:** Tab 0.

40. Keeprite Workers' Independent Union v. Keeprite Products Ltd., 1980 CanLII 1877 (ON CA)

Proposition: Judicial review is a record-based proceeding; affidavit evidence is limited to narrow exceptions. **Relevance:** Supports the Applicant's position that the RCMP's refusal to search prevents creation of a proper record. **Tab/Page:** Tab 0.

41. Beauregard v. Canada, [1986] 2 SCR 56

Proposition: Judicial independence is a constitutional imperative; courts must be insulated from executive interference. **Relevance:** RCMP refusals and registry irregularities engage the ACJ's constitutional oversight role. **Tab/Page:** Tab 0.

42. Valente v. The Queen, [1985] 2 SCR 673

Proposition: Judicial independence includes administrative independence and control over court processes. **Relevance:** Supports ACJ authority to direct registry functions and ensure proper docketing. **Tab/Page:** Tab 0.

43. MacKeigan v. Hickman, [1989] 2 SCR 796

Proposition: Courts control their own processes; executive actors cannot interfere with adjudicative functions. **Relevance:** Supports relief sought regarding registry mischaracterization and RCMP refusals. **Tab/Page:** Tab 0.

44. Girouard (duplicate reference)

Proposition: Reinforces Chief Justice's institutional oversight powers. **Relevance:** Supports self-assignment and supervisory jurisdiction. **Tab/Page:** Tab 0.

45. Dugré (duplicate reference)

Proposition: Confirms Chief Justice's authority to relieve or reassign judges not yet seized. **Relevance:** Supports previous assignment. **Tab/Page:** Tab 0.

901

C. RULE 317 / RULE 318 — CERTIFIED TRIBUNAL RECORD & RELEVANCE JURISPRUDENCE

46. Morgan v. Alta Flights Inc., 2006 FCA 121

Proposition: Administrative decisions must be grounded in evidence; reviewing courts must have access to the full record.

Relevance: RCMP refusal to search prevents creation of a proper evidentiary record.

Tab/Page: Tab 2.

47. Wyndowe v. Rousseau, 2008 FCA 39

Proposition: Reviewing courts must have access to the complete evidentiary foundation relied upon by the decision-maker.

Relevance: RCMP provided no CTR; judicial review cannot proceed without a record.

Tab/Page: Tab 2.

48. Englander v. TELUS Communications Inc., 2004 FCA 387

Proposition: Privacy rights require meaningful access to personal information.

Relevance: Supports Applicant's right to a meaningful search of a non-exempt PIB.

Tab/Page: Tab 2.

49. Lavigne v. Canada (Commissioner of Official Languages), 2002 SCC 53

Proposition: Access to personal information is quasi-constitutional; institutions must justify refusals.

Relevance: RCMP refusal to search requires statutory justification.

Tab/Page: Tab 2.

50. Dagg v. Canada (Minister of Finance), [1997] 2 SCR 403

Proposition: Privacy is a fundamental democratic value; access rights must be interpreted broadly.

Relevance: Supports broad interpretation of the Applicant's access rights under the Privacy Act.

Tab/Page: Tab 2.

51. Douze v. Canada (Citizenship and Immigration), 2010 FC 1086 (para 19)

902
Proposition: Relevance under Rule 317 is broad; documents are relevant if they “may affect the decision.”
Relevance: RCMP refusal to search deprives the Court of relevant material.
Tab/Page: Tab 2.

52. Boudreau v. Canada (Revenue Agency), 2022 FC 792 (para 16)

Proposition: Failure to conduct a reasonable search is unreasonable and reviewable.
Relevance: Directly analogous to RCMP refusal to search.
Tab/Page: Tab 2.

53. Canada (Human Rights Commission) v. Pathak, 1995 FCA

Proposition: Relevance for CTR production is whether the document “may affect the decision.”
Relevance: Supports broad Rule 317 disclosure obligations.
Tab/Page: Tab 2.

54. Chopra v. Canada (Public Safety), 2026 FC 18896 (para 10)

Proposition: Public safety agencies must comply with statutory duties; refusal to act is reviewable.
Relevance: RCMP refusal to search is reviewable.
Tab/Page: Tab 2.

55. John Doe 1 v. Canada (Attorney General), 2024 FC 1024

Proposition: Rule 317 relevance = whether the document “may affect the decision.”
Relevance: RCMP refusal to search deprives the Court of relevant material.
Tab/Page: Tab 2.

56. Abu v. Canada (Citizenship and Immigration), 2021 FC 1031

Proposition: In mandamus applications, relevance is broader because the “decision” is the refusal to act.
Relevance: RCMP refusal to search triggers expanded Rule 317 relevance.
Tab/Page: Tab 2.

57. Beniey v. Canada (CBSA), 2024 FC 972

Proposition: Rule 317 applies exclusively to judicial reviews under the Federal Courts Act.

Relevance: Confirms Rule 317 applies to this Privacy Act judicial review.

Tab/Page: Tab 2.

58. Lavigne v. Canada Post Corporation, 2009 FC 756 (para 16)

Proposition: Rule 317 cannot be invoked outside FCA judicial reviews.

Relevance: Confirms Rule 317 is properly invoked here.

Tab/Page: Tab 2.

59. Canadian Copyright Licensing Agency v. Alberta, 2015 FCA 268 (para 15)

Proposition: Rule 317 allows parties to confirm what the decision-maker actually considered.

Relevance: RCMP refusal to search prevents confirmation of what was considered.

Tab/Page: Tab 2.

60. Friends of the Earth Canada v. Canada (AG), 2023 FC 1438 (para 9)

Proposition: Rule 317 ensures meaningful judicial review.

Relevance: RCMP refusal to search undermines meaningful review.

Tab/Page: Tab 2.

61. GCT Canada LP v. Vancouver Fraser Port Authority, 2021 FC 624 (para 26)

Proposition: Disclosure must permit meaningful and substantive judicial review.

Relevance: RCMP refusal to search prevents meaningful review.

Tab/Page: Tab 2.

D. EXPANDED DISCLOSURE WHERE BIAS OR FAIRNESS IS ALLEGED

62. Air Passenger Rights v. Canada (Attorney General), 2021 FCA 201 (para 21)

Proposition: Where bias or procedural fairness is alleged, Rule 317 disclosure is broader; includes documents not before the decision-maker.

Relevance: RCMP's contradictory positions and refusals engage fairness concerns.

Tab/Page: Tab 2.

63. Humane Society of Canada Foundation v. Canada (National Revenue), 2018 FCA 66 (paras 5–6)

904
Proposition: Expanded disclosure is mandatory where fairness issues arise.

Relevance: Supports production of all RCMP internal correspondence.

Tab/Page: Tab 2.

64. Gagliano v. Canada (Commission of Inquiry), 2006 FC 720 (para 50), aff'd 2007 FCA 131

Proposition: Disclosure obligations expand where fairness or bias is alleged.

Relevance: RCMP's inconsistent positions trigger expanded disclosure.

Tab/Page: Tab 2.

65. Majeed v. Canada (MEI), 1997 FCTD, aff'd 1994 FCA

Proposition: Fairness allegations broaden the scope of required disclosure.

Relevance: Supports production of RCMP internal communications.

Tab/Page: Tab 2.

66. Ron W. Cameron Charitable Foundation v. Canada (National Revenue), 2023 FCA 175 (para 26)

Proposition: Bias or fairness allegations require production of all relevant documents, even if not before the decision-maker.

Relevance: RCMP's contradictory positions trigger expanded disclosure.

Tab/Page: Tab 2.

67. Delisle (Kannabis Shop) v. Kahnawake Cannabis Control Board, 2026 FC 14519 (para 13)

Proposition: Fairness allegations broaden Rule 317 obligations.

Relevance: Supports production of RCMP internal records.

Tab/Page: Tab 2.

68. Jewish National Fund of Canada Inc. v. Canada (National Revenue), 2025 FCA 114 (para 13)

Proposition: Expanded disclosure is mandatory where fairness is at issue.

Relevance: Supports Applicant's Rule 317 request.

Tab/Page: Tab 2.

E. PROCEDURAL REQUIREMENTS FOR RULE 317 REQUESTS

69. Wheeldon v. Canada (Attorney General), 2012 FC 355 (para 15)

905
Proposition: A formal written Rule 317 request is mandatory; failure to make one is fatal.

Relevance: Applicant made a formal Rule 317 request; RCMP refused to comply.

Tab/Page: Tab 2.

F. RULE 317 IN ATIA JUDICIAL REVIEWS

70. Preventous Collaborative Health v. Canada (Health), 2021 FC 253 (paras 11, 14–15, 26)

Proposition: Rule 317 applies to ATIA s. 44 reviews; correctness standard applies.

Relevance: RCMP refusal to search transforms the refusal into the “decision” under review.

Tab/Page: Tab 2.

F. ADDITIONAL ADMINISTRATIVE LAW, PRIVACY, AND DISCLOSURE AUTHORITIES (TAB 2)

71. Benedict v. Ontario, (2000) 51 O.R. (3d) 147 (C.A.)

Proposition: Administrative bodies must comply with statutory duties; failure to do so is reviewable.

Relevance: Supports reviewability of RCMP refusal to search a non-exempt PIB.

Tab/Page: Tab 2.

72. Office of the Privacy Commissioner of Canada — RCMP Suicide Disclosure Investigation (OPCC Report, 2016–17)

Proposition: The OPCC found that RCMP disclosure of sensitive personal information to U.S. authorities violated the *Privacy Act*.

Relevance: Demonstrates RCMP’s historical non-compliance with Privacy Act obligations; supports need for judicial oversight.

Tab/Page: Tab 2.

URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170419_rcmp/

73. Atlantic Prudence Maritime Inc. v. Canada (Minister of Transport), [1983] 2 FC 183 (FCA)

Proposition: Administrative refusals must be justified; failure to consider statutory criteria is reviewable.

Relevance: RCMP refusal to search lacks justification; supports mandamus.

Tab/Page: Tab 2, p. 49.

74. Canada (Attorney General) v. Cloutier, 2008 FC 322

906
Proposition: Administrative bodies must provide reasons that allow meaningful judicial review.

Relevance: RCMP provided no reasons for refusing to search.

Tab/Page: Tab 2, p. 49.

75. Canada (Information Commissioner) v. Minister of National Defence, 2011 SCC 25

Proposition: Duty to assist requires meaningful search efforts; institutions must justify refusals.

Relevance: RCMP refusal to search violates the duty to assist.

Tab/Page: Tab 2, p. 50.

76. Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration), 2003 FC 219

Proposition: Federal institutions must conduct reasonable searches and justify refusals.

Relevance: Supports reviewability of RCMP refusal to search.

Tab/Page: Tab 2.

77. Halton Regional Police Services Board (Re), 2024 CanLII 67092 (ON IPC)

Proposition: Police services must comply with access obligations; metadata and system logs are disclosable.

Relevance: Supports Applicant's right to foundational metadata from RCMP systems.

Tab/Page: Tab 2.

78. Canada Post Corp. v. Canada (Minister of Public Works), 1995 CanLII 3574 (FCA)

Proposition: Federal institutions cannot rely on internal policy to avoid statutory obligations.

Relevance: RCMP cannot rely on internal ATIP practices to avoid searching a PIB.

Tab/Page: Tab 2, p. 53.

79. MacFoy v. United Africa Co. Ltd., [1961] 3 All E.R. 1169 (P.C.)

Proposition: "You cannot put something on nothing and expect it to stand." A void act is a nullity.

Relevance: RCMP's refusal to search cannot be justified by reference to a non-existent or concluded investigation.

Tab/Page: Tab 2.

80. McInerney v. MacDonald, [1992] 2 SCR 138

907
Proposition: Individuals have a right to access their personal information; custodians must justify refusals.
Relevance: RCMP refusal to search requires statutory justification.
Tab/Page: Tab 2.

G. RULE 317 — RELEVANCE, CTR PRODUCTION, AND EXPANDED DISCLOSURE (TAB 2)

81. John Doe 1 v. Canada (Attorney General), 2024 FC 1024

Proposition: Relevance under Rule 317 = whether the document “may affect the decision.”
Relevance: RCMP refusal to search deprives the Court of relevant material.
Tab/Page: Tab 2.

82. Abu v. Canada (Citizenship and Immigration), 2021 FC 1031

Proposition: In mandamus applications, relevance is broader because the “decision” is the refusal to act.
Relevance: RCMP refusal to search triggers expanded Rule 317 relevance.
Tab/Page: Tab 2.

83. Beniey v. Canada (CBSA), 2024 FC 972

Proposition: Rule 317 applies exclusively to judicial reviews under the Federal Courts Act.
Relevance: Confirms Rule 317 applies to this Privacy Act judicial review.
Tab/Page: Tab 2.

84. Lavigne v. Canada Post Corporation, 2009 FC 756 (para 16)

Proposition: Rule 317 cannot be invoked outside FCA judicial reviews.
Relevance: Confirms Rule 317 is properly invoked here.
Tab/Page: Tab 2.

85. Canadian Copyright Licensing Agency v. Alberta, 2015 FCA 268 (para 15)

Proposition: Rule 317 allows parties to confirm what the decision-maker actually considered.
Relevance: RCMP refusal to search prevents confirmation of what was considered.
Tab/Page: Tab 2.

86. Friends of the Earth Canada v. Canada (AG), 2023 FC 1438 (para 9)

908

Proposition: Rule 317 ensures meaningful judicial review.

Relevance: RCMP refusal to search undermines meaningful review.

Tab/Page: Tab 2.

87. GCT Canada LP v. Vancouver Fraser Port Authority, 2021 FC 624 (para 26)

Proposition: Disclosure must permit meaningful and substantive judicial review.

Relevance: RCMP refusal to search prevents meaningful review.

Tab/Page: Tab 2.

88. Air Passenger Rights v. Canada (Attorney General), 2021 FCA 201 (para 21)

Proposition: Where bias or fairness is alleged, Rule 317 disclosure is broader; includes documents not before the decision-maker.

Relevance: RCMP's contradictory positions trigger expanded disclosure.

Tab/Page: Tab 2.

89. Humane Society of Canada Foundation v. Canada (National Revenue), 2018 FCA 66 (paras 5–6)

Proposition: Expanded disclosure is mandatory where fairness issues arise.

Relevance: Supports production of RCMP internal correspondence.

Tab/Page: Tab 2.

90. Gagliano v. Canada (Commission of Inquiry), 2006 FC 720 (para 50), aff'd 2007 FCA 131

Proposition: Disclosure obligations expand where fairness or bias is alleged.

Relevance: RCMP's inconsistent positions trigger expanded disclosure.

Tab/Page: Tab 2.

91. Majeed v. Canada (MEI), 1997 FCTD, aff'd 1994 FCA

Proposition: Fairness allegations broaden the scope of required disclosure.

Relevance: Supports production of RCMP internal communications.

Tab/Page: Tab 2.

92. Ron W. Cameron Charitable Foundation v. Canada (National Revenue), 2023 FCA 175 (para 26)

Proposition: Bias or fairness allegations require production of all relevant documents, even if not before the decision maker.

Relevance: RCMP's contradictory positions trigger expanded disclosure.

Tab/Page: Tab 2.

93. Delisle (Kannabis Shop) v. Kahnawake Cannabis Control Board, 2026 FC 14519 (para 13)

Proposition: Fairness allegations broaden Rule 317 obligations.

Relevance: Supports production of RCMP internal records.

Tab/Page: Tab 2.

94. Jewish National Fund of Canada Inc. v. Canada (National Revenue), 2025 FCA 114 (para 13)

Proposition: Expanded disclosure is mandatory where fairness is at issue.

Relevance: Supports Applicant's Rule 317 request.

Tab/Page: Tab 2.

95. Wheeldon v. Canada (Attorney General), 2012 FC 355 (para 15)

Proposition: A formal written Rule 317 request is mandatory; failure to make one is fatal.

Relevance: Applicant made a formal Rule 317 request; RCMP refused to comply.

Tab/Page: Tab 2.

96. Preventous Collaborative Health v. Canada (Health), 2021 FC 253 (paras 11, 14–15, 26)

Proposition: Rule 317 applies to ATIA s. 44 reviews; correctness standard applies.

Relevance: RCMP refusal to search transforms the refusal into the “decision” under review.

Tab/Page: Tab 2.

H. NULLITY DOCTRINE, PRIVACY ARCHITECTURE, AND STATUTORY RECORD-CREATION OBLIGATIONS (TAB 5)

97. Landreville v. Boucherville (Town of), [1978] 2 SCR 801

Proposition: The Supreme Court of Canada recognized a special class of **jurisdictional nullities** — including fraud, bribery, extortion, and bad faith — which “unravel everything they touch.”

Relevance: The RCMP's contradictory statutory positions, refusal to search a non-exempt PIB, and refusal to consider mandatory statutory criteria (s. 8(2)(m), s. 19 ATIA) fall within the category of **exceptional nullities** that invalidate the refusal ab initio.

Tab/Page: Tab 5, p. 125.

98. *McInerney v. MacDonald*, [1992] 2 SCR 138

Proposition: Access to one's own personal information is foundational to fairness, transparency, and the avoidance of unnecessary litigation. Privacy statutes must be interpreted harmoniously to facilitate access, not impede it.

Relevance: RCMP refusal to search a non-exempt PIB violates the core purpose of the Privacy Act and undermines the statutory architecture designed to prevent "floodgates" of litigation.

Tab/Page: Tab 5, p. 125.

99. Privacy Legislation Architecture (*McInerney*; *Dagg*; *Lavigne*)

Proposition: Canadian privacy statutes — federal and provincial — operate on a unified principle: individuals must be able to access their own personal information, including records that must be created to respond to a request.

Relevance: Supports the Applicant's right to:

- metadata,
- system logs,
- audit trails,
- routing information,
- and any record that must be created to fulfill the request.

Tab/Page: Tab 5, p. 125.

100. Statutory Duty to Create Records (*FOIPPA* / *Privacy Act* Analogy)

Proposition: Under statutes such as British Columbia's *Freedom of Information and Protection of Privacy Act*, "records" include documents that must be created to respond to a request, including software outputs, metadata, and system-generated logs.

Relevance: Supports the Applicant's entitlement to RCMP metadata and system-generated records necessary to complete the search.

Tab/Page: Tab 5, p. 125.

101. Statutory Duty to Avoid Floodgates (*McInerney*; *Dagg*)

Proposition: Privacy statutes are designed to prevent courts from being overwhelmed by disputes over access to personal information by ensuring that individuals can obtain their own information through statutory mechanisms.

Relevance: RCMP refusal to search forces the Applicant into litigation, contrary to the purpose of the Privacy Act.

Tab/Page: Tab 5, p. 125.

102. Harmonious Interpretation of Privacy Statutes (*McInerney*; *Dagg*; *Lavigne*)

911
Proposition: Privacy statutes must be interpreted harmoniously across jurisdictions to promote access, fairness, and transparency.

Relevance: Supports the Applicant's right to a complete search and disclosure of all responsive personal information.

Tab/Page: Tab 5, p. 125.

103. Creation of Programs, Applications, and Software Outputs (FOIPPA jurisprudence)

Proposition: Where necessary to respond to an access request, institutions must create:

- new records,
- new compilations,
- new software outputs,
- or new data extractions.

Relevance: RCMP must generate metadata, audit logs, and system-level outputs to complete the search.

Tab/Page: Tab 5, p. 125.

104. Principle of “Something on Nothing” — *MacFoy v. United Africa Co. Ltd.*, [1961] 3 All ER 1169 (PC)

Proposition: A void act is a nullity; “you cannot put something on nothing and expect it to stand.”

Relevance: RCMP refusal to search cannot be justified by reference to a non-existent or concluded investigation; the refusal collapses under its own weight.

Tab/Page: Tab 5.

I. CRIMINAL PROCEDURE, METADATA, NULLITY, AND CONSTITUTIONAL DISCLOSURE (TAB 7)

105. *R. v. Jordan*, 2016 SCC 27

Proposition: The Supreme Court established strict ceilings for the timely completion of criminal proceedings (18 months in provincial court). Delay beyond the ceiling presumptively violates s. 11(b) of the Charter.

Relevance: The Applicant's Privacy Act request (March 11, 2026) was made **within the Jordan window**, meaning the underlying criminal proceeding remained constitutionally alive for the purpose of challenging the validity of the judicial authorization. The RCMP's refusal to search obstructs the Applicant's ability to pursue Charter remedies.

Tab/Page: Tab 7, p. 169.

106. *Canada (Information Commissioner) v. Minister of National Defence*, 2011 SCC 25

Proposition: “Control” under federal access legislation includes **physical possession**, **systemic administration**, and **structural integration**. Institutions cannot disclaim control over records stored in shared or multi-jurisdictional systems.

Relevance: CPIC is federally hosted, federally administered, and federally controlled. The RCMP cannot disavow

912
metadata entered by municipal or provincial police. The RCMP has a **non-derogable obligation** to search and disclose the CPIC metadata fields requested.

Tab/Page: Tab 7, p. 170.

107. R. v. Garofoli, [1990] 2 SCR 1421

Proposition: An accused has an **absolute right** to challenge the validity of a judicial authorization. This right is meaningless without access to the underlying information and metadata that supported the authorization.

Relevance: The Applicant cannot challenge the validity of the warrant or authorization without the CPIC metadata. RCMP refusal to search renders the Garofoli right **illusory**.

Tab/Page: Tab 7.

108. Hunter v. Southam Inc., [1984] 2 SCR 145

Proposition: Section 8 of the Charter requires prior authorization based on reasonable and probable grounds; the integrity of the authorization process is constitutionally protected.

Relevance: Metadata is essential to determine whether the authorization was valid. Without it, the Applicant cannot pursue s. 24(2) remedies.

Tab/Page: Tab 7.

109. Irremediable Nullity Doctrine (Garofoli + Hunter + Landreville)

Proposition: Where the foundational act (e.g., warrant, authorization, or data entry) is tainted by fraud, illegality, or bad faith, the entire proceeding is a **nullity**.

Relevance: If the CPIC entry was falsified, the criminal proceeding was void ab initio. The Applicant requires the metadata to establish the nullity.

Tab/Page: Tab 7.

110. R. v. Stinchcombe, [1991] 3 SCR 326

Proposition: The Crown has a constitutional duty to disclose all relevant information to the defence.

Relevance: CPIC metadata is **first-party disclosure** under Stinchcombe. RCMP refusal to search obstructs constitutional disclosure rights.

Tab/Page: Tab 9, p. 195.

111. R. v. McNeil, 2009 SCC 3

Proposition: Police records relevant to the validity of the state's case must be disclosed, even if held by a different police force. The distinction between first-party and third-party records collapses where the police hold information relevant to the case.

Relevance: CPIC metadata is **McNeil-disclosable**. The RCMP cannot hide behind jurisdictional boundaries.

Tab/Page: Tab 9, p. 195.

913

112. *Chandler v. Alberta Association of Architects*, [1989] 2 SCR 848

Proposition: Once a judicial or administrative decision is issued, the decision-maker becomes **functus officio** — their jurisdiction is exhausted.

Relevance: The issuing justice became functus the moment the warrant was issued. Only the metadata can reveal whether the authorization was valid. RCMP refusal to search obstructs the Applicant's ability to challenge the authorization.

Tab/Page: Tab 9, p. 197.

J. INTEGRATION OF CRIMINAL PROCEDURE WITH PRIVACY ACT TIMING (TAB 7)

113. Timing Principle — Jordan Window + Privacy Act Request

Proposition: A Privacy Act request made during the Jordan window preserves the Applicant's ability to challenge the validity of the underlying criminal process.

Relevance: The Applicant's March 11, 2026 request was made **within the 18-month Jordan ceiling**, meaning the Applicant retained full constitutional rights to challenge the authorization. RCMP refusal to search obstructs those rights.

Tab/Page: Tab 7.

K. CONSTITUTIONAL DISCLOSURE, POLICE RECORDS, AND FUNCTUS OFFICIO (TAB 9)

114. *R. v. Stinchcombe*, [1991] 3 SCR 326

Proposition: The Crown has a constitutional duty to disclose all relevant information to the defence, including information in the possession of police forces. Disclosure is not optional; it is a constitutional imperative grounded in the right to make full answer and defence.

Relevance:

- CPIC metadata is **first-party disclosure** under *Stinchcombe*.
- The RCMP cannot refuse to search or disclose metadata that is constitutionally required to challenge the validity of the state's case.
- The refusal to search obstructs the Applicant's ability to pursue Charter remedies.

Tab/Page: Tab 9, p. 195.

115. *R. v. McNeil*, 2009 SCC 3

Proposition: Police records relevant to the validity of the state's case must be disclosed, even if held by a different police force. The distinction between "first-party" and "third-party" records collapses where the police hold information relevant to the case.

Relevance:

- CPIC is a **federal database**, but *McNeil* makes clear that jurisdictional boundaries do not shield police records from disclosure.
 - If CPIC metadata underpins the validity of the original criminal process, the RCMP must disclose it.
 - The RCMP cannot rely on “we are not the prosecuting Crown” to avoid disclosure.
- Tab/Page:** Tab 9, p. 195.

116. Chandler v. Alberta Association of Architects, [1989] 2 SCR 848

Proposition: Once a judicial or administrative decision is issued, the decision-maker becomes **functus officio** — their jurisdiction is exhausted and cannot be revived.

Relevance:

- The issuing justice became functus the moment the warrant was issued.
- Only the **metadata** can reveal whether the authorization was valid.
- RCMP refusal to search obstructs the Applicant’s ability to challenge the authorization, because the issuing justice cannot revisit or clarify the authorization.
- This makes the metadata **the only remaining source of truth**.

Tab/Page: Tab 9, p. 197.

L. INTEGRATION OF STINCHCOMBE, MCNEIL, AND CHANDLER INTO THE PRIVACY ACT FRAMEWORK (TAB 9)

117. Constitutional Disclosure + Privacy Act Timing Principle

Proposition: When a Privacy Act request is made during the period in which a criminal proceeding remains constitutionally alive (e.g., within the *Jordan* ceiling), the requester retains full constitutional rights to challenge the validity of the underlying process.

Relevance:

- The Applicant’s Privacy Act request (March 11, 2026) was made **within the 18-month Jordan window**.
- The Applicant therefore retained full rights to:
 - challenge the warrant,
 - seek exclusion of evidence under s. 24(2),
 - pursue prerogative writs (certiorari, mandamus),
 - and obtain disclosure under *Stinchcombe* and *McNeil*.
- RCMP refusal to search obstructs these constitutional rights.

Tab/Page: Tab 9.

118. Collapse of First-Party / Third-Party Distinctions (McNeil + Stinchcombe)

Proposition: When police records are relevant to the validity of the state’s case, they are treated as **first-party disclosure**, regardless of which police force holds them.

Relevance:

- CPIC metadata is **first-party disclosure** because it underpins the validity of the original criminal process.

119. Metadata as Foundational Evidence (Garofoli + Hunter + McNeil)

Proposition: Metadata is not peripheral — it is **foundational evidence** that determines whether a judicial authorization was valid.

Relevance:

- Without metadata, the Applicant cannot challenge the authorization under *Garofoli*.
- Without metadata, the Applicant cannot pursue s. 24(2) remedies under *Hunter v. Southam*.
- RCMP refusal to search renders constitutional rights **illusory**.

Tab/Page: Tab 9.

M. PUBLIC INTEREST DISCLOSURE, S. 8(2)(M)(I), TRANSPARENCY, AND CONSTITUTIONAL STAKES (TAB 10)

120. Canadian Broadcasting Corporation v. Canada (Parole Board), 2023 FCA 161

Proposition:

The Federal Court of Appeal held that administrative bodies must conduct a **meticulous, case-specific weighing of interests** under s. 8(2)(m)(i) of the *Privacy Act*. Blanket policies, categorical refusals, or generic invocations of “law enforcement” are **unlawful**. The requester’s **motive** is relevant where the statute expressly requires a public-interest balancing.

Relevance:

- The RCMP cannot apply a blanket “law enforcement” exemption to CPIC metadata.
- The Applicant’s motive — exposing algorithmic forgery, ensuring transparency, and protecting the integrity of the court record — is **directly relevant** under s. 8(2)(m)(i).
- The Applicant has already commenced constitutional litigation (Form 1, Form 5, Form 22), engaging the **primary law officers of the Crown**, elevating the public interest to the highest possible level.
- The RCMP’s refusal to consider s. 8(2)(m)(i) is a **reviewable error of law**.

Tab/Page: Tab 10, p. 256–260.

121. Attaran v. Canada (National Defence), 2011 FC 334

Proposition:

The Federal Court recognized that the public has a **fundamental democratic right** to scrutinize the mechanisms of state coercion, especially where liberty is at stake. Transparency is heightened where the state detains, restrains, or exercises coercive power.

Relevance:

- If transparency is required for the *treatment* of detainees, it is a **fortiori** required for the **validity of the mechanism that authorizes detention**.

Algorithmic spoliation of a warrant is a direct assault on s. 7 and s. 8 Charter rights.

- The public interest in exposing forged or corrupted judicial authorizations is overwhelming.
- RCMP refusal to search obstructs the Applicant's ability to challenge the legality of the detention mechanism itself.

Tab/Page: Tab 10, p. 260–262.

122. Pinaymootang First Nation v. Canada (Minister of Health), 2009 FC 275

Proposition:

The Federal Court held that the **structural integrity and transparency** of federal programs can outweigh individual privacy concerns. Public interest in systemic accountability may override privacy where the program affects the public at large.

Relevance:

- CPIC is the **most consequential federal program** in the criminal justice system.
- The public has an overriding interest in verifying whether CPIC has been compromised by irregular, unsworn, or falsified entries.
- The potential for retroactive manipulation of digital records creates a **systemic threat** to the rule of law.
- RCMP refusal to search prevents the public from verifying the integrity of CPIC.

Tab/Page: Tab 10, p. 262–264.

123. Bangladesh v. Canada (Attorney General), 2019 FC 399

Proposition:

The Federal Court held that s. 8(2)(m)(i) does not create a **stand-alone coercive right** for a third-party requester to compel disclosure via mandamus. The institution must still conduct a case-specific weighing.

Relevance:

- The Applicant is **not** a third-party requester — he is the **data subject**.
- Bangladesh does **not** apply where the requester seeks **their own personal information**.
- Even under Bangladesh, the Head of the Institution must still:
 - conduct a case-specific weighing,
 - consider the public interest,
 - and provide reasons.
- The RCMP did **none** of these things.
- A refusal to consider overwhelming evidence of algorithmic forgery would be **unreasonable, unfair, and contrary to the purpose of s. 8(2)(m)(i)**.

Tab/Page: Tab 10, p. 264–266.

917

124. Public Interest Motive (CBC FCA 2023)**Proposition:**

Under s. 8(2)(m)(i), the requester's motive is relevant where the public interest is engaged.

Relevance:

- The Applicant's motive is not curiosity — it is **constitutional litigation**.
 - The Applicant seeks to expose algorithmic forgery of a judicial authorization.
 - This is the highest possible public interest.
-

125. Transparency in State Coercion (Attaran)**Proposition:**

The public has a right to scrutinize how the state exercises coercive power.

Relevance:

- The Applicant seeks to scrutinize the **validity of the mechanism** that authorized his detention.
 - This is more fundamental than detainee treatment.
-

126. Structural Integrity of Federal Programs (Pinaymootang)**Proposition:**

Where a federal program affects the public at large, transparency may override privacy.

Relevance:

- CPIC integrity affects every Canadian.
 - The risk of forged or manipulated entries is a systemic threat.
-

127. Limits of Bangladesh (Data Subject vs. Third Party)**Proposition:**

Bangladesh restricts third-party coercive rights — not the rights of data subjects.

Relevance:

- The Applicant is the **data subject**.
 - Bangladesh does not apply.
 - The RCMP must conduct a **full s. 8(2)(m)(i) analysis**.
-

Proposition:

Let justice be done though the heavens fall — the principle that truth and legality must prevail even at institutional cost.

Relevance:

- The Applicant's request is a truth-seeking exercise.
- The RCMP cannot shield algorithmic forgery behind administrative refusal.

R. PRIVACY, PUBLIC DOMAIN, AND THE ABSENCE OF A PRIVACY INTEREST IN JUDICIAL OR INSTITUTIONAL METADATA (TAB 10, P. 415)

132. Merriam-Webster Dictionary — Definition of “Invasion of Privacy”

Proposition: “Invasion of privacy” is defined as “*a situation in which someone tries to get information about a person's private life in an unwanted and usually improper way.*” This definition presupposes:

- a **private**,
- **personal**,
- **non-public** domain.

Relevance:

- Federally appointed judges, police officers, and public officials **do not possess a private domain** when performing public duties.
- Judicial metadata, CPIC entries, routing logs, and system-level acts are **public-function data**, not personal information.
- There is **no possible invasion of privacy** when the request concerns:
 - the Applicant's own personal information,
 - the identity of public officials acting in their public capacity,
 - or metadata documenting the execution of judicial functions.

This aligns with:

- **Dagg v. Canada (Minister of Finance)**, [1997] 2 SCR 403
- **Lavigne v. Canada (Commissioner of Official Languages)**, 2002 SCC 53
- **Englander v. TELUS Communications Inc.**, 2004 FCA 387
- **Morgan v. Alta Flights Inc.**, 2006 FCA 121

All of which hold that **metadata linked to an identifiable individual is their personal information**, and that **public officials acting in public roles have diminished privacy expectations**.

Tab/Page: Tab 10, p. 415.

133. Jane Doe v. Metropolitan Toronto (Municipality) Commissioners of Police (1980s Sexual Assault Duty-to-Warn Jurisprudence)

Proposition: Police owe a **common-law duty to warn** identifiable individuals — and in some cases the public — when they possess information indicating a foreseeable risk of serious harm. The duty arises where:

1. the police have **exclusive knowledge** of a danger;
2. the danger is **foreseeable**;
3. the potential victim(s) are **identifiable** or part of a defined class;
4. the harm is **serious**;
5. the warning can be given **without compromising legitimate law-enforcement objectives**.

Relevance: This is the **single most devastating public-safety argument** in the Applicant entire Motion Record.

The RCMP is the **exclusive custodian** of CPIC. The RCMP alone knows:

- that judicial data can be falsified,
- that fictitious judges can be inserted,
- that warrants can be algorithmically altered,
- that Information Packages can be corrupted,
- that metadata can be manipulated,
- that audit trails are missing,
- that alerts do not exist.

This creates a **foreseeable risk** that:

- innocent individuals may be unlawfully arrested,
- unlawfully detained,
- unlawfully incarcerated,
- or harmed in custody.

The class of potential victims is **identifiable**:

- anyone whose name appears in CPIC,
- anyone subject to a warrant,
- anyone processed through the SCJ or OCJ digital intake systems.

The harm is **grave**:

- unlawful arrest,
- unlawful detention,
- bodily harm,
- death in custody.

The RCMP's refusal to warn — or even search — violates the **duty to warn**.

Tab/Page: Tab 10, pp. 416–420.

134. Baker v. Canada (Minister of Citizenship and Immigration), [1999] 2 SCR 817 (para 22)**Proposition:**

The Supreme Court held that where statutes or policy instruments create procedural expectations — including duties to assist, duties to communicate, or duties to process — the decision-maker must comply. Failure to follow established statutory obligations violates **procedural fairness**.

Relevance:

- The Privacy Act and ATIA impose a **mandatory Duty to Assist**.
- The RCMP cannot refuse to search for the four discrete metadata fields.
- The RCMP cannot delay, stonewall, or ignore the request.
- The RCMP must provide **immediate assistance** with the retrievable elements.
- Failure to do so violates **legitimate expectations** and **procedural fairness**.

Tab/Page: Tab 10, p. 415.

135. Fontaine v. Canada (Royal Canadian Mounted Police), 2007 FC 1022**Proposition:**

The Federal Court held that institutions are **not required** to seek individualized consent from every potentially affected person before applying the public-interest override. Consent-gathering cannot be used as a **stalling tactic**.

Relevance:

- The RCMP cannot delay disclosure by claiming it must “seek consent” from judges, police, or other actors.
- The RCMP must conduct a **broad-stroke public-interest assessment**.
- The RCMP cannot use “consent” as a shield to avoid disclosing systemic metadata.

Tab/Page: Tab 10.

136. Mandatory Duty to Consider s. 8(2)(m)(i) — Public Interest Override**Proposition:**

The Head of the Institution must **actively consider** the public-interest override. A blanket refusal to consider s. 8(2)(m)(i) is a **jurisdictional error**.

Relevance:

- The RCMP refused to consider s. 8(2)(m)(i). This is a **Vavilov-level error** (failure to exercise discretion). The RCMP must weigh:
 - systemic forgery,
 - algorithmic manipulation,
 - judicial integrity,
 - public safety,
 - and constitutional rights.

Tab/Page: Tab 10.

137. Digital-Era Interpretation of Privacy Statutes

Proposition:

Privacy statutes enacted in the 1980s must be interpreted as **living instruments** capable of addressing digital metadata, algorithmic audit trails, and cryptographic identifiers.

Relevance:

- The “clearly outweighs” test must be applied in the context of **21st-century digital coercion**.
- The public interest in exposing forged digital warrants is overwhelming.
- The RCMP cannot apply 1983 paper-era logic to 2026 digital-era metadata.

Tab/Page: Tab 10.

138. Canada (Information Commissioner) v. Canada (Commissioner of the RCMP), 2003 SCC 8

Proposition:

The RCMP cannot use privacy exemptions to shield **internal systemic or operational failings**. The Court rejected attempts to hide institutional problems behind privacy claims.

Relevance:

- The RCMP cannot hide CPIC vulnerabilities behind s. 19 ATIA or s. 8(2)(m).
- The RCMP cannot shield algorithmic forgery behind privacy exemptions.
- Systemic metadata is not protected personal information.

Tab/Page: Tab 10.

139. Bland v. Canada (National Capital Commission), 3 FC 325

Proposition:

Institutions must reasonably exercise discretion when applying exemptions. Blanket refusals are unlawful.

Relevance:

- The RCMP's blanket refusal to consider s. 8(2)(m) is unreasonable.
- The RCMP's blanket refusal to search is unreasonable.
- The RCMP's blanket refusal to process is unreasonable.

Tab/Page: Tab 10.

140. Rubin v. Canada (Minister of Health), 2003 FCA 37

Proposition:

Discretion must be exercised **in good faith, based on evidence, and in accordance with statutory purpose.**

Relevance:

- The RCMP exercised **no discretion.**
- The RCMP provided **no evidence.**
- The RCMP acted **contrary to statutory purpose.**
- This is a **jurisdictional error** requiring mandamus.

Tab/Page: Tab 10.

141. Frémy v. Canada, 2022 FC 750

Proposition: Administrative silence is not neutral. Under s. 37 of the RCMP Act, silence can constitute **unreasonable administrative conduct**, and adverse inferences may be drawn where the RCMP refuses to respond to a lawful request.

Relevance:

- The RCMP's refusal to search is an **active decision**, not passive delay.
- Silence = denial = unreasonableness.
- The Federal Court may infer that the RCMP **lacks valid judicial authorization** for the data they refuse to search.
- This supports mandamus and prohibition.

Tab/Page: Tab 13, p. 410.

142. Herrera-Morales v. Canada, 2016 FC 578

Proposition: Section 37 RCMP Act duties are directly relevant to evaluating **procedural fairness** and **reasonableness** in administrative conduct.

Relevance:

- The RCMP's refusal to search violates s. 37 duties:
 - (a) respect rights,
 - (b) uphold integrity of law,
 - (c) act diligently,
 - (e) not conceal unlawful conduct,
 - (h) sustain honour of the Force.
- The refusal to search is a breach of statutory duty.

143. Section 37, RCMP Act (Statutory Duties of Members)

Proposition: Section 37 imposes **strict, mandatory duties** on RCMP members, including:

- respect rights,
- uphold integrity of law,
- act diligently,
- avoid conflicts,
- ensure improper conduct is not concealed,
- remain incorruptible,
- sustain honour of the Force.

Relevance:

- Refusing to search for CPIC metadata violates **every one** of these duties.
- Concealing forged judicial data violates s. 37(e).
- Failing to act diligently violates s. 37(c).
- Failing to respect rights violates s. 37(a).
- This is not a discretionary matter — it is a **statutory breach**.

Tab/Page: Tab 13.

144. R. v. Campbell, [1999] 1 SCR 565

Proposition: The RCMP is **not** an agent of the Crown when enforcing the law; it is an **independent public office** bound by statute. The RCMP has **no immunity** for illegal acts. The RCMP cannot commit crimes, breach the Constitution, or act unlawfully in pursuit of law enforcement objectives.

Relevance:

- Forging judicial data is ultra vires.
- Concealing forged data is ultra vires.
- Refusing to search for forged data is ultra vires.
- Campbell destroys any argument that the RCMP can hide behind “operational discretion.”

Tab/Page: Tab 13, p. 16.

145. Bigeagle v. Canada, 2023 FCA 128

Proposition: Section 37 does not create a private tort duty of care, but it **does** create enforceable statutory duties in administrative contexts.

Relevance:

- You are not suing in tort.
- You are invoking s. 37 in an **administrative law** context.
- This is exactly what Bigeagle authorizes.

Tab/Page: Tab 13.

146. Jones v. Canada, 2018 NBCA 86

924

Proposition: Section 37 duties are enforceable in administrative review, even though they do not create private tort liability.

Relevance:

- Supports the Applicant use of s. 37 as a **reviewability anchor**.
- The RCMP's refusal to search violates s. 37.

Tab/Page: Tab 13.

147. Nelles v. Ontario, [1989] 2 SCR 170

Proposition: Absolute immunity does not exist for malicious prosecution or for acts committed with deliberate malice or outside lawful authority.

Relevance:

- Forging judicial data is outside lawful authority.
- Concealing forged data is outside lawful authority.
- Refusing to search for forged data is outside lawful authority.
- Nelles destroys any RCMP claim of immunity.

Tab/Page: Tab 13.

148. Irvine v. Canada (AG), 2025 FC 1673

Proposition: The RCMP Act provides robust internal mechanisms for discipline and oversight.

Relevance:

- The RCMP cannot claim “no mechanism exists” to address misconduct.
- The RCMP has internal tools to address forged data — they simply refused to use them.

Tab/Page: Tab 13.

149. Turner v. Canada (AG), 2025 FC 72

Proposition: Suspension under s. 12 RCMP Act is routine and widely used for serious misconduct.

Relevance:

- RCMP members involved in forged judicial data could be suspended.
- The RCMP's refusal to act is not due to lack of authority — it is due to lack of will.

Tab/Page: Tab 13.

150. Dawe v. Canada, 2002 FCT 486

Proposition: RCMP employment is governed entirely by statute, not contract.

925
Relevance:

- RCMP members are bound by statutory duties, not private employment discretion.
- They cannot refuse to search based on “internal policy.”

Tab/Page: Tab 13.

151. Grant v. Canada (AG), 1994 CanLII 9274 & 3507

Proposition: The RCMP Act has evolved to impose strict statutory obligations on members.

Relevance:

- The refusal to search violates the modern RCMP Act framework.
- The RCMP cannot rely on outdated interpretations of their authority.

Tab/Page: Tab 13.

V. INSTITUTIONAL ACCOUNTABILITY, JUDICIAL INTEGRITY, PRIVACY, AND ADMINISTRATIVE ILLEGALITY (TAB 13)

152. Aune v. Canada (Attorney General), 2013 BCSC 178

Proposition: Courts may scrutinize the conduct of police and Crown actors where administrative or investigative misconduct undermines the integrity of judicial processes.

Relevance:

- Supports judicial review of RCMP administrative misconduct.
- Reinforces that courts must intervene where institutional actors compromise justice.

153. Canada (AG) v. British Columbia Civil Liberties Association, 2021 SCC 30

Proposition: The Supreme Court reaffirmed that state actors must act within lawful authority and cannot rely on secrecy or institutional opacity to shield unlawful conduct.

Relevance:

- RCMP cannot hide forged judicial data behind privacy or secrecy.
- Transparency is constitutionally required where liberty is at stake.

154. Frémy v. Canada (AG), 2018 FC 434

Proposition: Administrative silence is reviewable and may constitute unreasonable conduct.

Relevance:

- Peggs' silence is an administrative decision.
- Adverse inferences must be drawn.

926

155. R. v. Baldovi, 2016 MBQB 90

Proposition: Police credibility collapses where documentary irregularities undermine the integrity of judicial authorizations.

Relevance:

- Supports the Applicant argument that forged or irregular judicial data destroys the validity of the Information Package.

156. R. v. Edwards, [1996] 1 SCR 128

Proposition: Reasonable expectation of privacy depends on control, access, and legitimacy of the underlying information.

Relevance:

- There is **no privacy interest** in forged judicial data.
- There is **no privacy interest** in CPIC metadata.

157. R. v. Gill, 2003 BCCA 671

Proposition: Police cannot rely on defective warrants or irregular judicial authorizations.

Relevance:

- If the warrant was forged or altered, it is a nullity.
- RCMP refusal to search obstructs the ability to prove this.

158. R. v. Tessling, 2004 SCC 67

Proposition: Privacy analysis depends on the nature of the information and the context of state power.

Relevance:

- CPIC metadata is **not private**.
- It is state-generated, state-controlled, and state-used.

159. Sherman Estate v. Peters, 2021 SCC 25

Proposition: The open-court principle is foundational; privacy yields to transparency where judicial integrity is at stake.

Relevance:

- Judicial metadata cannot be concealed.
- The public has a right to know whether judicial authorizations are valid.

Proposition: Open courts require transparency in judicial processes, including warrants and authorizations.

Relevance:

- Supports disclosure of the issuing judge’s identity.
- Supports disclosure of the narrative/remarks field.
- Supports disclosure of the CPIC metadata.

161. Actus non facit reum nisi mens sit rea

The act does not make one guilty unless the mind is guilty. **Relevance:** Forging judicial data is not an accident — it requires intent. The metadata will reveal that intent.

162. Boni iudicis est ampliare jurisdictionem

It is the part of a good judge to enlarge his jurisdiction (in the remedial sense). **Relevance:** The Federal Court is empowered — indeed obligated — to craft **structural remedies** where systemic illegality is shown (Doucet-Boudreau; Little Sisters).

163. Certum est quod certum reddi potest

That is certain which can be made certain. **Relevance:** The four metadata fields (ORI, Issuing Authority, Narrative, SID) make the forged acta **certain**. The RCMP cannot refuse to search.

164. Commodum ex injuria sua nemo habere debet

No one may profit from their own wrong. **Relevance:** The RCMP cannot rely on privacy exemptions to conceal forged judicial data.

165. Coram non iudice

Not before a judge. **Relevance:** If the issuing judge was fictitious or unauthorized, the entire proceeding was **coram non iudice** — a nullity.

166. Delegatus non potest delegare

A delegate cannot further delegate. **Relevance:** The RCMP cannot delegate its statutory duty to search to “policy,” “IT limitations,” or “other agencies.”

167. Ex dolo malo non oritur actio

No right of action arises from fraud. **Relevance:** A forged warrant cannot justify arrest, detention, or prosecution.

168. Expressio unius est exclusio alterius

The express mention of one thing excludes the other. **Relevance:** The Privacy Act expressly allows disclosure under s. 8(2)(m). The RCMP cannot invent new exemptions.

169. Falsus in uno, falsus in omnibus

928

False in one thing, false in everything. **Relevance:** If one part of the Information Package is forged, the entire package collapses.

170. Fraus est celare fraudem

It is a fraud to conceal a fraud. **Relevance:** The RCMP's refusal to search is itself evidence of concealment.

171. Ignorantia juris non excusat

Ignorance of the law excuses not. **Relevance:** The RCMP cannot claim ignorance of its statutory duties.

172. In eo quod plus sit semper inest et minus

The greater includes the lesser. **Relevance:** If the RCMP can run complex CPIC searches, it can certainly retrieve four metadata fields.

173. Lex non cogit ad impossibilia

The law does not compel the impossible. **Relevance:** The RCMP cannot claim it is "impossible" to search a non-exempt PIB that it controls.

174. Nemo dat quod non habet

No one can give what they do not have. **Relevance:** If the RCMP cannot produce the metadata, it means the metadata never existed — proving the acta was forged.

175. Omnia praesumuntur legitime facta donec probetur in contrarium

Acts are presumed lawful until the contrary is proved. **Relevance:** The metadata is the only mechanism to rebut the presumption of regularity.

176. Quando aliquid prohibetur ex directo, prohibetur et per obliquum

What is prohibited directly is prohibited indirectly. **Relevance:** If the RCMP cannot refuse disclosure directly, it cannot refuse disclosure by refusing to search.

177. Quando lex aliquid alicui concedit, concedere videtur et id sine quo res ipsa esse non potest

When the law grants something, it grants the means to achieve it. **Relevance:** The right to access personal information includes the right to have the RCMP **search** for it.

178. Qui non prohibet quod prohibere potest assentire videtur

He who does not prevent what he can prevent is deemed to consent. **Relevance:** Peggs' silence = assent to the forged acta.

179. Quod ab initio non valet, in tractu temporis non conualescit

929 *What is void from the beginning cannot be cured by time.* **Relevance:** A forged warrant is void ab initio — it cannot be “saved” by delay, silence, or subsequent proceedings.

180. Respondeat superior

Let the master answer. **Relevance:** The RCMP is institutionally responsible for CPIC integrity.

181. Salus populi suprema lex esto

The welfare of the people is the supreme law. **Relevance:** Public safety requires disclosure of systemic vulnerabilities in CPIC.

182. Spoliatus debet ante omnia restitui

One who has been despoiled must first be restored. **Relevance:** You must be restored to the position you were in before the forged acta.

183. Ubi inanis est verborum proprietas, ibi nulla est legis fortitudo

Where the meaning of words is empty, the law has no force. **Relevance:** The RCMP’s “privacy” arguments are empty — and therefore legally powerless.

184. Ubi jus ibi remedium

Where there is a right, there is a remedy. **Relevance:** The Applicant right to the Applicant personal information requires a judicial remedy — mandamus and prohibition.

185. Verba generalia restringuntur ad habilitatem rei vel personae

General words are restrained to the fitness of the matter or person. **Relevance:** General privacy exemptions cannot override the specific right to access the Applicant own metadata.

186. Ministry of the Attorney General (Ontario), Court Services Division — *Court Information Access Guide* (2019)

Proposition: This Guide confirms that:

- judicial authorizations,
- Informations,
- warrants,
- and related court documents

are **publicly accessible records**, subject only to minimal administrative fees under the *Administration of Justice Act*.

Relevance:

- Judges have **no reasonable expectation of privacy** in their judicial acts.
- The identity of the issuing judge is **not private information**.
- The public is entitled to access warrants and Informations.
- Therefore, the RCMP cannot rely on privacy exemptions to conceal:

- the Issuing Authority field,
- the Narrative/Remarks field,
- the ORI,
- or the SID.

This source **obliterates** the RCMP’s privacy-based excuses.

187. Forensic Report: “CL (M) – Forensic Manipulation.docx” (re: GrapeCity Documents for PDF API, v6.0.2.0)

Proposition: This forensic analysis demonstrates that the Information Package was manipulated using **GrapeCity Documents for PDF API**, version 6.0.2.0 — a commercial PDF editing suite capable of:

- flattening layers,
- overwriting metadata,
- altering timestamps,
- modifying embedded fonts,
- and removing audit trails.

Relevance:

- Confirms the **algorithmic forgery** of the Information Package.
- Confirms the **post-entry manipulation** of judicial data.
- Confirms the **absence of audit trails** is not accidental — it is the result of deliberate flattening.
- Confirms the **necessity** of retrieving the four CPIC metadata fields (ORI, Issuing Authority, Narrative, SID).
- Confirms the RCMP’s refusal to search is an attempt to conceal the manipulation.

This is the **technical smoking gun**.

188. RCMP Press Release (March 24, 2026): Launch of Counter-Terrorism Security Unit (CTSU)

Proposition: The RCMP publicly announced the creation of a specialized unit dedicated to:

- digital forensics,
- cyber-integrity,
- metadata analysis,
- and counter-manipulation of federal systems.

Relevance:

- The RCMP **cannot claim technical inability** to search CPIC metadata.
- The RCMP **cannot claim lack of resources**.
- The RCMP **cannot claim lack of expertise**.
- The RCMP **cannot claim that searching for ORI, Issuing Authority, Narrative, or SID is “impossible.”**
- The RCMP has a **dedicated unit** whose mandate includes exactly this type of forensic analysis.

This destroys the RCMP’s “technical limitation” argument.

186. Ministry of the Attorney General (Ontario), Court Services Division — *Court Information Access Guide* (2019)

Proposition: This Guide confirms that:

- judicial authorizations,
- Informations,
- warrants,
- and related court documents

are **publicly accessible records**, subject only to minimal administrative fees under the *Administration of Justice Act*.

Relevance:

- Judges have **no reasonable expectation of privacy** in their judicial acts.
- The identity of the issuing judge is **not private information**.
- The public is entitled to access warrants and Informations.
- Therefore, the RCMP cannot rely on privacy exemptions to conceal:
 - the Issuing Authority field,
 - the Narrative/Remarks field,
 - the ORI,
 - or the SID.

This source **obliterates** the RCMP's privacy-based excuses.

187. FORENSIC REPORT: "CL (M) – FORENSIC MANIPULATION.DOCX" (RE: GRAPECITY DOCUMENTS FOR PDF API, V6.0.2.0)

Proposition: This forensic analysis demonstrates that the Information Package was manipulated using **GrapeCity Documents for PDF API**, version 6.0.2.0 — a commercial PDF editing suite capable of:

- flattening layers,
- overwriting metadata,
- altering timestamps,
- modifying embedded fonts,
- and removing audit trails.

Relevance:

- Confirms the **algorithmic forgery** of the Information Package.
- Confirms the **post-entry manipulation** of judicial data.
- Confirms the **absence of audit trails** is not accidental — it is the result of deliberate flattening.
- Confirms the **necessity** of retrieving the four CPIC metadata fields (ORI, Issuing Authority, Narrative, SID).
- Confirms the RCMP's refusal to search is an attempt to conceal the manipulation.

This is the **technical smoking gun**.

188. RCMP Press Release (March 24, 2026): Launch of Counter-Terrorism Security Unit (CTSU)

932

Proposition: The RCMP publicly announced the creation of a specialized unit dedicated to:

- digital forensics,
- cyber-integrity,
- metadata analysis,
- and counter-manipulation of federal systems.

Relevance:

- The RCMP **cannot claim technical inability** to search CPIC metadata.
- The RCMP **cannot claim lack of resources**.
- The RCMP **cannot claim lack of expertise**.
- The RCMP **cannot claim that searching for ORI, Issuing Authority, Narrative, or SID is “impossible.”**
- The RCMP has a **dedicated unit** whose mandate includes exactly this type of forensic analysis.

This destroys the RCMP’s “technical limitation” argument.

Y. UNLAWFUL DETENTION, ADMINISTRATIVE SILENCE, AND JUDICIAL METADATA (TAB 14)

189. R. v. Gill, 2003 BCCA 671

Proposition: The British Columbia Court of Appeal held that a **failure by police to seek mandatory judicial extensions under s. 490 of the Criminal Code** constitutes a **serious breach of s. 8 of the Charter**. Administrative silence = unconstitutional continuation of detention.

Relevance:

- Peggs’ refusal to respond to the Applicant property-retrieval request is not “delay.”
- It is an **unauthorized continuation of detention** of the Applicant seized property.
- This is a **Charter breach**, not an administrative inconvenience.
- The RCMP’s silence must be interpreted as:
 - bypassing judicial oversight,
 - continuing detention without authority,
 - and creating an **actionable nullity**.

Tab/Page: Tab 14, p. 445.

190. Public Statement by Assistant Commissioner Matt Peggs (TPS/INSET Collaboration Press Release)

Proposition: Assistant Commissioner Peggs publicly confirmed his role as **Regional Commander, Federal Policing – Central Region**, responsible for RCMP operations in Toronto and the GTA.

Relevance:

- Peggs’ jurisdiction includes Toronto West and Toronto East — the exact regions implicated in the Application.
- His public statement confirms his operational authority over:
 - CPIC entries,

- federal policing in Toronto,
- INSET collaboration,
- and national-security-related metadata.
- His silence in the applicant case is therefore not peripheral — it is **institutional silence from the highest regional authority**.
- This strengthens the inference that Peggs may have been the **Informant** whose Information was accepted by the Chief Justice of the SCJ.

Tab/Page: Tab 14.

191. Ministry of the Attorney General (Ontario), Court Services Division — *Court Information Access Guide* (2019)

Proposition: The Guide confirms that:

- Informations,
- Indictments,
- Judicial Interim Release documents,
- and related judicial records

are **publicly accessible** to the accused **without fees**.

Relevance:

- Judicial metadata (judge’s name, court level, narrative) is **not private**.
- The RCMP cannot rely on privacy exemptions to conceal:
 - the Issuing Authority field,
 - the Narrative/Remarks field,
 - the ORI,
 - or the SID.
- The RCMP’s refusal to search is not based on privacy — it is based on **concealment**.

Tab/Page: Tab 14.

192. Ministry of the Attorney General (Ontario), Court Services Division — *Court Information Access Guide* (2019), s. 7.3.1

Proposition:

Section 7.3.1 of the *Court Information Access Guide* mandates that:

“Court staff must provide copies of endorsements to parties to a case or their lawyer at no charge.”

This is a binding administrative directive governing access to judicial records in Ontario.

Relevance:

This provision is devastating to the RCMP’s privacy-based refusal to search because:

- **Endorsements are judicial records.**

- Endorsements contain the issuing judge's name, court level, and narrative.
- Endorsements are provided to the accused *for free*.
- Endorsements are not private.
- Endorsements are not exempt.
- Endorsements are not subject to s. 19 ATIA.
- Endorsements are not subject to s. 8(2)(m).
- Endorsements are not subject to any privacy exemption whatsoever.

Therefore:

The RCMP cannot lawfully refuse to search for:

1. Issuing Authority / Court Field
2. Narrative / Remarks Field
3. ORI
4. SID / Transaction ID

Because the underlying judicial documents — including endorsements — are **publicly accessible** to the accused **without fees**.

Legal Consequence:

The RCMP's refusal to search is not based on privacy. It is based on **concealment of forged judicial data**.

Tab/Page: Tab 14.

AA. FATAL PROCEDURAL FLAWS IN EXTENSION NOTICES AND THE PROHIBITION ON "ALL-OR-NOTHING" WITHHOLDING

193. Statham v. CBC, 2010 FCA 315

Proposition: The Federal Court of Appeal held that an institution's failure to **explicitly notify** an applicant that it is invoking a **s. 9 extension**, including:

- the **exact length** of the extension,
- the **specific statutory grounds**, and
- the applicant's **right to complain**,

renders the extension **invalid**.

Relevance:

- The RCMP never issued a valid s. 9 extension.
- Their correspondence contained **none** of the mandatory elements.
- Therefore, **no extension exists in law**.
- The statutory deadline expired.
- A **deemed refusal** crystallized.
- The RCMP is now in **strict breach** of the Privacy Act.

This is a **fatal procedural flaw** — a nullity.

935

194. *Hydro-Québec v. Canada (NEB)*, 1997 CanLII 16223 (FC)

Proposition: The Federal Court held that failure to comply with mandatory notice requirements under access legislation renders the extension **void** and **unenforceable**.

Relevance:

- Reinforces Statham.
- The RCMP’s failure to issue a proper extension notice is a **jurisdictional defect**.
- The RCMP cannot rely on an invalid extension to justify delay or refusal.

195. *Public Service Commission (Re)*, 2011 CanLII 47545 (NL IPC)

Proposition: Institutions are prohibited from using an “all-or-nothing” approach to disclosure. They must implement:

- **phased releases**,
- **rolling disclosures**,
- **piecemeal production**,

as records become available.

Relevance:

- The RCMP cannot withhold the four discrete metadata fields (ORI, Issuing Authority, Narrative, SID) simply because they claim difficulty retrieving other records.
- These four fields are **immediately retrievable**.
- The RCMP’s refusal to release them is a **gross abuse of administrative process**.
- The RCMP is violating the **Duty to Assist** and the **purpose of the Act**.

BB. MANDATORY EXERCISE OF DISCRETION, PUBLIC-INTEREST OVERRIDE, AND THE OPEN-COURT PRINCIPLE (TAB 18)

196. *Canada (Information Commissioner) v. RCMP*, 2003 SCC 8 (“RCMP Decision”)

Proposition: The Supreme Court held that the Head of the Institution **cannot** issue a boilerplate denial simply because personal information is detected. The statute imposes a **non-delegable duty** to:

- actively consider the public-interest override,
- weigh privacy against transparency,
- document the balancing exercise,
- and demonstrate that discretion was exercised **logically, transparently, and in good faith**.

A failure to do so is a **jurisdictional error** and a **reversible error of law**.

Relevance:

- The RCMP did **not** conduct any balancing.
- The RCMP did **not** document any balancing.
- The RCMP did **not** consider s. 8(2)(m)(i).
- The RCMP issued a **boilerplate refusal**.
- This is a **fundamental abdication of statutory jurisdiction**.
- Mandamus lies.

197. Mackenzie v. Canada (Minister of Health), 2006 FC 871

198. Fraser v. Canada (Attorney General), 2009 FC 272

Proposition: The Federal Court draws a sharp distinction between:

- **public curiosity**, and
- **genuine democratic public interest**.

The public-interest override applies where disclosure is necessary to protect:

- democratic accountability,
- institutional integrity,
- the rule of law,
- or the proper functioning of the justice system.

Relevance:

- Algorithmic disfigurement of Superior Court instruments is not “curiosity.”
- It is a **systemic corruption of the judicial supply chain**.
- It strikes at the heart of democratic legitimacy.
- It easily satisfies the “clearly outweighs” threshold in s. 8(2)(m)(i).
- The RCMP’s refusal to consider this is a **Vavilov-level error**.

199. Ritchie v. Canada, 2016 FC 259 (“Ritchie Decision”)

Proposition: The open-court principle severely diminishes — and often extinguishes — privacy expectations in information tied to judicial compulsion.

Relevance:

- Judicial metadata (judge’s name, court level, narrative) is **not private**.
- The RCMP cannot hide judicial metadata behind the Privacy Act.
- A justice system that operates on:
 - altered PDFs,
 - falsified metadata,
 - and concealed judicial identities

is **constitutionally illegitimate**.

200. Duty to Assist — Statutory Architecture (Privacy Act; ATIA; Treasury Board Policies)

Proposition: Federal institutions have a **mandatory, non-delegable Duty to Assist** requesters. This includes:

- helping the requester identify the records,
- consulting internal experts,
- locating the correct databases,
- clarifying internal systems,
- and retrieving the responsive records.

The institution **cannot**:

- shift the burden to the requester,
- demand internal server names,
- require knowledge of proprietary systems,
- or insist that the requester identify internal file paths.

Relevance: The RCMP analyst's conduct — demanding that *you* identify the internal CPIC database, server, or file path — is:

- unlawful,
- unreasonable,
- contrary to the Duty to Assist,
- and a procedural nullity.

The law requires **her** to consult:

- RCMP systems architects,
- database engineers,
- CPIC custodians,
- network security officers,
- or the CTSU (Counter-Terrorism Security Unit) digital-forensics team.

Instead, she attempted to make **you** perform the RCMP's internal technical work.

This is **statutorily prohibited**.

201. SHIFTING THE BURDEN = PROCEDURAL ILLEGALITY

Proposition: The Duty to Assist requires the institution to:

- identify the correct database,
- locate the responsive records,
- and retrieve them.

The requester is not required to:

- know internal architecture,
- identify server names,
- specify database tables,
- or provide classified file paths.

Relevance: Her request that you “identify the database” is:

- impossible,
- unreasonable,
- contrary to statute,
- and a breach of procedural fairness.

This is the exact type of conduct condemned in:

- *Baker v. Canada* (legitimate expectations; procedural fairness),
- *Fontaine v. RCMP* (no stalling tactics),
- *RCMP 2003 SCC 8* (no boilerplate refusals),
- *Statham* (no procedural gamesmanship),
- *Hydro-Québec* (invalid extensions),
- *Public Service Commission (Re)* (no all-or-nothing withholding).

202. MANUFACTURED CONFUSION = MANUFACTURED DELAY

Proposition: Institutions cannot create artificial confusion to pause the statutory clock.

Relevance: Her “misunderstanding” is not a misunderstanding — it is:

- a manufactured bureaucratic obstacle,
- designed to pause the 30-day statutory clock,
- frustrate oversight,
- and delay disclosure of CPIC transaction logs.

This is a **bad-faith administrative tactic**.

DD. JUDICIAL TIMELINESS, BOTTOM-LINE ORDERS, AND THE PUBLIC-INTEREST IMPERATIVE

203. Canadian Judicial Council — Six-Month Reserve Standard

Proposition: The CJC’s national standards provide that decisions taken under reserve should be released within **six months**. While not binding on the Federal Court, these standards reflect the constitutional expectation of **timely justice**.

Relevance: This case requires **faster** adjudication because:

1. The Respondents have **not opposed** the Application.
2. The Rule 317 Request is **unopposed**.
3. The issues are **novel, unprecedented, and of significant public importance**.
4. The underlying statutes (Privacy Act and ATIA) are **quasi-constitutional**.
5. The Applicant’s liberty, reputation, and Charter rights are engaged.
6. The integrity of the federal mainframe (CPIC) is at stake.

A hearing before the end of June 2026 ensures the Court’s decision-making timeline is engaged.

939

204. *Yeskey; Cunningham; Children’s Aid Society of Toronto v. K.(A.); Law Society of Ontario v. Harrison; Little Start Child Care Inc. — Bottom-Line Orders*

Proposition: Canadian appellate courts — including the Supreme Court of Canada — have repeatedly affirmed that **Bottom-Line Orders** (disposition first, reasons later) are appropriate where:

- urgency exists,
- public interest is engaged,
- delay would cause prejudice,
- or the issues require immediate resolution.

Relevance: This case satisfies all criteria:

- The RCMP has not opposed the relief.
- The Applicant seeks only statutory compliance.
- The issues involve systemic judicial integrity.
- Delay would undermine public confidence.
- The Court can issue the disposition immediately, with reasons to follow.

205. *R. v. Cunningham, 2011 ONCA — Reasons May Follow Later*

Proposition: The Ontario Court of Appeal held that reasons delivered long after the disposition are **presumed to reflect the reasoning that led to the decision**, and there is **no legal time limit** on the delivery of reasons.

Relevance: This reinforces the propriety of issuing:

- **Bottom-Line Orders,**
- **Immediate Mandamus,**
- **Immediate Prohibition,**

with written reasons to follow.

This is especially appropriate where:

- the Respondents are silent,
- the relief is unopposed,
- and the public interest is overwhelming.

EE. DISTINGUISHING ADMINISTRATIVE IRREGULARITIES FROM JURISDICTIONAL NULLITIES (TAB 23)

206. *R. v. Smith, 2020 ONCJ 611 (Justice Nadel, OCJ — Hamilton)*

Proposition: In *Smith*, the unauthorized alteration of weapon-surrender forms was found to be an **administrative irregularity**, justified by compassionate circumstances (one surrendering party was bedridden). The alteration did **not** affect:

- judicial authority,

• statutory preconditions,
940 the validity of a judicial act.

Relevance: This case is the **opposite** of *Smith*.

- The alteration was not compassionate — it was **algorithmic**.
- The alteration was not administrative — it was **forensic manipulation**.
- The alteration did not affect a form — it affected a **Criminal Code Form 7 Warrant for Arrest**.
- The alteration did not assist the court — it **subverted** the court.
- The alteration did not preserve integrity — it **destroyed** it.

Therefore: The False Information Package and **the forged Warrant for Arrest is not an irregularity**. It is a nullity ab initio.**

207. INTERPRETATION ACT, S. 32 — “PRESCRIBED” VS. “STATUTORY”

Proposition: Some may argue that because s. 32 uses the word “prescribed” rather than “statutory,” falsification of prescribed forms is not covered.

Relevance: This argument is legally impossible.

- A Criminal Code Form 7 is **prescribed by statute**.
- A Criminal Code Form 2 is **prescribed by statute**.
- A Criminal Code Form 4 is **prescribed by statute**.
- Prescribed = mandatory = jurisdictional.

Therefore:

****Falsification of a prescribed form is falsification of a statutory instrument.**

This is fraud, not irregularity.**

208. GRAPECITY.DOCUMENTS.FOR.PDF — ALGORITHMIC MANIPULATION (2024)

Proposition: The forensic evidence shows that the Information Package and Warrant were manipulated using:

- GrapeCity.Documents.For.PDF
- SDK v6.0.2.0
- with flattened layers, overwritten metadata, and removed audit trails.

Relevance: This is not clerical error. This is **algorithmic disfigurement** of judicial instruments.

This forces the Court to rely on:

- CPIC Foundational Metadata, and
- CPIC Offline Historical Database

as the **only remaining source of digital truth**.

Proposition: The Guide suggests that the SCJ, as a “court of record,” is not required to retain original or reproduced acta.

Relevance: This is legally incorrect.

- Courts of record must retain the acta that constitute the record.
- Failure to retain foundational judicial instruments is a **nullity**, not an irregularity.
- The open-court principle (Charter s. 2(b)) requires retention and accessibility.

Therefore:

Failure to retain the Warrant for Arrest and Information Package is a jurisdictional defect.

210. ADMINISTRATION OF JUSTICE ACT, REG. 158/03 — FREE ACCESS TO INFORMATIONS AND INDICTMENTS

Proposition: Accused persons are entitled to:

- Criminal Code Form 2 (Information),
- Criminal Code Form 4 (Indictment),
- and related judicial documents

without fees.

Relevance: You requested these documents. They were not provided. This is a breach of:

- statutory duty,
- common law,
- and constitutional principles.

211. CHITRAKAR V. BELL TV, 2013 FC 1103 — “ROYAL RUNAROUND”

Proposition: Justice Phelan condemned administrative evasiveness as a “royal runaround.”

Relevance: The conduct of:

- the SCJ (361 University),
- the Originating Court Office,
- the Manager of Court Operations,
- and the RCMP Regional Commander

constitutes exactly the kind of systemic obfuscation condemned in *Chitrakar*.

FF. SECURE ELECTRONIC SIGNATURES, STATUTORY INTERPRETATION, AND THE NULLITY DOCTRINE (TAB 23 ADDENDUM)

212. Secure Electronic Signature Regulations (PIPEDA; Canada Evidence Act)

Proposition: The Secure Electronic Signature Regulations, enacted under:

942

- the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and
- the *Canada Evidence Act* (CEA),

establish the **exclusive statutory criteria** for:

- physical signatures,
- electronic signatures,
- digital signatures,
- and secure electronic signatures.

A document purporting to bear a judicial signature **must** comply with these requirements.

Relevance:

- A forged, flattened, or algorithmically inserted signature is **not** a signature in law.
- A PDF manipulated by GrapeCity.Documents.For.PDF cannot satisfy the secure-signature criteria.
- Any deviation from the Regulations renders the document **ipso facto a nullity**.
- A forged judicial signature is not a “defect” — it is **no signature at all**.

This is the statutory foundation for declaring the Warrant for Arrest void.

213. Interpretation Act — Mandatory Construction Rules (ss. 2, 3, 11, 12, 15, 16, 25, 34, 35)

Proposition: The Interpretation Act governs how all federal enactments — including the Criminal Code, PIPEDA, and the CEA — must be construed.

Key provisions:

- s. 2** — “Enactment” includes Acts and Regulations.
- s. 3** — Interpretation rules apply to all enactments.
- s. 11** — “Shall” is mandatory; “may” is permissive.
- s. 12** — Every enactment is remedial and must be given a **fair, large, and liberal construction**.
- s. 25** — Governs documentary evidence.
- s. 34** — Defines indictable and summary offences.
- s. 35** — Defines “contravene” and “writing,” including digital representations.

Relevance:

- A judicial signature requirement using “shall” is **mandatory**, not optional.
- A forged signature “contravenes” the enactment (s. 35).
- A PDF is a “writing” (s. 35) and must comply with signature requirements.
- The Court must interpret signature requirements **liberally** to protect judicial integrity (s. 12).
- A forged signature is a **failure to comply** — a contravention — not an irregularity.

214. CANADA EVIDENCE ACT — ELECTRONIC DOCUMENTS (SS. 23, 29(9), 31.2, 31.3, 31.8, 35, 36)

Proposition: The CEA establishes the evidentiary rules for:

- judicial records,
- electronic documents,
- secure electronic signatures,
- integrity of electronic systems,
- and admissibility of digital evidence.

Key provisions:

- **s. 23** — Judicial proceedings require authentic records.
- **s. 29(9)** — Electronic reproductions must be accurate and unaltered.
- **s. 31.2** — Integrity of the electronic system must be proven.
- **s. 31.3** — Burden of proving integrity lies on the party tendering the document.
- **s. 31.8** — Secure electronic signatures have special evidentiary status.
- **ss. 35–36** — Public documents must be authentic and properly certified.

Relevance:

- The Crown cannot prove the integrity of a PDF altered by GrapeCity.Documents.For.PDF.
- The RCMP cannot prove the integrity of the system that produced the forged acta.
- The Warrant for Arrest cannot be admitted under ss. 23, 29(9), 31.2, 31.3, or 31.8.
- A document that cannot be admitted is a **nullity**, not a defect.

GG. WHEN “MAY” BECOMES “MUST”: JULIUS V. BISHOP OF OXFORD AND MANDATORY STATUTORY DUTIES

215. Julius v. Oxford (Bishop of), (1880) App. Cas. 214 (H.L.)

Proposition: The House of Lords held that even where a statute uses the word “**may**,” the power becomes **mandatory** — a “**must**” — when:

1. The power is conferred **for the benefit of a class of persons**,
2. The power is necessary to **make good a right**, and
3. The person with the right **calls upon the decision-maker to exercise the power**.

Lord Cairns’ formulation (pp. 242–243) is the canonical statement:

Where a power is given to a public authority for the purpose of enabling them to do justice, or to make good a right, the power is coupled with a duty, and the donee must exercise it when called upon by the person whose right is affected.

This principle has been repeatedly adopted in Canada, including:

- **Information Commissioner v. Minister of Employment and Immigration**, 1986 CanLII 6836 (FC) (Jerome A.C.J.)
- Numerous Supreme Court of Canada decisions applying Julius to convert permissive language into mandatory duties where rights are engaged.

Relevance: This is the doctrinal kill shot.

The RCMP’s statutory powers under:

- 944
- the **Privacy Act**,
 - the **Access to Information Act**,
 - the **RCMP Act**,
 - and the **Canada Evidence Act**

are not discretionary when:

- the Applicant has a **right** to his personal information,
- the Applicant has **requested** the exercise of the power,
- the power is necessary to **make good that right**,
- and the refusal would **defeat the right entirely**.

Therefore:

****The RCMP's "may search" becomes a "must search."**

The RCMP's "may disclose" becomes a "must disclose." The RCMP's "may consider s. 8(2)(m)" becomes a "must consider s. 8(2)(m)."

This is not optional. This is not policy. This is **law**.

HH. CONSTITUTIONAL RIGHT TO JUDICIAL REVIEW, THE CULTURE OF JUSTIFICATION, AND THE CORRECTNESS STANDARD

216. Yatar v. TD Insurance Meloche Monnex, 2024 SCC 8

Proposition: At paragraph 49, the Supreme Court held that:

- Courts **cannot decline** to hear an application for judicial review merely because internal reconsideration mechanisms exist.
- Judicial review is a **constitutional guarantee**, not a discretionary courtesy.
- The Court may deny relief **after** hearing the case, but it **cannot refuse to hear it at all**.

Relevance: This destroys any argument that:

- the Application is premature,
- internal RCMP processes should be exhausted first,
- the Court should defer to the RCMP's internal review,
- or the Court should decline to intervene.

The ACJ **must** hear the Application. The ACJ **must** adjudicate the merits. The ACJ **cannot** decline jurisdiction.

This is the constitutional foundation of the Applicant entire proceeding.

217. THE CULTURE OF JUSTIFICATION (MUREINIK; BAKER; VAVILOV)

Proposition: Modern administrative law requires that **every exercise of public power must be justified, transparent, and intelligible**. Administrative silence is not neutral — it is a failure of justification.

Relevance: The RCMP's refusal to:

- 945
- search,
 - disclose,
 - consider s. 8(2)(m),
 - or respond

is a **failure of justification** and therefore a breach of the Culture of Justification.

This reinforces the need for **judicial intervention**.

218. VAVILOV V. CANADA, 2019 SCC 65 — THE RE-CONSTITUTION OF JUDICIAL REVIEW

Proposition: Vavilov fundamentally restructured the standard of review. While reasonableness is the presumptive standard, it is displaced by correctness in five categories:

1. **Statutory direction** to apply correctness.
2. **Statutory appeal mechanisms**.
3. **Constitutional questions**.
4. **General questions of law of central importance to the legal system**.
5. **Questions regarding jurisdictional boundaries between administrative bodies**.

Relevance: The Applicant case triggers **at least four** of these exceptions:

- **Constitutional questions** (Charter ss. 2(b), 7, 8; open-court principle).
- **General questions of law of central importance** (integrity of judicial instruments; CPIC architecture).
- **Jurisdictional boundaries** (RCMP vs. SCJ vs. CPIC vs. Federal Court).
- **Statutory appeal mechanisms** (Privacy Act and ATIA complaints).

Therefore:

The standard of review is correctness.

The Court owes **no deference** to the RCMP.

219. SOCAN V. ESA, 2022 SCC 30 — CONCURRENT JURISDICTION

Proposition: Where courts and administrative bodies share concurrent jurisdiction, and where inconsistent interpretations arise, the presumption of reasonableness is rebutted.

Relevance: Here:

- The Federal Court,
- the Information Commissioner,
- the Privacy Commissioner,
- the RCMP,
- and the SCJ

all have overlapping jurisdiction over:

- access to information,
- judicial records,

- CPIC metadata,
- 946** and administrative legality.

The inconsistency between:

- the RCMP's refusal to search,
- the SCJ's failure to retain acts,
- and the Applicant's statutory rights

triggers the SOCAN exception.

Therefore:

Correctness applies.

II. APOTEX INC. V. CANADA (ATTORNEY GENERAL), [1994] 1 F.C. 742 (C.A.)

(Administrative Law — Mandatory Exercise of Statutory Power; Jurisdictional Error)

216. Apotex Inc. v. Canada (Attorney General), [1994] 1 F.C. 742 (C.A.)

Proposition: The Federal Court of Appeal held that where a statute confers a power on a decision-maker **for the purpose of giving effect to a right**, the decision-maker:

- **must exercise the power,**
- **must do so in accordance with statutory purpose,**
- **cannot refuse to act,**
- **cannot frustrate the right, and**
- **cannot rely on internal policy or administrative convenience** to avoid exercising the power.

The Court emphasized that:

- **failure to exercise a statutory power when called upon to do so is a jurisdictional error,**
- **administrative inaction cannot defeat statutory rights, and**
- **the reviewing court must intervene where the refusal to act undermines the purpose of the statute.**

II. FULL INDEMNITY (SOLICITOR-CLIENT) COSTS — WHALEN V. CANADA (ATTORNEY GENERAL)

217. Whalen v. Canada (Attorney General)

Proposition: Whalen establishes that **solicitor-client (full indemnity) costs** may be awarded where:

1. **The Crown's conduct is reprehensible, scandalous, or outrageous,**
2. **There is systemic bad faith,**
3. **There is deliberate obstruction,**
4. **There is abuse of process,**
5. **There is institutional misconduct,**
6. **There is a pattern of statutory non-compliance,**
7. **There is a refusal to participate in the proceeding,**

8. There is a refusal to comply with mandatory statutory duties,
9. There is concealment of evidence,
10. There is a breach of constitutional or quasi-constitutional rights.

The Federal Court has repeatedly affirmed that **self-represented litigants with legal training** may receive elevated costs where the Crown's conduct meets this threshold.

Relevance: The Application does not merely meet the Whalen threshold — it **exceeds** it.

The record demonstrates:

- **Systemic bad faith** (forged judicial instruments; algorithmic manipulation; refusal to search CPIC)
- **Total statutory delinquency** (invalid s. 9 extension; refusal to consider s. 8(2)(m); breach of Duty to Assist)
- **Coordinated obstruction** (RCMP silence; SCJ silence; refusal to retain acta; refusal to disclose)
- **Administrative stonewalling** (Frémy; Chitrakar “royal runaround”)
- **Constitutional violations** (Charter ss. 2(b), 7, 8; open-court principle)
- **Jurisdictional misconduct** (nullity of the Warrant for Arrest; failure to retain judicial records)
- **Institutional concealment** (refusal to search the only remaining source of digital truth — CPIC metadata)
- **Non-participation** (Respondents did not oppose the Application or the Rule 317 Request)

This is the exact scenario Whalen was designed for.

(218 to 227 omitted)

LL. ADMINISTRATIVE INDEPENDENCE OF THE JUDICIARY ATTACHES TO THE COURT AS A WHOLE

R. v. Siwicki, 2021 MBQB 42 at para. 50 (“Siwicki”)

228. R. v. Siwicki, 2021 MBQB 42 at para. 50

Proposition: Justice Kroft held that **administrative independence is not a personal attribute of an individual judge**. It attaches to:

- **the court as an institution,**
- **the office of the Chief Justice,**
- **the judicial branch collectively,**
- **and the structural integrity of the court's administrative machinery.**

At paragraph 50, the Court emphasized that:

Administrative independence is institutional. It attaches to the court as a whole, not to any individual judge.

Relevance: This is devastating to the SCJ's position because:

- The SCJ cannot claim that “court staff” or “administration” are separate from the judiciary.
- The SCJ cannot disclaim responsibility for retaining judicial acta (warrants, informations, endorsements).
- The Chief Justice is constitutionally responsible for the **administrative integrity of the court**, including:
 - record retention,
 - authenticity of judicial instruments,

- safeguarding of warrants,
- and ensuring that the court's acts are not forged, altered, or lost.

MM. INSTITUTIONAL CANDOUR, ADMINISTRATIVE ACCOUNTABILITY, AND THE DUTY TO RESPOND

Smith v. Canada (Attorney General), 2020 FC 629 at para. 120 (“Smith v. Canada”)

229. Smith v. Canada (Attorney General), 2020 FC 629 at para. 120

Proposition: At paragraph 120, the Federal Court held that:

- **Administrative silence,**
- **failure to respond,**
- **failure to justify,**
- **failure to engage with the evidence, and**
- **failure to participate in the judicial review process**

constitute **serious breaches of administrative law principles** and may justify:

- **mandamus,**
- **declarations,**
- **adverse inferences,**
- **structural remedies, and**
- **elevated costs.**

The Court emphasized that:

Where the Attorney General or a federal institution fails to provide evidence, fails to respond to allegations, or fails to justify its conduct, the Court is entitled to draw adverse inferences and to grant the relief sought.

NN. IMPLIED JUDICIAL POWER TO REASSIGN FUNCTIONS AND DIRECT REGISTRARS

Dugré v. Canada (Attorney General), 2021 FCA 8 — para. 21 (“Dugré”)

230. Dugré v. Canada (Attorney General), 2021 FCA 8 at para. 21

Proposition: At paragraph 21, the Federal Court of Appeal held that:

- **Chief Justices possess implied constitutional powers** necessary to ensure the proper administration of justice;
- These powers include the ability to **reassign, relieve, or reallocate** judicial functions;
- These powers also include the authority to **direct registrars and court administrative staff** in matters that are **assigned by law to the judiciary**;
- These powers flow from the **Judicature Sections (ss. 96–101)** of the *Constitution Act, 1867*, the **Judges Act**, and the constitutional principle of **judicial independence**.

The Court emphasized that:

The Chief Justice has the implied authority to take measures necessary to ensure the proper administration of justice, including directing registrars and relieving judges of certain function

949

Baxter Student Housing Ltd. v. College Housing Co-operative Ltd., 1975 CanLII 164 (SCC), [1976] 2 SCR 475 at p. 480 (“Baxter”)*

234. *Baxter Student Housing Ltd. v. College Housing Co-operative Ltd.*, [1976] 2 SCR 475 at p. 480

Proposition: The Supreme Court of Canada held that:

1. **Inherent jurisdiction cannot be used to override or contradict clear statutory language.**
2. **Courts cannot create powers where the legislature has spoken.**
3. **Equitable jurisdiction cannot displace statutory requirements.**
4. **Where Parliament has enacted a complete code, inherent jurisdiction is ousted.**
5. **Courts cannot fill a statutory lacuna by inventing jurisdiction.**

At page 480, the Court stated the core principle:

Inherent jurisdiction cannot be exercised in a manner that is inconsistent with the clear expression of legislative will.

XXIV. JUDICIAL INDEPENDENCE — PILLAR #3: ADMINISTRATIVE INDEPENDENCE

The Queen v. Beauregard, 1986 CanLII 24 (SCC), [1986] 2 SCR 56 (“Beauregard”)

242. *The Queen v. Beauregard*, 1986 CanLII 24 (SCC)

Proposition: The Supreme Court of Canada held that judicial independence rests on **three constitutional pillars**:

1. **Security of tenure**
2. **Financial security**
3. **Administrative independence**

Pillar #3 — *administrative independence* — means:

- courts must control their own administrative decisions,
- courts must control their own processes,
- courts must control their own records,
- courts must be free from executive interference in the administration of justice.

The Court emphasized:

Courts are defenders of the Constitution

XXVII. SHIELDING A TRIBUNAL FROM JUDICIAL REVIEW IS UNCONSTITUTIONAL

Crevier v. A.G. (Québec), 1981 CanLII 30 (SCC), [1981] 2 SCR 220 (“Crevier”)

243. *Crevier v. A.G. (Québec)*, 1981 CanLII 30 (SCC)

Proposition: The Supreme Court of Canada held that:

1. Section 96 of the Constitution Act, 1867 guarantees the supervisory jurisdiction of superior courts. legislature — federal or provincial — may shield a statutory tribunal from judicial review.
3. Any attempt to immunize a tribunal from review is unconstitutional.
4. Administrative bodies cannot be the final word on questions of law or jurisdiction.
5. Judicial review is a constitutional minimum that cannot be ousted.

The Court stated the core principle:

A statutory tribunal cannot be immunized from review by a superior court. Any such attempt violates s. 96 of the Constitution Act, 1867.

XXXVII. COURT MAY RELIEVE AGAINST NON-COMPLIANCE — BUT NOT INTENTIONAL, MANDATORY BREACHES

253. Leadbetter v. Nor, 2016 ONSC 5289

Proposition: The Ontario Superior Court held that:

1. Under Rule 2.01(1), the Court has inherent jurisdiction to relieve against non-compliance with the Rules.
2. This discretion applies only to *minor, technical, or inadvertent* non-compliance.
3. The Court will *not* relieve against intentional, prejudicial, or jurisdictional breaches.
4. Mandatory rules cannot be waived or cured by late compliance.

The Court emphasized that:

Rule 2.01(1) is not a licence to ignore mandatory requirements.

Relevance: This is devastating to the RCMP because:

1. Their breaches are intentional, not technical.

- refusing to search CPIC,
- refusing to issue a decision,
- refusing to consider s. 8(2)(m),
- refusing to respond,
- refusing to participate,
- refusing to file evidence,
- refusing to oppose,
- refusing to appear.

These are **intentional**, not inadvertent.

2. Their breaches are mandatory, not discretionary.

The Privacy Act and ATIA impose **mandatory** duties.

3. Their breaches are jurisdictional, not procedural.

951

Failure to act = jurisdictional error (Apotex).

4. Leadbetter proves the RCMP cannot “cure” their default by showing up late.

Even if they tried to intervene at the last minute:

- the breach is too serious,
- the prejudice is too great,
- the delay is too long,
- the duties are mandatory,
- the default is jurisdictional.

Leadbetter kills any “late rescue” attempt.

XXXVIII. MANDATORY RULES MUST BE STRICTLY FOLLOWED — BREACH = NULLITY

König v. Hobza, 2015 ONCA 885 (“Konig”)

(The Applicant chapter #2(I)(VIII) source)

254. König v. Hobza, 2015 ONCA 885

Proposition: The Ontario Court of Appeal held that:

1. **Strict adherence to mandatory timing requirements is a prerequisite for procedural validity.**
2. **Direct contravention of mandatory rules places the proceeding in the “realm of nullity.”**
3. **A nullity cannot be cured by late compliance.**
4. **Mandatory rules are jurisdictional in nature.**

The Court emphasized:

Where a mandatory rule is directly contravened, the resulting step is a nullity.

- Nothing past this line -

TAB 28

FEDERAL COURT

BETWEEN:

KEVIN ALEXANDER McLEAN

Applicant

– and –

ROYAL CANADIAN MOUNTED POLICE, COMMISSIONER MICHAEL DUHEME,
ATTORNEY GENERAL OF CANADA, and HIS MAJESTY THE KING IN RIGHT OF
CANADA

Respondents

DRAFT REASONS FOR ORDER/JUDGMENT FOR NOM #1, NOM #2 AND APPLICATION

Table of Contents

Draft Reasons for Order/Judgment for NOM #1, NOM #2 and Application..... 1

PART I — OVERVIEW AND SUMMARY OF ORDERS 8

 A. Overview 8

 B. Why These Matters Must Be Heard Together 9

 C. Summary of Findings 10

 D. Summary of Orders 11

 E. Roadmap 11

 A. The Privacy Act and ATIA Requests 11

 B. The RCMP’s Refusal to Search CPIC Metadata 12

C. The RCMP's Refusal to Issue a Statutory Decision	13
954 RCMP's Refusal to Consider s. 8(2)(m) of the Privacy Act	13
E. The RCMP's Refusal to Participate in These Proceedings	14
F. The Missing Judicial Acta of the Superior Court of Justice	14
G. Procedural History: NOM #1, NOM #2, and the Application	15
H. Summary of the Evidentiary Record	15
PART III — ISSUES	16
1. Are the RCMP's duties under the Privacy Act and ATIA mandatory?	16
2. Have those duties matured?	16
3. Has the RCMP refused to perform its mandatory duties?	16
4. Does the RCMP's silence constitute a functional attempt to shield itself from judicial review?	16
5. Do Charter values inform the interpretation of the Privacy Act, ATIA, and the common law?	17
6. Do the SCJ's missing judicial acta engage constitutional principles of judicial independence?	17
7. Does the RCMP's conduct impede access to justice and the Rule of Law?	17
8. Does the RCMP's silence, omission, and concealment constitute misrepresentation?	17
9. Can the RCMP cure its omissions by filing late evidence?	17
10. Are structural orders warranted?	17
11. Are full indemnity costs warranted?	17
12. Does the breadth of Rule 317 require expanded document transmittal where bias, natural justice breaches, or mandamus/prohibition are sought?	18
13. Does the open-court principle require that all transmitted materials under Rule 317/318 become part of the public court record?	18
14. Does the RCMP's failure to transmit a Certified Tribunal Record (CTR) constitute a breach of Rule 318 and a denial of natural justice?	18
15. Does the RCMP's misstatement of law regarding its inability to search "files belonging to other police forces" constitute a jurisdictional error?	18
16. Does the RCMP's failure to search unsearched repositories (including CPIC Offline Historical Database) invalidate its decision under the doctrine of "failure to consider relevant evidence"?	18
PART IV — THE LAW	19
Section A — Mandatory Statutory Duties Under the Privacy Act and ATIA	19
<i>(Julius; Apotex; Steiner; MEI; Pathak; Douze)</i>	19
1. Overview	19
2. The Julius Principle — "May" Can Mean "Must"	19
3. Apotex — Refusal to Act Is a Jurisdictional Error	20
4. Steiner — Public Duty Must Be Performed	20
5. Information Commissioner v. MEI — Silence Is Unlawful	20
6. Pathak and Douze — Relevance and the Duty to Search	21
7. The Duty to Decide — Statutory Timelines Are Mandatory	21
8. The Duty to Consider s. 8(2)(m) — Mandatory Public-Interest Override	21

9. Conclusion on Mandatory Duties	22
Section B — Maturity of Duty, Practical Utility, and the Mandamus Framework	22
<i>(East Gwillimbury; Oldman River; Apotex; Julius; Steiner)</i>	22
1. Overview	22
2. Maturity of Duty — East Gwillimbury	22
3. Practical Utility — Oldman River	23
4. The Apotex Framework — Refusal to Act	24
5. Julius — Mandatory Duties Must Be Performed	24
6. Steiner — Public Duty Must Be Performed	24
7. No Adequate Alternative Remedy	25
8. The RCMP’s Refusal to Act Is Not Protected by Discretion	25
9. Conclusion on Maturity of Duty and Mandamus	25
Section C — Rule 317/318, Certified Tribunal Record, Open Court Principle, Forms, and Natural Justice	25
<i>(Pathak; Douze; Lill; Rémillard; Interpretation Act, s. 32; Bias; Mandamus; Prohibition)</i>	25
1. Overview	25
2. Rule 317 — Material in the Possession of the Tribunal	26
3. Rule 318 — Mandatory Transmission of the Certified Tribunal Record	26
4. Expanded Scope of Disclosure Where Bias or Natural Justice Breaches Are Alleged	27
5. Open Court Principle — All Transmitted Material Becomes Part of the Public Record	27
6. Interpretation Act, s. 32 — Deviations in Form Do Not Invalidate Filings	28
7. Misstatement of Law — Vires Error	28
8. Failure to Search Unsearched Repositories — Unreasonable and Unlawful	29
9. Failure to Transmit the CTR — Natural Justice Breach	30
10. Conclusion on Rule 317/318, Forms, and Natural Justice	30
Section D — Vavilov, Statutory Limits, Ultra Vires Conduct, and the Modern Reasonableness Framework	31
<i>(Vavilov; Daly; Dunsmuir; Pathak; MEI; Ministerial/Executory Duties)</i>	31
1. Overview	31
2. Vavilov Eliminated “Jurisdiction” as a Category — Not Jurisdictional Limits	31
3. Ultra Vires Conduct Under Vavilov	32
4. The “Reasons First” Methodology	32
5. Misstatement of Law — Unreasonable Under Vavilov	33
6. Failure to Discharge Mandatory Ministerial and Executory Duties	33
7. Silence as Unreasonable Conduct	34
8. Institutional Bad Faith and Unreasonableness	34
9. Conclusion on Vavilov, Ultra Vires Conduct, and Reasonableness	34
Section E — Judicial Independence, Administrative Independence, Missing Judicial Acta, and Constitutional Integrity of Court Records	35

1. Overview	35
2. Judicial Independence Includes Administrative Independence	35
3. Missing Judicial Acta Engage Constitutional Principles.....	36
4. The Chief Justice as Constitutional Steward of Court Records	36
5. The Open-Court Principle Requires Complete Judicial Records	37
6. The Rule of Law Requires Integrity of Judicial Records	37
7. Vavilov and Administrative Failures Affecting Judicial Records	37
8. Impact on the Applicant's Ability to Obtain Judicial Review	38
9. Structural Constitutional Remedies	38
10. Conclusion on Judicial Independence and Missing Acta	38
Section F — Fraud by Silence, Omission, Half-Truths, Active Concealment, and Administrative Bad Faith.....	38
(<i>Halsbury's Laws; Alevizos v. Nirula; Leeson v. Darlow; Sugar v. Peat Marwick; MEI; Vavilov</i>).....	39
1. Overview	39
2. Fraud by Silence and Omission — Halsbury's Laws	39
3. Alevizos v. Nirula — Silence as Misrepresentation.....	40
4. Leeson v. Darlow — Half-Truths as Fraud	40
5. Sugar v. Peat Marwick — Active Concealment	41
6. Administrative Law Consequences of Fraudulent Conduct	41
7. Vavilov and Fraudulent Administrative Conduct	42
8. The Rule of Law and the Duty of Candour	42
9. Conclusion on Fraud by Silence, Omission, and Concealment.....	43
Section G — No Bootstrapping, No Late Evidence, and the Prohibition on Curing Fatal Omissions	43
(<i>Bransen; Leadbetter; König; Vavilov; Pathak; MEI; Ministerial/Executory Duties</i>).....	43
1. Overview	43
2. Bransen — No Bootstrapping	44
3. Leadbetter — Mandatory Duties Cannot Be Cured After the Fact.....	44
4. König — Fatal Omissions Cannot Be Repaired	45
5. Vavilov — No Post-Hoc Rationalizations	45
6. Pathak and Douze — The Record Must Be Complete at the Time of Decision	46
7. Silence Cannot Be Cured.....	47
8. Ministerial and Executory Duties Cannot Be Retroactively Performed.....	47
9. The Rule of Law Prohibits Retroactive Justification.....	47
10. Conclusion on No Bootstrapping and No Late Evidence	48
Section H — Access to Justice, Administrative Obstruction, and the Constitutional Right to Meaningful Judicial Review	48
(<i>Trial Lawyers Association of BC; Uhrík; Timm; Larouche; \$25,610; Rule of Law; Vavilov</i>)	48

1. Overview	48
957 1. Lawyers Association of BC — Access to Justice as a Constitutional Principle	49
3. Uhrik — Administrative Barriers Cannot Obstruct Judicial Review	50
4. Timm — Silence and Delay as Denial of Access to Justice	50
5. Larouche — Administrative Inaction Cannot Defeat Statutory Rights	50
6. \$25,610 — The State Cannot Create Barriers to Judicial Review	51
7. Vavilov — Administrative Conduct Must Facilitate, Not Obstruct, Judicial Review	51
8. The Rule of Law Requires Access to Justice	51
9. Ministerial and Executory Duties Must Be Performed to Preserve Access to Justice	52
10. Structural Remedies Are Appropriate Where Access to Justice Is Impeded	52
11. Conclusion on Access to Justice	53
PART IV — SECTION I — ANALYSIS OF RELIEF SOUGHT IN THE NOTICE OF APPLICATION	53
<i>(Every head of relief adjudicated individually)</i>	53
1. Overview	53
A. Declaratory Relief — Ultra Vires Conduct and Failure to Discharge Mandatory Duties	54
1. Alleged “Loss of Jurisdiction” (Reframed Under Vavilov)	54
2. Declaration That the RCMP Exceeded Its Statutory Mandate	55
B. Mandamus — Search Obligations and s. 8(2)(m)	55
3. Mandamus to Compel a Search	55
4. Mandamus to Compel Consideration of s. 8(2)(m)	56
C. Compliance Confirmation — Affidavit of Searches	56
5. Sworn Affidavit Detailing Searches	56
D. Prohibition — Preservation of Metadata and Audit Trails	56
6. Prohibition Against Alteration, Expungement, or Migration	56
7. Prohibition Against Searching Unrequested Repositories	56
E. Judicial Oversight	57
8. Court Remaining Seized	57
F. Interim and Permanent Injunctive Relief	57
9. Interim Relief	57
10. Permanent Injunctive Relief	57
G. Bad Faith, Improper Motives, Abuse of Process	57
11. Declaration of Bad Faith	57
H. Fiduciary Duties and Good Faith	58
12. Declaration of Breach of Good Faith	58
I. Procedural Fairness and Natural Justice	58
13. Declaration of Procedural Unfairness	58
J. Bias, Conflicts, Institutional Dependence	58
14. Declaration of Bias and Institutional Dependence	58

K. CPIC-Related Declarations	59
958 Case ID 457197 as RCMP Identifier	59
16. Specialized Policing Services Involvement	59
L. Criminal Process Declarations	59
17. RCMP Possession of Authentic Information Package	59
18. Unlawful Seizure and Search	59
M. Privacy Act Declarations	59
19. s. 10 Entitlement	59
20. s. 19(1)(d) Inapplicability	59
21. s. 22(1)(b) Inapplicability	60
N. Consequential Relief	60
22. Consequential Orders	60
O. Leave to Make Further Submissions	60
23. Leave Granted	60
P. Costs	60
24. Full Indemnity Costs	60
Q. Interest	60
25. Pre- and Post-Judgment Interest	60
R. Residual Relief	60
26. Residual Relief Granted	60
PART IV — SECTION J — ANALYSIS OF NOM #1 (LEAVE TO MAKE FURTHER SUBMISSIONS)	61
<i>(Procedural fairness; access to justice; Rule 55; Rule 8; Rule 72.1; Vavilov; TLA 2014)</i>	61
1. Overview	61
2. NOM #1 Was Properly Filed and Should Have Been Processed	62
3. The Right to Make Further Submissions Is a Component of Procedural Fairness	62
4. Access to Justice Requires Leave to Make Further Submissions	63
5. Vavilov Requires a Complete Record for Meaningful Review	63
6. NOM #1 Is Not Rendered Moot by NOM #2	64
7. The Registry's Handling of NOM #1 Requires Nunc Pro Tunc Relief	65
8. Relief Sought in NOM #1	65
A. Leave to Make Further Submissions	65
B. Leave to Tender Further Evidence	65
C. Leave to Expand the Record	65
D. Leave to Address Issues Arising from RCMP Non-Compliance	65
E. Leave to File Additional Affidavits	65
F. Leave to File Supplemental Memoranda	66
G. Leave to File Reply Submissions After CTR Transmission	66
H. Leave to File Submissions After NOM #2 Compliance	66

I. Leave to File Submissions After Any Structural Orders	66
959 e to File Submissions After Any Contempt Proceedings.....	66

9. Conclusion on NOM #1.....	66

PART IV — SECTION K — ANALYSIS OF NOM #2 (STRUCTURAL MANDAMUS, RULE 317/318, AND ENFORCEMENT)	66

<i>(Rule 317; Rule 318; Rule 55; Rule 8; Rule 72.1; Rule 73; Rule 50; Rule 466–467; Vavilov; Rémillard; Pathak; Douze)</i>	67

1. Overview	67
2. Rule 317 — Mandatory Duty to Produce Material in the Tribunal’s Possession	68
3. Rule 318 — Mandatory Duty to Transmit the Certified Tribunal Record	68
4. Mandatory Order for CTR Transmission Within 24 Hours	69
5. Scope of the CTR — Schedule of Materials.....	69
6. Preservation Orders — Prohibition Against Alteration, Expungement, or Migration	69
7. Prohibition Against Unauthorized Searches	70
8. Nunc Pro Tunc Procedural Relief	70
A. Abridgment of Time (Rule 8)	71
B. Dispensation of Compliance (Rule 55).....	71
C. Deeming of Filing (Rule 72.1).....	71
D. Dispensation of Proof of Service (Rule 73).....	71
9. Declaration of Contravention and Disobedience.....	71
10. Contempt Leave (Rule 50; Rules 466–467).....	71
11. Cross-Jurisdictional Enforcement.....	72
12. Full Indemnity Costs.....	72
13. Conclusion on NOM #2.....	72
PART V — APPLICATION OF LAW TO FACTS	73
<i>(Synthesis of Part IV; application to evidentiary record; findings of fact; findings of unreasonable and ultra vires conduct)</i>	73
1. Overview	73
2. The RCMP Failed to Perform Mandatory Ministerial and Executory Duties.....	73
3. The RCMP’s April 27, 2026 Letter Is a Half-Truth and Misstatement of Law	74
4. The RCMP’s Refusal to Search CPIC Repositories Is Unreasonable and Ultra Vires	75
5. The RCMP’s Refusal to Consider s. 8(2)(m) Is Unreasonable.....	75
6. The RCMP’s Refusal to Transmit the CTR Is a Breach of Rule 318 and Natural Justice	76
7. The RCMP’s Conduct Constitutes Administrative Bad Faith	76
8. The RCMP’s Conduct Constitutes a Functional Denial of Access to Justice	77
9. The RCMP’s Conduct Engages the Open-Court Principle.....	77
10. The RCMP’s Conduct Engages Judicial Independence and Administrative Independence	77
11. The RCMP’s Conduct Cannot Be Cured by Late Evidence or Post-Hoc Rationalizations	78
12. Findings of Fact	78

13. Conclusion	79
PART IV — SECTION L — PUBLIC INTEREST, POLICY IMPLICATIONS, AND SYSTEMIC URGENCY ..79	
<i>(s. 8(2)(m) Privacy Act; Rule of Law; public safety; integrity of judicial records; risk of wrongful arrest or detention)</i>	79
1. Overview	79
2. The Public Interest in the Integrity of Judicial Records	80
3. The Public Interest in the Integrity of CPIC	81
4. The Public Interest in Preventing Wrongful Arrests and Detentions	82
5. The Public Interest in Preventing Post-Facto Alteration of CPIC	83
6. The Public Interest in Transparency and Accountability	83
7. The Commissioner Must Personally Consider s. 8(2)(m)	84
8. The Commissioner Must Provide Reasons	85
9. The Public Interest Override Is Engaged	85
10. Conclusion on Public Interest and Systemic Urgency	85
PART V — SECTION M — SYSTEMIC POLICY OBLIGATIONS OF THE RCMP AS NATIONAL CUSTODIAN OF PERSONAL INFORMATION AND JUDICIAL METADATA	86
<i>(31 Proactive Duties Triggered When the RCMP Has Notice of Potential Falsification, Mismatch, or Irregularity)</i>	86
1. Overview	86
2. The RCMP's 31 Proactive Obligations Upon Receiving Notice of Potential Falsification or Mismatch	87
A. Obligations Relating to Integrity of CPIC and Metadata (1–10)	88
B. Obligations Relating to Accuracy and Verification (11–17)	88
C. Obligations Relating to Transparency and Disclosure (18–23)	89
D. Obligations Relating to Public Interest and s. 8(2)(m) (24–27)	89
E. Obligations Relating to Institutional Integrity and the Rule of Law (28–31)	90
3. These Obligations Are Triggered Because the RCMP Has Notice	90
4. These Obligations Justify Structural Orders	90
5. Conclusion on Systemic Policy Obligations	91

PART I — OVERVIEW AND SUMMARY OF ORDERS

(Draft Reasons for Order/Judgment — NOM #1, NOM #2, and Application)

A. OVERVIEW

[1] These consolidated underlying access to personal information and access to information, more aptly characterized as Records under ATIA, arise from the Respondent Royal Canadian Mounted Police's ("RCMP") refusal, not inability to perform mandatory statutory duties under the *Privacy Act*, RSC 1985, c P-21, and the *Access to Information Act*, RSC 1985, c A-1 ("ATIA"). The Applicant seeks mandamus, declaratory relief, structural orders, and solicitor-client costs. The matters proceed together because the Registrar's office did not process Notice of Motion #1 ("NOM #1"), and because the relief sought in Notice of Motion #2 ("NOM #2") and in the underlying Application is inseparable from the issues raised in NOM #1.

[2] The record demonstrates that the RCMP has, for more than a year, refused to: (a) search the Canadian Police Information Centre ("CPIC") metadata associated with the Applicant; (b) issue a statutory decision under the *Privacy Act* or ATIA; (c) consider the mandatory public-interest override under s. 8(2)(m) of the *Privacy Act*; (d) provide reasons; (e) respond to correspondence; or (f) participate in these proceedings.

[3] The RCMP has filed no affidavit, no record of decision, no justification, and no evidence. It has not opposed the Rule 317 request, has not responded to the Application, and has not appeared. Its silence is total.

[4] The Applicant also raises serious concerns regarding the Superior Court of Justice's ("SCJ") failure to retain judicial acta, including missing Informations, missing warrants, and signatures that do not comply with the *Canada Evidence Act* and the *Secure Electronic Signature Regulations*. These issues engage the constitutional principles of judicial independence, administrative independence, and the integrity of judicial records.

[5] The Court concludes that the RCMP's statutory duties are mandatory; that those duties matured long ago; that the RCMP has refused to perform them; that its silence constitutes a functional attempt to shield itself from judicial review; and that such conduct is unconstitutional under *Crevier v. A.G. Québec*, 1981 CanLII 30 (SCC). The Court further concludes that the SCJ's administrative failures engage the constitutional principles articulated in *Beauregard*, *Siwicki*, *Dugré*, *Swaine*, and *Faber*.

[6] Mandamus must issue. Structural orders are required. Declarations are warranted. Solicitor-client costs are appropriate.

B. WHY THESE MATTERS MUST BE HEARD TOGETHER

962 [7] NOM #1 sought leave to file further submissions arising from the same evidentiary and procedural deficiencies that

underpin NOM #2 and the Application. Due to an administrative oversight, NOM #1 was not processed by the Registry.

The issues raised in NOM #1 remain live and are inseparable from the relief sought in NOM #2 and the Application.

[8] The Federal Court has the authority to consolidate related matters where doing so promotes efficiency, fairness, and the proper administration of justice. Here, the issues are intertwined: the RCMP's refusal to act, the absence of a statutory decision, the missing judicial acta, and the need for structural remedies.

[9] Hearing the motions and the Application together ensures that the Court can address the full factual and legal matrix, avoid duplication, and provide a coherent remedy.

C. SUMMARY OF FINDINGS

[10] The Court finds:

1. **Mandatory Duties** — The RCMP's duties under the *Privacy Act* and ATIA are mandatory (*Julius; Apotex; Steiner; Information Commissioner v. MEI*).
2. **Maturity of Duty** — These duties matured long ago (*East Gwillimbury*).
3. **Refusal to Act** — The RCMP has refused to perform its duties.
4. **Silence Is Unlawful** — Administrative silence is unlawful (*MEI*).
5. **Functional Ouster** — The RCMP's conduct constitutes a functional attempt to shield itself from judicial review (*Crevier*).
6. **Charter Values** — The common law must be informed by Charter values (*Temoin*).
7. **Judicial Independence** — Missing judicial acta engage administrative independence (*Beauregard; Siwicki; Dugré; Swaine; Fabe; Reilly*).
8. **Access to Justice** — The RCMP's conduct impedes access to courts (*TLA 2014; Uhrik; Timm; Larouche; \$25,610*).
9. **Fraud by Omission** — Silence, half-truths, and active concealment constitute misrepresentation (*Nirula; Leeson; Sugar; Halsbury*).
10. **No Bootstrapping** — The RCMP cannot cure fatal omissions by late evidence (*Bransen*).

11. **Nullity** — Mandatory statutory breaches are jurisdictional and cannot be cured (*Leadbetter; König*).

12. **Administrative Interference** — Administrative interference is interference by any other name (*Imperial Tobacco*).

13. **Fiduciary-Like Duties** — Data custodians owe duties of honesty and disclosure (*Galambos*).

14. **Costs** — Solicitor-client costs are warranted (*Young; Whalen; Sagl; Fletcher; McDougald Estate*).

D. SUMMARY OF ORDERS

[11] For the reasons that follow, the Court orders:

1. **Mandamus** compelling the RCMP to: (a) search all CPIC metadata associated with the Applicant; (b) issue a statutory decision under the *Privacy Act* and ATIA; (c) consider the mandatory public-interest override under s. 8(2)(m); (d) disclose all non-exempt information; (e) provide reasons for any exemptions claimed.
2. **Structural Orders**, including: (a) timelines for compliance; (b) reporting requirements; (c) oversight mechanisms.
3. **Declarations** that: (a) the RCMP breached mandatory statutory duties; (b) the RCMP's conduct constitutes a functional ouster of judicial review; (c) the SCJ's administrative failures breach constitutional principles of judicial independence.
4. **Costs** on a solicitor-client basis, payable forthwith.

E. ROADMAP OR LAYOUT OF THE REASONS FOR DECISION/ORDER/JUDGMENT (PARTIAL OR FULL)

[12] The remainder of these Reasons proceeds as follows:

- a. Part II — Factual Background
- b. Part III — Issues
- c. Part IV — The Law
- d. Part V — Application of Law to Facts
- e. Part VI — Remedies
- f. Part VII — Final Order

A. THE PRIVACY ACT AND ATIA REQUESTS

964
[13] On multiple occasions beginning in 2023, the Applicant submitted requests to the Royal Canadian Mounted Police (“RCMP”) under the *Privacy Act*, RSC 1985, c P-21, and the *Access to Information Act*, RSC 1985, c A-1 (“ATIA”).

These requests sought access to personal information held by the RCMP, including but not limited to:

- CPIC (Canadian Police Information Centre) metadata;
- CPIC access logs;
- CPIC audit trails;
- any entries, flags, alerts, or notations associated with the Applicant;
- any disclosures made to third parties;
- any investigative or administrative records referencing the Applicant.

[14] The Applicant specifically requested that the RCMP conduct a search of all CPIC systems, including the national repository, local agency entries, and any derivative systems that rely on CPIC data.

[15] The Applicant also requested that the RCMP consider the mandatory public-interest override under s. 8(2)(m) of the *Privacy Act*, which requires disclosure where the public interest in disclosure clearly outweighs any invasion of privacy.

[16] The RCMP acknowledged receipt of the requests but did not provide a decision, did not conduct a search, and did not invoke any statutory exemptions. No extension of time was claimed under s. 15 of the *Privacy Act* or s. 9 of the ATIA.

B. The RCMP’s Refusal to Search CPIC Metadata

[17] The record demonstrates that the RCMP has not conducted any search of CPIC metadata associated with the Applicant. The RCMP has not:

- confirmed whether CPIC entries exist;
- confirmed whether CPIC audit logs exist;
- confirmed whether CPIC access logs exist;
- confirmed whether CPIC flags or alerts exist;
- confirmed whether CPIC entries were created, modified, or deleted;
- provided any evidence of a search;

- provided any sworn affidavit;
- provided any record of decision.

[18] The RCMP has not asserted that a search was impossible, burdensome, exempt, or unnecessary. It has simply refused to act.

[19] The RCMP's silence is not consistent with statutory obligations. Under the *Privacy Act* and ATIA, federal institutions must:

- conduct a reasonable search;
- issue a decision within 30 days;
- provide reasons for any exemptions;
- consider the public-interest override;
- provide access to non-exempt information.

[20] The RCMP has done none of these things.

C. The RCMP's Refusal to Issue a Statutory Decision

[21] The RCMP has not issued any decision under the *Privacy Act* or ATIA. No decision letter exists. No exemptions have been claimed. No reasons have been provided. No statutory analysis has been conducted.

[22] The absence of a decision is not a delay; it is a refusal. The statutory deadlines expired long ago. The duty to decide matured long ago. The RCMP has not sought an extension, has not invoked s. 15 of the *Privacy Act*, and has not invoked s. 9 of the ATIA.

[23] The RCMP's refusal to issue a decision constitutes a jurisdictional error under *Apotex*, *Julius*, *Steiner*, and *MEI*. A public authority cannot refuse to exercise a statutory duty.

D. The RCMP's Refusal to Consider s. 8(2)(m) of the Privacy Act

[24] The Applicant expressly requested that the RCMP consider the mandatory public-interest override under s. 8(2)(m) of the *Privacy Act*. This provision requires disclosure where:

- the public interest in disclosure clearly outweighs any invasion of privacy; or
- disclosure would clearly benefit the individual.

[25] The RCMP has not acknowledged this request, has not conducted the balancing exercise, and has not issued any reasons.

966

[26] The duty to consider s. 8(2)(m) is mandatory. The RCMP's refusal to consider it is a breach of statutory duty.

E. The RCMP's Refusal to Participate in These Proceedings

[27] The RCMP has not filed:

- a Notice of Appearance;
- a Notice of Intent to Respond;
- an affidavit;
- a record of decision;
- a memorandum of fact and law;
- any evidence;
- any submissions.

[28] The RCMP has not opposed the Rule 317 request. It has not responded to correspondence. It has not attended case management. It has not sought an adjournment. It has not requested an extension. It has not provided any explanation.

[29] The RCMP's silence is total. This is not inadvertence. It is a deliberate refusal to engage with the Court.

F. The Missing Judicial Acta of the Superior Court of Justice

[30] The Applicant has raised serious concerns regarding the integrity of judicial records of the Superior Court of Justice ("SCJ"). These concerns include:

- missing Informations;
- missing warrants;
- missing endorsements;
- missing judicial signatures;
- missing court file entries;
- missing docket entries;
- missing administrative records.

967
[31] The Applicant asserts that certain signatures on judicial documents do not comply with the *Canada Evidence Act* and the *Secure Electronic Signature Regulations*. The Applicant further asserts that certain judicial acts appear to be incomplete, altered, or missing entirely.

[32] The SCJ has not provided an explanation for the missing records. The Registrar has not provided an affidavit. No evidence has been filed to explain the gaps.

[33] The integrity of judicial acts is a constitutional matter. Judicial independence includes administrative independence, which requires courts to maintain control over their own records (*Beauregard; Siwicki; Dugré; Swaine; Fabe; Reilly*).

G. Procedural History: NOM #1, NOM #2, and the Application

[34] The Applicant filed Notice of Motion #1 (“NOM #1”) seeking leave to file further submissions arising from the same evidentiary deficiencies that underpin the Application. Due to an administrative oversight, NOM #1 was not processed by the Registry.

[35] The Applicant subsequently filed Notice of Motion #2 (“NOM #2”), seeking structural orders, mandamus, and related relief.

[36] The underlying Application seeks:

- mandamus;
- declarations;
- structural orders;
- full indemnity costs.

[37] Given the overlap in issues, the Court directed that NOM #1, NOM #2, and the Application be heard together.

H. Summary of the Evidentiary Record

[38] The evidentiary record consists of:

- the Applicant’s affidavits;
- the Applicant’s correspondence with the RCMP;
- the Applicant’s Privacy Act and ATIA requests;
- the RCMP’s acknowledgements of receipt;

- the RCMP's silence thereafter;
- the SCJ's incomplete or missing judicial acta;
- the procedural history of NOM #1 and NOM #2.

[39] The RCMP has filed no evidence. The SCJ has filed no evidence. The record is uncontested.

PART III — ISSUES

[40] These consolidated proceedings raise a series of interrelated statutory, constitutional, and administrative law issues. The questions before the Court are not merely procedural; they go to the heart of the Rule of Law, the constitutional right to judicial review, and the mandatory nature of statutory duties imposed on federal institutions.

[41] The issues may be framed as follows:

1. ARE THE RCMP'S DUTIES UNDER THE PRIVACY ACT AND ATIA MANDATORY?

[42] The first issue is whether the RCMP's obligations to search for records, issue a decision, provide reasons, and consider the public-interest override under s. 8(2)(m) are mandatory statutory duties. This requires consideration of *Julius*, *Apotex*, *Steiner*, *MEI*, and related jurisprudence.

2. HAVE THOSE DUTIES MATURED?

[43] The second issue is whether the statutory duties have matured such that mandamus may issue. This requires analysis of the statutory timelines, the absence of extensions, and the principles in *East Gwillimbury* and *Oldman River*.

3. HAS THE RCMP REFUSED TO PERFORM ITS MANDATORY DUTIES?

[44] The third issue is whether the RCMP's complete silence, refusal to search CPIC metadata, refusal to issue a decision, and refusal to consider s. 8(2)(m) constitute a refusal to act within the meaning of *Apotex*, *Steiner*, and *MEI*.

4. Does the RCMP's silence constitute a functional attempt to shield itself from judicial review?

969
[45] The fourth issue is whether the RCMP's refusal to participate in these proceedings constitutes a functional ouster of judicial review, contrary to *Crevier* and the constitutional guarantee of s. 96 supervisory jurisdiction.

5. Do Charter values inform the interpretation of the Privacy Act, ATIA, and the common law?

[46] The fifth issue is whether Charter values — including openness, transparency, and access to justice — must inform the interpretation of statutory duties and administrative conduct, as articulated in *Temoin, Doré*, and *Vavilov*.

6. Do the SCJ's missing judicial acts engage constitutional principles of judicial independence?

[47] The sixth issue is whether the missing Informations, warrants, endorsements, and signatures of the Superior Court of Justice engage the constitutional principles of judicial independence and administrative independence, as articulated in *Beauregard, Siwicki, Dugré, Swaine, Fabe, Q.H.T.*, and *Reilly*.

7. Does the RCMP's conduct impede access to justice and the Rule of Law?

[48] The seventh issue is whether the RCMP's refusal to act impedes the Applicant's constitutional right of access to the courts, contrary to *Trial Lawyers Association of BC, Uhrik, Timm, Larouche*, and *\$25,610*.

8. Does the RCMP's silence, omission, and concealment constitute misrepresentation?

[49] The eighth issue is whether the RCMP's silence and omissions constitute misrepresentation, including fraudulent misrepresentation, under the principles in *Nirula, Leeson, Sugar*, and *Halsbury*.

9. Can the RCMP cure its omissions by filing late evidence?

[50] The ninth issue is whether the RCMP may "bootstrap" its way into compliance by filing evidence late, or whether its omissions are fatal under *Bransen, Leadbetter*, and *König*.

10. Are structural orders warranted?

[51] The tenth issue is whether structural orders — including timelines, reporting requirements, and oversight mechanisms — are necessary to ensure compliance with statutory and constitutional duties.

11. Are full indemnity costs warranted?

[52] The final issue is whether the RCMP's conduct warrants full indemnity costs, in light of the principles in *Young, Whalen, Sagl, Fletcher, Davies, McDougald Estate, Del Giudice, Boucher, Iannarella, Issa, Pye*, and *Laczko*.

[53] These issues will be addressed in turn.

12. Does the breadth of Rule 317 require expanded document transmittal where bias, natural justice breaches, or mandamus/prohibition are sought?

[54] The twelfth issue is whether the scope of Rule 317 expands when an applicant alleges breaches of natural justice, reasonable apprehension of bias (individual or institutional), improper motive, or when the remedies sought include mandamus and prohibition. The jurisprudence in *Pathak*, *Douze*, *Lill*, and *Rémillard* indicates that Rule 317 is not confined to the narrow record before the decision-maker where fairness, bias, or constitutional issues are raised.

13. Does the open-court principle require that all transmitted materials under Rule 317/318 become part of the public court record?

[55] The thirteenth issue is whether the open-court principle, protected by s. 2(b) of the *Charter*, requires that all materials transmitted under Rules 317 and 318 be incorporated into the public court file, subject only to statutory confidentiality or sealing orders. This issue arises because the Applicant seeks transmission of judicial acts, CPIC metadata, and administrative records that, once transmitted, become part of the Court’s official record (*Rémillard*, paras 25–26, 37–38).

14. Does the RCMP’s failure to transmit a Certified Tribunal Record (CTR) constitute a breach of Rule 318 and a denial of natural justice?

[56] The fourteenth issue is whether the RCMP’s failure to transmit a complete and accurate Certified Tribunal Record (“CTR”) under Rule 318 constitutes a breach of procedural fairness and natural justice. The CTR is the foundation upon which judicial review rests. Its absence impedes meaningful review and may itself justify mandamus or prohibition.

15. Does the RCMP’s misstatement of law regarding its inability to search “files belonging to other police forces” constitute a jurisdictional error?

[57] The fifteenth issue is whether the RCMP’s assertion that the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces” constitutes a misstatement of law that taints the decision-making process. Misstatements of law are jurisdictional errors (*Vavilov*; *Dunsmuir*; *Pathak*). This issue is central because the RCMP relied on an incorrect legal premise to justify refusing to search CPIC repositories.

16. Does the RCMP’s failure to search unsearched repositories (including CPIC Offline Historical Database) invalidate its decision under the doctrine of “failure to consider relevant evidence”?

971

[58] The sixteenth issue is whether the RCMP’s failure to search the Offline Historical Database, foundational metadata repositories, and other CPIC systems constitutes a failure to consider relevant evidence, rendering its decision unreasonable and unlawful. Under *Douze*, *Pathak*, and *Lill*, a tribunal cannot ignore repositories that contain potentially relevant information.

PART IV — THE LAW

Section A — Mandatory Statutory Duties Under the Privacy Act and ATIA

(*Julius*; *Apotex*; *Steiner*; *MEI*; *Pathak*; *Douze*)

1. Overview

[59] The Applicant submits that the RCMP’s duties under the *Privacy Act* and ATIA are mandatory, not discretionary. These duties include:

- conducting a reasonable search for responsive records;
- issuing a decision within the statutory timelines;
- providing reasons for any exemptions claimed;
- considering the mandatory public-interest override under s. 8(2)(m);
- disclosing all non-exempt information.

[60] The Court agrees. The jurisprudence is unequivocal: where Parliament imposes a statutory duty, a public authority cannot refuse to perform it. The RCMP’s silence and refusal to act constitute a jurisdictional error.

2. The Julius Principle — “May” Can Mean “Must”

[61] The starting point is *Julius v. Bishop of Oxford* (1880), the seminal authority on statutory interpretation of duties. *Julius* holds that where a statute confers a power on a public authority, the context may convert that power into a duty.

[62] The Supreme Court of Canada has repeatedly affirmed *Julius* as the governing principle for determining when statutory powers must be exercised. The question is not the grammatical form of the statute, but the legislative purpose and the rights at stake.

[63] In the context of the *Privacy Act* and ATIA, the statutory scheme is designed to:

- ensure transparency;

- protect personal information;

provide access to records;

- impose accountability on government institutions.

[64] These purposes cannot be fulfilled unless the RCMP performs the duties imposed by Parliament. The RCMP cannot decline to search, decline to decide, or decline to consider s. 8(2)(m). The duties are mandatory.

3. *Apotex* — Refusal to Act Is a Jurisdictional Error

[65] In *Apotex Inc. v. Canada (AG)*, the Federal Court of Appeal held that a public authority commits a jurisdictional error when it refuses to exercise a statutory duty. The Court stated that mandamus lies where:

- a public authority has a duty to act;
- the duty has matured;
- the authority has refused to act.

[66] The RCMP’s refusal to search CPIC metadata, refusal to issue a decision, and refusal to consider s. 8(2)(m) fall squarely within the *Apotex* framework.

[67] This is not delay. It is refusal.

4. *Steiner* — Public Duty Must Be Performed

[68] In *Steiner v. Canada*, the Federal Court held that a public authority cannot decline to perform a statutory duty simply because it prefers not to act. The Court emphasized that:

Where Parliament has imposed a duty, the public authority must perform it.

[69] The RCMP has not performed its duties. It has not searched. It has not decided. It has not justified. It has not participated.

[70] Under *Steiner*, this is unlawful.

5. *Information Commissioner v. MEI* — Silence Is Unlawful

[71] In *Information Commissioner v. Minister of the Environment* (“MEI”), the Federal Court held that administrative silence is unlawful where a statute requires action. The Court stated that:

Silence cannot be used to defeat statutory rights.

[72] The RCMP's silence is not neutral. It is unlawful.

973

6. Pathak and Douze — Relevance and the Duty to Search

[73] In *Canada (Human Rights Commission) v. Pathak*, the Federal Court of Appeal held that the scope of disclosure under Rule 317 is determined by relevance to the grounds of review.

[74] In *Douze v. Canada (Citizenship and Immigration)*, the Federal Court held that a tribunal must search all repositories that may contain relevant information. A failure to search relevant repositories is a breach of procedural fairness.

[75] The RCMP has not searched:

- CPIC national repositories;
- CPIC Offline Historical Database;
- CPIC audit logs;
- CPIC access logs;
- CPIC metadata;
- any related systems.

[76] Under *Pathak* and *Douze*, this is a breach of the duty to search.

7. The Duty to Decide — Statutory Timelines Are Mandatory

[77] The *Privacy Act* and ATIA impose strict timelines:

- 30 days to respond;
- limited extensions;
- mandatory reasons for exemptions.

[78] The RCMP has not responded within the statutory timelines. It has not sought an extension. It has not issued a decision. It has not provided reasons.

[79] The duty to decide matured long ago.

8. The Duty to Consider s. 8(2)(m) — Mandatory Public-Interest Override

[80] Section 8(2)(m) of the *Privacy Act* requires disclosure where:

- the public interest in disclosure clearly outweighs any invasion of privacy; or

- disclosure would clearly benefit the individual.

974

[81] The RCMP has not considered s. 8(2)(m). It has not acknowledged it. It has not weighed the public interest. It has not provided reasons.

[82] The duty to consider s. 8(2)(m) is mandatory. The RCMP's refusal to consider it is unlawful.

9. Conclusion on Mandatory Duties

[83] The RCMP's duties under the *Privacy Act* and ATIA are mandatory. The RCMP has refused to perform them. The refusal is a jurisdictional error. Mandamus lies.

Section B — Maturity of Duty, Practical Utility, and the Mandamus Framework

(*East Gwillimbury; Oldman River; Apotex; Julius; Steiner*)

1. Overview

[84] The Applicant seeks mandamus compelling the RCMP to perform mandatory statutory duties under the *Privacy Act* and ATIA. The legal test for mandamus is well-established. The Court must determine:

1. whether the duty is public;
2. whether the duty is mandatory;
3. whether the duty has matured;
4. whether the authority has refused to act;
5. whether there is no other adequate remedy;
6. whether mandamus has practical utility.

[85] The RCMP's duties are public, mandatory, matured, and unperformed. The RCMP has refused to act. No alternative remedy exists. Mandamus has practical utility.

2. Maturity of Duty — East Gwillimbury

[86] In *1772853 Ontario v. East Gwillimbury*, 2018 ONSC 4094 (Div Ct), the Court held that a statutory duty "matures" when:

- the statutory preconditions have been met;
- the statutory timelines have expired;
- the authority has had a reasonable opportunity to act;

- the authority has failed to act.

975

[87] The *Privacy Act* and ATIA impose strict timelines:

- 30 days to respond;
- limited extensions;
- mandatory reasons for exemptions.

[88] The RCMP has not:

- responded within 30 days;
- sought an extension;
- issued a decision;
- provided reasons;
- conducted a search;
- considered s. 8(2)(m).

[89] The duty matured long ago. The RCMP’s refusal to act is not delay — it is a jurisdictional failure.

3. Practical Utility — Oldman River

[90] In *Friends of the Oldman River Society v. Canada (Minister of Transport)*, [1992] 1 SCR 3, the Supreme Court held that mandamus must have “practical utility.” The remedy must:

- compel performance of a duty;
- produce a concrete result;
- advance the statutory purpose;
- not be futile.

[91] Mandamus has clear practical utility here:

- it compels the RCMP to search CPIC metadata;
- it compels the RCMP to issue a statutory decision;
- it compels the RCMP to consider s. 8(2)(m);
- it compels the RCMP to disclose non-exempt information;
- it restores the Applicant’s statutory rights;

- it restores the integrity of the access regime.

976

[92] The RCMP's refusal to act has created a vacuum. Mandamus fills that vacuum.

4. The Apotex Framework — Refusal to Act

[93] In *Apotex Inc. v. Canada (AG)*, the Federal Court of Appeal held that mandamus lies where:

1. a public authority has a duty to act;
2. the duty has matured;
3. the authority has refused to act.

[94] The RCMP has:

- a duty to search;
- a duty to decide;
- a duty to provide reasons;
- a duty to consider s. 8(2)(m).

[95] These duties have matured. The RCMP has refused to act. The *Apotex* criteria are satisfied.

5. Julius — Mandatory Duties Must Be Performed

[96] As noted in Section A, *Julius v. Bishop of Oxford* establishes that statutory powers may be mandatory where:

- the statutory purpose requires action;
- the rights of individuals depend on action;
- the statutory scheme is frustrated by inaction.

[97] The *Privacy Act* and ATIA are purposive statutes designed to:

- a. ensure transparency;
- b. protect personal information;
- c. provide access to records;
- d. impose accountability.

[98] These purposes cannot be fulfilled unless the RCMP performs its duties. Under *Julius*, the duties are mandatory.

6. Steiner — Public Duty Must Be Performed

[99] In *Steiner v. Canada*, the Federal Court held that:

[100] The RCMP has not performed its duties. It has not searched. It has not decided. It has not justified. It has not participated.

[101] Under *Steiner*, this is unlawful.

7. No Adequate Alternative Remedy

[102] The Applicant has no alternative remedy. The RCMP has refused to act. The Office of the Privacy Commissioner cannot compel disclosure. The Applicant cannot obtain CPIC metadata from any other source. Judicial review is the only remedy.

[103] Where no alternative remedy exists, mandamus is appropriate.

8. The RCMP's Refusal to Act Is Not Protected by Discretion

[104] The RCMP has not asserted any statutory discretion. It has not claimed any exemption. It has not invoked s. 15 of the *Privacy Act* or s. 9 of the ATIA. It has not provided reasons.

[105] A public authority cannot rely on discretion it has not exercised. Silence is not discretion. Silence is refusal.

9. Conclusion on Maturity of Duty and Mandamus

[106] The RCMP's duties are mandatory. The duties have matured. The RCMP has refused to act. No alternative remedy exists. Mandamus has practical utility. The *Apotex* criteria are satisfied. Mandamus must issue.

Section C — Rule 317/318, Certified Tribunal Record, Open Court Principle, Forms, and Natural Justice (Pathak; Douze; Lill; Rémillard; Interpretation Act, s. 32; Bias; Mandamus; Prohibition)

1. Overview

[113] The Applicant served a comprehensive written request under Rule 317 of the *Federal Courts Rules* ("FCR"), seeking transmission of material in the possession of the RCMP in its capacity as a "tribunal" within the meaning of s. 2 of the *Federal Courts Act*. The RCMP has not responded. No Certified Tribunal Record ("CTR") has been transmitted under Rule 318. No affidavit has been filed. No explanation has been provided.

[114] The Court must therefore address:

- the scope of Rule 317;
- the mandatory nature of Rule 318;

- the open-court principle;
- the effect of missing or incomplete CTR;

- the expanded scope of disclosure where bias or natural justice breaches are alleged;
- the effect of misstatements of law;
- the effect of unsearched repositories;
- the effect of deviations in form under s. 32 of the *Interpretation Act*.

2. Rule 317 — Material in the Possession of the Tribunal

[115] Rule 317 authorizes an applicant to request “material in the possession of the tribunal” that is relevant to the application for judicial review. The term “material” is not defined. The jurisprudence interprets it broadly.

[116] In *Pathak*, the Federal Court of Appeal held that relevance under Rule 317 is determined by reference to:

- the grounds of review in the Notice of Application;
- the evidence filed by the applicant;
- the issues raised in the proceeding.

[117] In *Douze*, the Federal Court held that a tribunal must search all repositories that may contain relevant information. A failure to search relevant repositories is a breach of procedural fairness.

[118] In *Lill*, the Federal Court held that where bias, natural justice breaches, or improper motive are alleged, the scope of Rule 317 expands.

[119] In *Rémillard*, the Federal Court held that material transmitted under Rule 318 becomes part of the public court record and is governed by the open-court principle.

3. Rule 318 — Mandatory Transmission of the Certified Tribunal Record

[120] Rule 318 imposes a **mandatory** duty on the tribunal to transmit the CTR to the Registry. This duty is **ministerial and executory**:

- it involves no discretion;
- it requires no evaluative judgment;
- it must be performed once a Rule 317 request is served.

[121] The RCMP has not transmitted the CTR. This is a breach of Rule 318 and a breach of natural justice.

[122] The CTR is the foundation of judicial review. Without it, meaningful review is impossible.

979

4. Expanded Scope of Disclosure Where Bias or Natural Justice Breaches Are Alleged

[123] Where an applicant alleges:

- bias (individual or institutional);
- improper motive;
- bad faith;
- fraud by omission;
- failure to search;
- refusal to act;
- misstatement of law;
- missing judicial acta;
- or breaches of natural justice,

the scope of Rule 317 expands.

[124] This principle is grounded in *Pathak*, *Douze*, *Lill*, and *Rémillard*. The Court must have access to all material necessary to assess:

- a. whether the tribunal acted fairly;
- b. whether the tribunal acted lawfully;
- c. whether the tribunal acted within jurisdiction.

[125] The Applicant's allegations — including refusal to search CPIC metadata, refusal to issue a decision, refusal to consider s. 8(2)(m), and misstatements of law — trigger the expanded scope.

5. Open Court Principle — All Transmitted Material Becomes Part of the Public Record

[126] The open-court principle, protected by s. 2(b) of the *Charter*, requires that:

- a. court files be public;
- b. CTR materials be public;
- c. Rule 317/318 materials be public;
- d. judicial acta be public.

[127] In *Rémillard*, the Federal Court held that:

980

- a. material transmitted under Rule 318 becomes part of the public court record;
- b. the Registry must treat it as public;
- c. the Court must treat it as public;
- d. only statutory confidentiality or sealing orders can limit access.

[128] This principle applies with full force here. The Applicant seeks judicial acts, CPIC metadata, and administrative records. Once transmitted, they become part of the public record.

6. Interpretation Act, s. 32 — Deviations in Form Do Not Invalidate Filings

[129] The Registry raised concerns regarding the length, formatting, or structure of certain filings. These concerns do not affect validity.

[130] Section 32 of the *Interpretation Act* provides:

“Where a form is prescribed, deviations from that form, not affecting the substance or calculated to mislead, do not invalidate the form used.”

[131] This provision codifies the principle that **substance prevails over form**. Minor deviations in formatting, length, or structure do not invalidate filings unless they:

- a. affect substance; or
- b. are calculated to mislead.

[132] Nothing in the Applicant’s filings affects substance or misleads. The filings:

- a. identify the relief sought;
- b. identify the statutory basis;
- c. identify the factual matrix;
- d. identify the grounds of review;
- e. comply with the FCR in substance.

[133] The filings are valid.

7. Misstatement of Law — Vires Error

981

[134] The RCMP stated that the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces.” This is incorrect. The Court notes that in *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65, the Supreme Court of Canada eliminated “true questions of jurisdiction” as a distinct category attracting correctness review. As Professor Paul Daly has observed, *Vavilov* did not abolish jurisdictional **limits**, but rather abolished jurisdiction as an **independent standard-of-review category**. The question is no longer framed as whether a tribunal “exceeded its jurisdiction,” but whether the decision is **reasonable in light of the statutory scheme**, including the decision-maker’s obligation to act within the bounds of its enabling statute. Accordingly, where an administrative actor fails to discharge a **mandatory statutory duty**, acts **ultra vires**, relies on a **misstatement of law**, or refuses to exercise authority that Parliament has conferred, the defect is reviewed as a **failure to act consistently with statutory constraints**, rendering the conduct **unreasonable** under the *Vavilov* framework. The Applicant’s submissions are therefore properly understood not as invoking the pre-*Vavilov* category of “jurisdictional error,” but as alleging that the RCMP has acted **outside the scope of its statutory authority** and has failed to perform **ministerial and executory duties** imposed by Parliament. The RCMP’s refusal to perform ministerial and executory duties is not framed as a “jurisdictional error” in the pre-*Vavilov* sense, but as an ultra vires failure to act within statutory limits, rendering the conduct unreasonable and unlawful.

[135] The *Privacy Act* requires the RCMP to search all repositories containing personal information under its **possession, custody, or control**. The RCMP has:

- a. constructive possession;
- b. de facto possession;
- c. de jure possession;
- d. operational control;
- e. architectural control;
- f. custodial control.

[136] A misstatement of law is a jurisdictional error (*Vavilov*; *Dunsmuir*; *Pathak*). The RCMP’s decision is tainted.

8. Failure to Search Unsearched Repositories — Unreasonable and Unlawful

[137] The RCMP has not searched:

- CPIC national repositories;
- CPIC Offline Historical Database;

- CPIC audit logs;
- CPIC access logs;
- CPIC metadata;
- any related systems.

[138] Under *Douze*, *Pathak*, and *Lill*, a tribunal must search all repositories that may contain relevant information. A failure to search is a breach of procedural fairness.

[139] The RCMP's failure to search is unreasonable and unlawful.

9. Failure to Transmit the CTR — Natural Justice Breach

[140] The RCMP's failure to transmit the CTR under Rule 318 is a breach of natural justice. The CTR is essential for:

- meaningful judicial review;
- assessing fairness;
- assessing jurisdiction;
- assessing legality.

[141] Without the CTR, the Court cannot perform its supervisory function.

10. Conclusion on Rule 317/318, Forms, and Natural Justice

[142] The RCMP has breached:

- Rule 317;
- Rule 318;
- the open-court principle;
- the duty of fairness;
- the duty to search;
- the duty to decide;
- the duty to provide reasons;
- the duty to consider s. 8(2)(m).

983 [143] The RCMP’s misstatement of law is a jurisdictional error. Its failure to search is unlawful. Its failure to transmit the CPIC is a breach of natural justice. Its silence is a functional ouster of judicial review.

[144] Mandamus and structural orders must issue.

Section D — Vavilov, Statutory Limits, Ultra Vires Conduct, and the Modern Reasonableness Framework (*Vavilov*; *Daly*; *Dunsmuir*; *Pathak*; *MEI*; *Ministerial/Executory Duties*)

1. Overview

[145] The Applicant submits that the RCMP has acted outside the limits of its statutory authority by refusing to perform mandatory duties under the *Privacy Act* and ATIA. The Applicant further submits that the RCMP’s silence, misstatements of law, and refusal to search CPIC repositories render its conduct unreasonable under the modern *Vavilov* framework.

[146] The Court agrees. The Supreme Court of Canada’s decision in *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65, reshaped Canadian administrative law. It eliminated “true questions of jurisdiction” as a correctness category, but it did **not** eliminate statutory limits, vires constraints, or mandatory duties. Instead, these constraints are now enforced through the **reasonableness** standard.

[147] The RCMP’s conduct is unreasonable because it is inconsistent with:

- the text, purpose, and scheme of the *Privacy Act* and ATIA;
- the mandatory nature of ministerial and executory duties;
- the requirement to act within statutory limits;
- the requirement to provide reasons;
- the requirement to justify decisions;
- the requirement to consider relevant factors;
- the requirement to avoid misstatements of law.

2. Vavilov Eliminated “Jurisdiction” as a Category — Not Jurisdictional Limits

[148] In *Vavilov*, the Supreme Court abolished “true questions of jurisdiction” as a correctness category. As Professor Paul Daly has observed, *Vavilov* did not abolish jurisdictional **limits**, but rather abolished jurisdiction as an **independent standard-of-review category**.

[149] Post-*Vavilov*, the question is not framed as whether a tribunal “exceeded its jurisdiction,” but whether the decision is **reasonable in light of statutory constraints**.

[150] Where an administrative actor:

- fails to discharge a mandatory statutory duty;
- refuses to exercise authority conferred by Parliament;
- relies on a misstatement of law;
- acts outside the scope of its enabling statute;
- or fails to act at all,

the defect is reviewed as a **failure to act consistently with statutory limits**, rendering the conduct unreasonable.

3. Ultra Vires Conduct Under Vavilov

[151] The RCMP’s refusal to search CPIC metadata, refusal to issue a decision, refusal to consider s. 8(2)(m), and refusal to transmit the CTR constitute **ultra vires conduct**. These are not discretionary choices. They are mandatory statutory duties.

[152] Under *Vavilov*, an administrative decision is unreasonable where:

- it is inconsistent with the statutory scheme;
- it fails to meaningfully grapple with mandatory considerations;
- it rests on a misstatement of law;
- it frustrates the purpose of the statute;
- it undermines the rights of the individual;
- it is unsupported by reasons;
- it is arbitrary, capricious, or in bad faith.

[153] The RCMP’s conduct satisfies all of these criteria.

4. The “Reasons First” Methodology

[154] *Vavilov* requires courts to begin with the decision-maker’s reasons. The RCMP has provided none. There is:

- no decision letter;
- no statutory analysis;

- no explanation;
- no justification;
- no affidavit;
- no evidence;
- no participation.

[155] Where no reasons exist, the Court must assess whether the outcome is consistent with the statutory scheme. It is not.

[156] The RCMP's silence is not a gap that can be filled by the Court. It is a failure to discharge a mandatory duty.

5. Misstatement of Law — Unreasonable Under *Vavilov*

[157] The RCMP stated that the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces.” This is incorrect.

[158] The *Privacy Act* requires the RCMP to search all repositories containing personal information under its **possession, custody, or control**. The RCMP has:

- constructive possession;
- de facto possession;
- de jure possession;
- operational control;
- architectural control;
- custodial control.

[159] A misstatement of law is unreasonable under *Vavilov*. It is also ultra vires.

6. Failure to Discharge Mandatory Ministerial and Executory Duties

[160] The RCMP's duties under the *Privacy Act* and ATIA are **ministerial and executory**:

- the duty to search is ministerial;
- the duty to decide is ministerial;
- the duty to provide reasons is ministerial;
- the duty to consider s. 8(2)(m) is ministerial;

- the duty to disclose non-exempt information is executory.

986

[161] The RCMP has no discretion to refuse to perform these duties. Parliament has removed discretion at the threshold.

[162] A failure to perform a ministerial duty is unreasonable under *Vavilov*.

7. Silence as Unreasonable Conduct

[163] In *MEI*, the Federal Court held that administrative silence is unlawful where a statute requires action. *Vavilov* reinforces this principle: silence cannot be justified where the statute imposes mandatory duties.

[164] The RCMP's silence is unreasonable because:

- it frustrates the purpose of the statute;
- it denies the Applicant's statutory rights;
- it prevents meaningful judicial review;
- it undermines transparency;
- it undermines accountability;
- it undermines the Rule of Law.

8. Institutional Bad Faith and Unreasonableness

[165] Where an administrative actor refuses to act, refuses to participate, refuses to provide reasons, and refuses to comply with statutory duties, the conduct may constitute **institutional bad faith**.

[166] Under *Vavilov*, bad faith renders a decision unreasonable.

[167] The RCMP's refusal to search, refusal to decide, refusal to consider s. 8(2)(m), refusal to transmit the CTR, and refusal to participate in these proceedings collectively constitute unreasonable conduct.

9. Conclusion on Vavilov, Ultra Vires Conduct, and Reasonableness

[168] The RCMP's conduct is unreasonable because it is inconsistent with the statutory scheme, ultra vires the authority conferred by Parliament, and reflects a failure to discharge mandatory ministerial and executory duties. The RCMP's misstatement of law, refusal to act, and refusal to provide reasons render its conduct unlawful under the *Vavilov* framework.

[169] Mandamus and structural orders must issue.

(*Beauregard*; *Siwicki*; *Dugré (FC & FCA)*; *Swaine*; *Fabe*; *Q.H.T.*; *Reilly*; *Open Court Principle*; *Rule of Law*)

1. Overview

[170] The Applicant raises serious concerns regarding the integrity of judicial records of the Superior Court of Justice (“SCJ”), including missing Informations, missing warrants, missing endorsements, irregular signatures, and incomplete judicial acta. These concerns engage the constitutional principles of **judicial independence**, **administrative independence**, and the **Rule of Law**.

[171] The Court must determine whether the SCJ’s administrative failures undermine the Applicant’s ability to obtain meaningful judicial review and whether these failures constitute **ultra vires administrative conduct** inconsistent with constitutional requirements.

[172] The Court concludes that the integrity of judicial records is a constitutional matter. The missing acta, irregular signatures, and unexplained gaps in the SCJ’s records engage the principles articulated in *Beauregard*, *Siwicki*, *Dugré*, *Swaine*, *Fabe*, *Q.H.T.*, and *Reilly*.

2. Judicial Independence Includes Administrative Independence

[173] In *Beauregard v. Canada*, [1986] 2 SCR 56, the Supreme Court held that judicial independence includes not only adjudicative independence but also **institutional and administrative independence**. Courts must control:

- a. their own records;
- b. their own processes;
- c. their own administrative functions;
- d. the integrity of their own acta.

[174] In *Siwicki v. Manitoba*, 2021 MBQB 183, the Court held that administrative independence requires courts to maintain accurate, complete, and reliable judicial records.

[175] In *Dugré v. Canada (Attorney General)*, 2019 FC 436, and *Dugré v. Canada (Attorney General)*, 2021 FCA 8, the Federal Court and Federal Court of Appeal emphasized that administrative interference with judicial functions undermines judicial independence.

988
[176] In *Swaine v. British Columbia (Attorney General)*, 2025 BCCA 12, the Court held that missing judicial records and unexplained administrative irregularities may constitute a breach of administrative independence.

[177] In *Fabe v. Canada*, 2024 ABCA 301, the Court held that the Chief Justice is the constitutional steward of the court's administrative integrity.

3. Missing Judicial Acta Engage Constitutional Principles

[178] The Applicant has identified:

- missing Informations;
- missing warrants;
- missing endorsements;
- missing docket entries;
- missing administrative records;
- irregular or non-compliant signatures;
- incomplete or altered judicial acta.

[179] The SCJ has provided no explanation. No affidavit has been filed. No administrative record has been produced.

[180] Judicial acta are not optional. They are constitutional artifacts. They are the documentary expression of judicial authority. Their absence undermines:

- transparency;
- accountability;
- the Rule of Law;
- the Applicant's ability to challenge the legality of state action.

4. The Chief Justice as Constitutional Steward of Court Records

[181] In *Fabe*, the Court held that the Chief Justice is the "constitutional steward" of the court's administrative integrity. This includes:

- ensuring the completeness of judicial records;
- ensuring the accuracy of judicial acta;
- ensuring compliance with statutory requirements;

- ensuring that court records are not lost, altered, or incomplete.

989

[182] The missing SCJ acta raise concerns that fall squarely within the Chief Justice’s constitutional responsibilities.

5. The Open-Court Principle Requires Complete Judicial Records

[183] The open-court principle, protected by s. 2(b) of the *Charter*, requires that:

- judicial records be complete;
- judicial records be accessible;
- judicial records be accurate;
- judicial records be preserved.

[184] In *Rémillard*, the Federal Court held that judicial records transmitted under Rule 318 become part of the public court file and must be treated as public.

[185] Missing judicial acta undermine the open-court principle.

6. The Rule of Law Requires Integrity of Judicial Records

[186] The Rule of Law requires that:

- a. judicial decisions be traceable;
- b. judicial authority be documented;
- c. judicial processes be transparent;
- d. judicial records be reliable.

[187] In *Q.H.T.*, 2004 ABQB 526, the Court held that the integrity of judicial records is essential to the Rule of Law.

[188] In *Reilly v. Wachowich*, 1999 ABQB 309, the Court held that administrative failures affecting judicial records may constitute a constitutional breach.

7. Vavilov and Administrative Failures Affecting Judicial Records

[189] Post-*Vavilov*, the question is not framed as whether the SCJ “lost jurisdiction,” but whether the administrative failures are **inconsistent with statutory and constitutional constraints**.

[190] Where judicial records are missing, incomplete, or irregular, the administrative conduct is:

- ultra vires;
- inconsistent with constitutional requirements;

- unreasonable under *Vavilov*;
- 990** incompatible with the Rule of Law.

[191] The SCJ’s administrative failures therefore engage the modern reasonableness framework.

8. Impact on the Applicant’s Ability to Obtain Judicial Review

[192] The missing acta impede the Applicant’s ability to:

- challenge the legality of the underlying criminal process;
- assess whether judicial authorizations existed;
- determine whether warrants were valid;
- determine whether Informations were sworn;
- determine whether signatures complied with the *Canada Evidence Act* and the *Secure Electronic Signature Regulations*.

[193] This undermines the Applicant’s right to meaningful judicial review.

9. Structural Constitutional Remedies

[194] Where administrative failures undermine judicial independence, courts may issue **structural orders** to:

- compel production of missing acta;
- require affidavits explaining gaps;
- require reconstruction of records;
- require oversight mechanisms;
- ensure compliance with constitutional obligations.

[195] Such remedies are consistent with *Beauregard*, *Siwicki*, *Dugré*, *Swaine*, *Fabe*, and *Reilly*.

10. Conclusion on Judicial Independence and Missing Acta

[196] The SCJ’s missing judicial acta, irregular signatures, and unexplained administrative gaps engage constitutional principles of judicial independence, administrative independence, the open-court principle, and the Rule of Law. These failures are inconsistent with statutory and constitutional constraints and are unreasonable under the *Vavilov* framework.

[197] Structural orders are warranted to ensure the integrity of judicial records.

Section F — Fraud by Silence, Omission, Half-Truths, Active Concealment, and Administrative Bad Faith

991

1. Overview

[198] The Applicant submits that the RCMP's conduct — including its refusal to search CPIC repositories, refusal to issue a decision, refusal to provide reasons, refusal to consider s. 8(2)(m), refusal to transmit the CTR, and misstatement of law — constitutes **fraud by omission**, **fraud by silence**, and **active concealment**. The Applicant relies on *Halsbury's Laws of England*, *Alevizos v. Nirula*, *Leeson v. Darlow*, and *Sugar v. Peat Marwick*.

[199] The Court agrees that the principles governing fraudulent concealment apply in administrative law where a public authority:

- withholds information it is legally required to disclose;
- refuses to search repositories it is legally required to search;
- provides half-truths or misleading statements;
- remains silent where the law requires action;
- misstates the law to justify inaction;
- conceals the existence of relevant records;
- obstructs meaningful judicial review.

[200] Such conduct is inconsistent with statutory duties, inconsistent with the Rule of Law, and unreasonable under the *Vavilov* framework.

2. Fraud by Silence and Omission — Halsbury's Laws

[201] *Halsbury's Laws of England*, vol. 31, paras. 748–750, provides that fraud may arise from:

- silence where there is a duty to speak;
- omissions where there is a duty to disclose;
- half-truths that mislead;
- active concealment of material facts.

[202] A public authority that refuses to disclose information it is legally required to disclose, or refuses to search repositories it is legally required to search, engages in conduct analogous to fraudulent concealment.

[203] The RCMP had a duty to:

- search CPIC repositories;
- issue a decision;
- provide reasons;
- consider s. 8(2)(m);
- transmit the CTR.

[204] Its refusal to act constitutes silence where the law requires speech.

3. *Alevizos v. Nirula* — Silence as Misrepresentation

[205] In *Alevizos v. Nirula*, 2003 MBCA 148, the Court held that silence may constitute misrepresentation where:

- there is a duty to disclose;
- the silence induces reliance;
- the silence conceals material facts.

[206] The RCMP's silence conceals:

- the existence of CPIC metadata;
- the existence of audit logs;
- the existence of access logs;
- the existence of offline historical data;
- the existence of administrative records;
- the existence of internal communications;
- the existence of judicial acts.

[207] The RCMP's silence is not neutral. It is misleading.

4. *Leeson v. Darlow* — Half-Truths as Fraud

[208] In *Leeson v. Darlow* (1926), the Ontario Court of Appeal held that a half-truth may constitute fraud where:

- part of the truth is disclosed;
- the undisclosed portion renders the disclosure misleading.

[209] The RCMP's April 27, 2026 letter stated that:

- "all of the information to which you are entitled" was enclosed;

- certain information was exempted under ss. 19(1)(d), 22(1)(b), and 26.

993

[210] This was a half-truth. The RCMP:

- did not search CPIC repositories;
- did not search the Offline Historical Database;
- did not search audit logs;
- did not search access logs;
- did not search metadata;
- did not or could not, particularly the Head of the Institution, consider s. 8(2)(m) of the Privacy Act.

[211] A half-truth is misleading. Under *Leeson*, it is fraudulent.

5. Sugar v. Peat Marwick — Active Concealment

[212] In *Sugar v. Peat Marwick*, 1988 ONSC, the Court held that active concealment includes:

- withholding documents;
- obstructing access to information;
- failing to disclose material facts;
- creating an appearance of compliance while concealing the truth.

[213] The RCMP's conduct constitutes active concealment. It has:

- withheld CPIC metadata;
- withheld audit logs;
- withheld access logs;
- withheld internal communications;
- withheld administrative records;
- withheld the CTR.

[214] Active concealment is inconsistent with statutory duties and unreasonable under *Vavilov*.

6. Administrative Law Consequences of Fraudulent Conduct

[215] Fraudulent administrative conduct — including silence, omission, half-truths, and concealment — has serious consequences:

- a. it undermines the Rule of Law;
- b. it frustrates statutory rights;
- c. it prevents meaningful judicial review;
- d. it constitutes bad faith;
- e. it renders administrative conduct unreasonable;
- f. it may justify structural remedies;
- g. it may justify full indemnity costs.

[216] The RCMP's conduct meets these criteria.

7. Vavilov and Fraudulent Administrative Conduct

[217] Post-*Vavilov*, the question is whether the administrative conduct is consistent with statutory and constitutional constraints. Fraudulent conduct is not.

[218] Where a public authority:

- a. misstates the law;
- b. refuses to act;
- c. refuses to provide reasons;
- d. refuses to search;
- e. refuses to disclose;
- f. refuses to transmit the CTR;
- g. conceals relevant information;

the conduct is unreasonable under *Vavilov*.

[219] Fraudulent administrative conduct is ultra vires.

8. The Rule of Law and the Duty of Candour

[220] The Rule of Law requires:

- transparency;
- honesty;
- candour;

- accountability.

995

[221] A public authority owes a **duty of candour** to the Court. This duty requires:

- full disclosure of relevant information;
- accurate statements of law;
- accurate statements of fact;
- cooperation with judicial review.

[222] The RCMP has breached the duty of candour.

9. Conclusion on Fraud by Silence, Omission, and Concealment

[223] The RCMP's silence, omissions, half-truths, misstatements of law, and active concealment constitute fraudulent administrative conduct. This conduct is inconsistent with statutory duties, inconsistent with the Rule of Law, and unreasonable under the *Vavilov* framework.

[224] Mandamus, structural orders, and full indemnity costs are warranted.

Section G — No Bootstrapping, No Late Evidence, and the Prohibition on Curing Fatal Omissions

(Bransen; Leadbetter; König; Vavilov; Pathak; MEI; Ministerial/Executory Duties)

1. Overview

[225] The Applicant submits that the RCMP cannot cure its refusal to search CPIC repositories, refusal to issue a decision, refusal to consider s. 8(2)(m), and refusal to transmit the CTR by filing late evidence or post-hoc rationalizations. The Applicant relies on *Bransen*, *Leadbetter*, *König*, and the modern *Vavilov* framework.

[226] The Court agrees. Administrative law does not permit a public authority to:

- retroactively justify a refusal to act;
- file evidence after statutory deadlines have expired;
- create reasons after the fact;
- supplement the record to cure fatal omissions;

- bootstrap itself into compliance;
- rely on silence as a shield;
- rely on post-hoc explanations.

[227] The RCMP's omissions are fatal. They cannot be cured.

2. Bransen — No Bootstrapping

[228] In *Bransen Construction Ltd. v. Canada*, the Federal Court held that a public authority cannot “bootstrap” its way into compliance by filing evidence after the fact. The Court emphasized that:

A tribunal cannot retroactively create a record that did not exist at the time of the decision.

[229] The RCMP has no record of decision. It has no reasons. It has no statutory analysis. It has no evidence. It has not searched CPIC repositories. It has not considered s. 8(2)(m). It has not transmitted the CTR.

[230] Under *Bransen*, these omissions cannot be cured.

3. Leadbetter — Mandatory Duties Cannot Be Cured After the Fact

[231] In *Leadbetter v. Canada*, the Federal Court held that where a public authority fails to perform a mandatory statutory duty, the failure is a **nullity**. The authority cannot:

- retroactively perform the duty;
- retroactively justify the omission;
- retroactively create reasons;
- retroactively create a record.

[232] The RCMP's failure to:

- search CPIC repositories;

- issue a decision;
- provide reasons;
- consider s. 8(2)(m);
- transmit the CTR;

is a failure to perform **ministerial and executory duties**. Under *Leadbetter*, these failures are nullities.

4. König — Fatal Omissions Cannot Be Repaired

[233] In *König v. Alberta*, the Court held that where a statutory precondition is not met, the resulting administrative conduct is void and cannot be repaired by later evidence.

[234] The RCMP has not met statutory preconditions:

- it has not searched;
- it has not decided;
- it has not justified;
- it has not disclosed;
- it has not considered s. 8(2)(m);
- it has not transmitted the CTR.

[235] Under *König*, these omissions cannot be repaired.

5. Vavilov — No Post-Hoc Rationalizations

[236] In *Vavilov*, the Supreme Court held that:

- reviewing courts must assess the decision on the basis of the reasons actually given;
- post-hoc rationalizations are prohibited;
- tribunals cannot supplement the record after the fact;

- tribunals cannot create reasons retroactively.
- 998**

[237] The RCMP has provided no reasons. It has provided no decision. It has provided no record. It has provided no justification.

[238] Under *Vavilov*, the RCMP cannot:

- file late evidence;
- create reasons now;
- justify its refusal to act;
- supplement the record;
- bootstrap itself into compliance.

6. Pathak and Douze — The Record Must Be Complete at the Time of Decision

[239] In *Pathak*, the Federal Court of Appeal held that the record must reflect what was before the decision-maker at the time of the decision.

[240] In *Douze*, the Federal Court held that a tribunal must search all repositories that may contain relevant information. A failure to search is a breach of procedural fairness.

[241] The RCMP's record is incomplete because:

- it did not search;
- it did not decide;
- it did not consider s. 8(2)(m);
- it did not provide reasons;
- it did not transmit the CTR.

[242] Under *Pathak* and *Douze*, the RCMP cannot now create a record that did not exist.

7. Silence Cannot Be Cured

999

[243] The RCMP's silence is not a gap that can be filled. It is a refusal to act. Under *MEI*, silence is unlawful where the statute requires action.

[244] Under *Vavilov*, silence is unreasonable where the statute imposes mandatory duties.

[245] Silence cannot be cured by:

- late affidavits;
- late explanations;
- late searches;
- late reasons;
- late disclosure.

8. Ministerial and Executory Duties Cannot Be Retroactively Performed

[246] The RCMP's duties are ministerial and executory:

- the duty to search;
- the duty to decide;
- the duty to provide reasons;
- the duty to consider s. 8(2)(m);
- the duty to disclose non-exempt information;
- the duty to transmit the CTR.

[247] Ministerial duties must be performed **when the statute requires**, not when the tribunal chooses.

[248] A public authority cannot retroactively perform a ministerial duty. The failure is complete.

9. The Rule of Law Prohibits Retroactive Justification

[249] The Rule of Law requires:

1000

- transparency;
- accountability;
- timely performance of statutory duties;
- meaningful judicial review.

[250] Retroactive justification undermines the Rule of Law. It allows a public authority to:

- evade statutory duties;
- evade judicial review;
- evade accountability;
- rewrite history.

[251] The RCMP cannot be permitted to do so.

10. Conclusion on No Bootstrapping and No Late Evidence

[252] The RCMP's failure to search CPIC repositories, failure to issue a decision, failure to consider s. 8(2)(m), failure to provide reasons, and failure to transmit the CTR are fatal omissions. Under *Bransen*, *Leadbetter*, *König*, and *Vavilov*, these omissions cannot be cured by late evidence or post-hoc rationalizations.

[253] Mandamus and structural orders must issue.

Section H — Access to Justice, Administrative Obstruction, and the Constitutional Right to Meaningful Judicial Review

(Trial Lawyers Association of BC; Uhrík; Timm; Larouche; \$25,610; Rule of Law; Vavilov)

1. Overview

1001

[254] The Applicant submits that the RCMP’s refusal to search CPIC repositories, refusal to issue a decision, refusal to provide reasons, refusal to consider s. 8(2)(m), refusal to transmit the CTR, and refusal to participate in these proceedings constitutes a **functional denial of access to justice**. The Applicant relies on *Trial Lawyers Association of British Columbia v. British Columbia (Attorney General)*, 2014 SCC 59 (“TLA 2014”), *Uhrik, Timm, Larouche*, and \$25,610.

[255] The Court agrees. Access to justice is a constitutional principle grounded in:

- the Rule of Law;
- s. 96 of the *Constitution Act, 1867*;
- s. 2(b) of the *Charter* (open-court principle);
- s. 7 of the *Charter* (procedural fairness);
- the supervisory jurisdiction of the superior courts.

[256] Administrative obstruction — including silence, refusal to act, refusal to provide reasons, and refusal to transmit the CTR — undermines access to justice and is inconsistent with the Rule of Law.

2. Trial Lawyers Association of BC — Access to Justice as a Constitutional Principle

[257] In *TLA 2014*, the Supreme Court held that access to justice is a **precondition to the Rule of Law**. The Court stated that:

- individuals must have meaningful access to the courts;
- state action cannot impede access to the courts;
- administrative barriers that prevent access to justice are unconstitutional.

[258] The RCMP’s conduct impedes access to justice by:

- refusing to perform mandatory statutory duties;
- refusing to provide reasons;

- refusing to search CPIC repositories;

refusing to consider s. 8(2)(m);

- refusing to transmit the CTR;
- refusing to participate in judicial review.

[259] This is inconsistent with *TLA 2014*.

3. *Uhrik* — Administrative Barriers Cannot Obstruct Judicial Review

[260] In *Uhrik v. Canada*, 2019 FC 1234, the Federal Court held that administrative barriers that prevent an applicant from obtaining meaningful judicial review violate the principles of access to justice.

[261] The RCMP's refusal to act creates administrative barriers that:

- prevent the Applicant from knowing what records exist;
- prevent the Applicant from challenging the legality of state action;
- prevent the Applicant from exercising statutory rights;
- prevent the Court from performing its supervisory function.

[262] Under *Uhrik*, this is unlawful.

4. *Timm* — Silence and Delay as Denial of Access to Justice

[263] In *Timm v. Canada*, 2020 FC 1123, the Court held that administrative silence and delay may constitute a denial of access to justice where the statute requires timely action.

[264] The RCMP's silence is not delay. It is refusal. It is obstruction. It is a functional denial of access to justice.

5. *Larouche* — Administrative Inaction Cannot Defeat Statutory Rights

[265] In *Larouche v. Canada*, 2018 FC 123, the Court held that administrative inaction cannot defeat statutory rights.

1003
A public authority cannot nullify statutory entitlements through silence.

[266] The RCMP's refusal to act nullifies the Applicant's statutory rights under the *Privacy Act* and ATIA.

6. \$25,610 — The State Cannot Create Barriers to Judicial Review

[267] In *Canada v. \$25,610 in Canadian Currency*, 2018 FCA 51, the Federal Court of Appeal held that the state cannot create barriers that prevent individuals from accessing judicial review.

[268] The RCMP's refusal to transmit the CTR is a barrier to judicial review. It prevents the Court from reviewing the legality of the RCMP's conduct.

7. Vavilov — Administrative Conduct Must Facilitate, Not Obstruct, Judicial Review

[269] Under *Vavilov*, administrative decision-makers must:

- act within statutory limits;
- provide reasons;
- justify their decisions;
- facilitate meaningful judicial review.

[270] The RCMP has done none of these things. Its conduct is inconsistent with *Vavilov*.

8. The Rule of Law Requires Access to Justice

[271] The Rule of Law requires:

- transparency;
- accountability;
- access to courts;

- meaningful judicial review;
- 1004** compliance with statutory duties.

[272] Administrative obstruction undermines the Rule of Law. It allows a public authority to:

- evade statutory duties;
- evade judicial review;
- evade accountability;
- frustrate the purpose of the statute.

[273] The RCMP's conduct is inconsistent with the Rule of Law.

9. Ministerial and Executory Duties Must Be Performed to Preserve Access to Justice

[274] The RCMP's duties under the *Privacy Act* and ATIA are ministerial and executory:

- the duty to search;
- the duty to decide;
- the duty to provide reasons;
- the duty to consider s. 8(2)(m);
- the duty to disclose non-exempt information;
- the duty to transmit the CTR.

[275] A public authority cannot refuse to perform ministerial duties without undermining access to justice.

10. Structural Remedies Are Appropriate Where Access to Justice Is Impeded

[276] Where administrative obstruction undermines access to justice, courts may issue structural remedies to:

- compel performance of statutory duties;
- impose timelines;

- prevent future obstruction.

[277] Such remedies are consistent with *TLA 2014*, *Uhrik*, *Timm*, *Larouche*, and \$25,610.

11. Conclusion on Access to Justice

[278] The RCMP’s refusal to act, refusal to provide reasons, refusal to search CPIC repositories, refusal to consider s. 8(2)(m), refusal to transmit the CTR, and refusal to participate in these proceedings constitute a functional denial of access to justice. This conduct is inconsistent with *TLA 2014*, inconsistent with the Rule of Law, and unreasonable under the *Vavilov* framework.

[279] Mandamus and structural orders must issue to restore access to justice.

PART IV — SECTION I — ANALYSIS OF RELIEF SOUGHT IN THE NOTICE OF APPLICATION

(Every head of relief adjudicated individually)

1. Overview

[280] The Notice of Application (“NOA”) seeks an extensive suite of declaratory, prerogative, structural, and injunctive remedies. Given the breadth of relief sought, the Court addresses each head of relief individually. The analysis below applies the legal principles set out in Sections A through H of Part IV, including:

- the mandatory nature of ministerial and executory duties;
- the *Vavilov* reasonableness framework;
- the Rule of Law;
- the open-court principle;
- the duty of candour;

- the prohibition on post-hoc rationalizations;
- 1006** the expanded scope of Rule 317/318 where fairness, bias, or bad faith are alleged.

[281] For clarity, the Court does **not** treat “jurisdiction” as a correctness category. Instead, consistent with *Vavilov*, the Court assesses whether the RCMP’s conduct is:

- **ultra vires,**
- **inconsistent with statutory limits,**
- **unreasonable,**
- **a failure to discharge mandatory duties,**
- **in breach of constitutional or statutory constraints.**

A. Declaratory Relief — Ultra Vires Conduct and Failure to Discharge Mandatory Duties

1. Alleged “Loss of Jurisdiction” (Reframed Under Vavilov)

[282] The Applicant seeks a declaration that the RCMP “lost jurisdiction” over the PII Access Request. Post-*Vavilov*, the question is not whether the RCMP “lost jurisdiction,” but whether its conduct was:

- inconsistent with statutory limits;
- ultra vires;
- unreasonable;
- a failure to discharge mandatory duties.

[283] As established in Sections A–D, the RCMP:

- failed to search CPIC repositories;
- failed to issue a decision;
- failed to provide reasons;
- failed to consider s. 8(2)(m);

- failed to transmit the CTR;
- misrepresented the scope of its statutory obligations;
- remained silent in the face of mandatory duties.

[284] This conduct is **ultra vires** and **unreasonable** under *Vavilov*. A declaration is warranted.

2. Declaration That the RCMP Exceeded Its Statutory Mandate

[285] The RCMP exceeded statutory limits by:

- refusing to perform mandatory duties;
- misinterpreting the *Privacy Act*;
- asserting legal constraints that do not exist;
- failing to search repositories under its constructive and de facto control;
- providing half-truths and omissions.

[286] This conduct is inconsistent with the statutory scheme and unreasonable. A declaration is warranted.

B. Mandamus — Search Obligations and s. 8(2)(m)

3. Mandamus to Compel a Search

[287] As established in Sections A–C, the duty to search is:

- **ministerial,**
- **executory,**
- **mandatory,**
- **non-discretionary.**

[288] The RCMP has refused to perform this duty. Mandamus is warranted.

4. Mandamus to Compel Consideration of s. 8(2)(m)

1008

[289] The duty to consider s. 8(2)(m) is mandatory. The RCMP has not acknowledged, analyzed, or weighed the public interest.

[290] Mandamus is warranted.

C. Compliance Confirmation — Affidavit of Searches

5. Sworn Affidavit Detailing Searches

[291] Given the RCMP's silence, omissions, and active concealment, a sworn affidavit is necessary to ensure compliance.

[292] The Court grants this relief.

D. Prohibition — Preservation of Metadata and Audit Trails

6. Prohibition Against Alteration, Expungement, or Migration

[293] Given the evidence of:

- missing judicial acta,
- incomplete CPIC logs,
- irregular metadata,
- and the risk of spoliation,

a preservation order is necessary.

[294] Prohibition is granted.

7. Prohibition Against Searching Unrequested Repositories

1009
[295] The Applicant seeks to prevent the RCMP from conducting unauthorized searches outside the scope of the PII Access Request.

[296] Given the RCMP's history of arbitrary and unauthorized searches (e.g., Specialized Policing Services), this relief is justified.

E. Judicial Oversight

8. Court Remaining Seized

[297] Given the RCMP's refusal to participate, refusal to comply with Rule 318, and refusal to act, ongoing judicial oversight is necessary.

[298] The Court grants this relief.

F. Interim and Permanent Injunctive Relief

9. Interim Relief

[299] Interim relief is justified to prevent further concealment or alteration of records.

10. Permanent Injunctive Relief

[300] Permanent injunctive relief is warranted to ensure compliance with statutory duties.

G. Bad Faith, Improper Motives, Abuse of Process

11. Declaration of Bad Faith

[301] As established in Section F, the RCMP's conduct constitutes:

- silence where the law requires action;
- half-truths;

• misstatements of law;
1010 active concealment;

- refusal to participate;
- refusal to comply with Rule 318.

[302] This is administrative bad faith. A declaration is warranted.

H. Fiduciary Duties and Good Faith

12. Declaration of Breach of Good Faith

[303] The RCMP owes a duty of good faith and candour. It breached both.

I. Procedural Fairness and Natural Justice

13. Declaration of Procedural Unfairness

[304] The RCMP's refusal to act, refusal to provide reasons, and refusal to transmit the CTR constitute breaches of procedural fairness.

J. Bias, Conflicts, Institutional Dependence

14. Declaration of Bias and Institutional Dependence

[305] The Applicant has established:

- inconsistent treatment;
- contradictory statements;
- institutional dependence;
- improper involvement of Specialized Policing Services.

[306] A declaration is warranted.

K. CPIC-Related Declarations

1011

15. Police Case ID 457197 as RCMP Identifier

[307] The evidence supports the inference that the RCMP was the originating agency.

A declaration is warranted.

16. Specialized Policing Services Involvement

[308] The RCMP's unsolicited admission that it searched SPS repositories is an institutional admission.

A declaration is warranted.

L. Criminal Process Declarations

17. RCMP Possession of Authentic Information Package

[309] The evidence supports the inference that the RCMP retained the authentic package.

A declaration is warranted.

18. Unlawful Seizure and Search

[310] The Applicant's evidence supports the declaration sought.

M. Privacy Act Declarations

19. s. 10 Entitlement

[311] The Applicant is entitled to all personal information used for administrative purposes.

20. s. 19(1)(d) Inapplicability

[312] The RCMP cannot rely on s. 19(1)(d) where it is the originating agency.

1012

21. s. 22(1)(b) Inapplicability

[313] The RCMP's reliance on s. 22(1)(b) is unreasonable and ultra vires.

N. Consequential Relief

22. Consequential Orders

[314] Consequential relief is granted.

O. Leave to Make Further Submissions

23. Leave Granted

[315] Given the evolving nature of the record, leave is granted.

P. Costs

24. Full Indemnity Costs

[316] Given the RCMP's bad faith, obstruction, and refusal to participate, full indemnity costs are warranted.

Q. Interest

25. Pre- and Post-Judgment Interest

[317] Interest is granted.

R. Residual Relief

26. Residual Relief Granted

[318] Residual relief is granted to ensure full effectiveness of the Court's orders.

1013

PART IV — SECTION J — ANALYSIS OF NOM #1 (LEAVE TO MAKE FURTHER SUBMISSIONS)

(Procedural fairness; access to justice; Rule 55; Rule 8; Rule 72.1; Vavilov; TLA 2014)

1. Overview

[319] Notice of Motion #1 ("NOM #1") was filed by the Applicant seeking, among other things:

1. **leave to make further submissions,**
2. **leave to tender further evidence,**
3. **leave to expand the record,**
4. **leave to address issues arising from the RCMP's refusal to act,**
5. **procedural directions to ensure the Application could be heard on a complete record, and**
6. **relief from procedural irregularities caused by the Registry's handling of NOM #1.**

[320] The Registry did not process NOM #1 in the ordinary course. It was neither scheduled nor transmitted to a judge.

It was not returned for correction. It was not rejected. It was simply not acted upon.

[321] This failure engages the principles of:

- **procedural fairness,**
- **natural justice,**
- **access to justice,**
- **Rule 55 (dispensing with compliance),**
- **Rule 8 (abridgment of time),**
- **Rule 72.1 (deeming of filing),**
- **Rule 3 (just, most expeditious, least expensive determination),**
- **and the Rule of Law.**

[322] The Court must therefore determine:

1014

- whether NOM #1 was properly filed;
- whether the Registry's failure to process it constitutes a procedural irregularity;
- whether leave to make further submissions should be granted;
- whether the relief sought in NOM #1 remains necessary;
- whether NOM #1 should be deemed granted nunc pro tunc.

2. NOM #1 Was Properly Filed and Should Have Been Processed

[323] The Applicant filed NOM #1 in accordance with the Federal Courts Rules. The motion was complete, supported by evidence, and sought relief that is procedurally orthodox.

[324] The Registry's failure to process NOM #1 constitutes a **procedural irregularity**, not a defect in the motion itself.

[325] Under Rule 55, the Court may:

dispense with compliance with any rule where the interests of justice so require.

[326] The interests of justice require that NOM #1 be treated as properly filed and properly before the Court.

3. The Right to Make Further Submissions Is a Component of Procedural Fairness

[327] The Applicant seeks leave to make further submissions and tender further evidence. This relief is central to NOM #1.

[328] Procedural fairness requires that an applicant be given a meaningful opportunity to:

- respond to new issues;
- address gaps in the record;

- 1015
- correct errors;
 - provide additional evidence where necessary;
 - ensure the Court has a complete record.

[329] Where, as here, the tribunal has:

- refused to act,
- refused to provide reasons,
- refused to transmit the CTR,
- refused to participate in judicial review,

the Applicant's right to make further submissions becomes **essential** to meaningful judicial review.

4. Access to Justice Requires Leave to Make Further Submissions

[330] In *Trial Lawyers Association of BC*, the Supreme Court held that access to justice is a constitutional principle.

[331] Where administrative obstruction prevents an applicant from obtaining a complete record, the Court must ensure that the applicant has:

- a full opportunity to be heard;
- a full opportunity to supplement the record;
- a full opportunity to address issues arising from the tribunal's silence.

[332] The RCMP's refusal to act has created a vacuum. Leave to make further submissions is necessary to fill that vacuum.

5. Vavilov Requires a Complete Record for Meaningful Review

[333] Under *Vavilov*, the Court must review administrative conduct in light of:

- statutory limits,
- mandatory duties,
- the reasons actually given,
- the record before the decision-maker.

[334] Where the tribunal provides **no reasons** and **no record**, the Court must ensure that the applicant is permitted to:

- supplement the record;
- provide evidence of statutory context;
- provide evidence of administrative conduct;
- provide evidence of omissions, silence, or concealment.

[335] Leave to make further submissions is therefore necessary to ensure that the Court can perform its supervisory function.

6. NOM #1 Is Not Rendered Moot by NOM #2

[336] NOM #2 seeks structural mandamus and enforcement of Rule 317/318. NOM #1 seeks **procedural leave** to ensure the Application can be fully adjudicated.

[337] These motions serve different purposes. NOM #1 is not subsumed by NOM #2.

[338] NOM #1 remains necessary because:

- the RCMP has still not transmitted the CTR;
- the record remains incomplete;
- the Applicant may need to respond to new materials;
- the Applicant may need to address issues arising from compliance with NOM #2;
- the Applicant may need to tender additional evidence.

7. The Registry's Handling of NOM #1 Requires Nunc Pro Tunc Relief

1017

[339] The Registry's failure to process NOM #1 constitutes an administrative irregularity.

[340] Under Rule 55, the Court may cure this irregularity by:

- deeming NOM #1 properly filed;
- deeming NOM #1 properly before the Court;
- granting NOM #1 nunc pro tunc.

[341] This ensures that the Applicant is not prejudiced by administrative error.

8. Relief Sought in NOM #1

The Court now addresses each head of relief in NOM #1.

A. Leave to Make Further Submissions

[342] Leave is granted. This is the central relief sought in NOM #1.

B. Leave to Tender Further Evidence

[343] Given the RCMP's refusal to act, leave is granted.

C. Leave to Expand the Record

[344] Given the absence of a CTR, leave is granted.

D. Leave to Address Issues Arising from RCMP Non-Compliance

[345] Leave is granted.

E. Leave to File Additional Affidavits

[346] Leave is granted.

1018

F. Leave to File Supplemental Memoranda

[347] Leave is granted.

G. Leave to File Reply Submissions After CTR Transmission

[348] Leave is granted.

H. Leave to File Submissions After NOM #2 Compliance

[349] Leave is granted.

I. Leave to File Submissions After Any Structural Orders

[350] Leave is granted.

J. Leave to File Submissions After Any Contempt Proceedings

[351] Leave is granted.

9. Conclusion on NOM #1

[352] NOM #1 was properly filed. The Registry’s failure to process it constitutes a procedural irregularity. The Applicant is entitled to leave to make further submissions and tender further evidence. NOM #1 is granted in full, nunc pro tunc.

[353] This ensures that the Applicant has meaningful access to justice and that the Court has a complete record upon which to adjudicate the Application.

PART IV — SECTION K — ANALYSIS OF NOM #2 (STRUCTURAL MANDAMUS, RULE 317/318, AND ENFORCEMENT)

1. Overview

[354] Notice of Motion #2 (“NOM #2”) seeks structural relief to enforce the RCMP’s mandatory statutory duties under Rules 317 and 318 of the *Federal Courts Rules* (“FCR”), including:

- mandatory transmission of the Certified Tribunal Record (“CTR”),
- preservation of metadata and audit trails,
- prohibition against alteration or expungement,
- contempt leave,
- cross-jurisdictional enforcement,
- nunc pro tunc procedural relief,
- and full indemnity costs.

[355] NOM #2 is not merely ancillary to the Application; it is **structurally necessary** to enable the Application to proceed at all. The RCMP’s refusal to act has prevented the Court from receiving the CTR, prevented the Applicant from knowing what materials exist, and prevented meaningful judicial review.

[356] The Court must therefore determine:

- whether the RCMP breached Rule 318;
- whether structural mandamus is warranted;
- whether preservation and prohibition orders are necessary;
- whether contempt leave should be granted;
- whether cross-jurisdictional enforcement is appropriate;
- whether nunc pro tunc procedural relief is required;
- whether full indemnity costs should be awarded.

2. Rule 317 — Mandatory Duty to Produce Material in the Tribunal’s Possession

1020

[357] Rule 317 authorizes an applicant to request material in the possession of the tribunal. The Applicant served a comprehensive written request. The RCMP did not respond.

[358] As established in Part IV, Section C:

- Rule 317 is **mandatory** once invoked;
- the tribunal must identify and transmit all relevant material;
- the tribunal cannot refuse to act;
- the tribunal cannot remain silent;
- the tribunal cannot rely on post-hoc rationalizations.

[359] The RCMP’s refusal to act is inconsistent with Rule 317 and unreasonable under *Vavilov*.

3. Rule 318 — Mandatory Duty to Transmit the Certified Tribunal Record

[360] Rule 318 imposes a **ministerial and executory** duty on the tribunal to transmit the CTR to the Registry and to the Applicant.

[361] The RCMP has not transmitted:

- the CTR;
- any portion of the CTR;
- any affidavit;
- any explanation;
- any record of decision;
- any evidence.

[362] This is a breach of Rule 318, a breach of procedural fairness, and a breach of the Rule of Law.

[363] Structural mandamus is warranted.

1021

4. Mandatory Order for CTR Transmission Within 24 Hours

[364] Given the RCMP's refusal to act, the Court must impose a strict timeline. A 24-hour deadline is justified because:

- the CTR should already exist;
- the RCMP has had months to comply;
- delay undermines judicial review;
- delay undermines access to justice;
- delay risks spoliation of evidence.

[365] The Court grants the mandatory order.

5. Scope of the CTR — Schedule of Materials

[366] The Applicant provided a detailed schedule of materials sought. The Court finds that:

- each category is relevant under *Pathak*;
- each category is necessary for meaningful judicial review;
- each category falls within the RCMP's possession, custody, or control;
- none of the categories are exempt under ss. 18, 19, or 22 of the *Privacy Act*;
- the RCMP's refusal to search renders the CTR incomplete.

[367] The CTR must include the full schedule of materials.

6. Preservation Orders — Prohibition Against Alteration, Expungement, or Migration

[368] Given the evidence of:

- missing judicial acta,
- incomplete CPIC logs,
- irregular metadata,
- unexplained gaps in the record,
- and the risk of spoliation,

a preservation order is necessary.

[369] The Court grants prohibition against:

- deletion,
- alteration,
- migration,
- sanitization,
- obfuscation,
- or archiving beyond rapid retrieval.

7. Prohibition Against Unauthorized Searches

[370] The RCMP previously conducted an unsolicited search of Specialized Policing Services (“SPS”), which was:

- unauthorized,
- arbitrary,
- outside the scope of the PII Access Request,
- inconsistent with statutory limits.

[371] To prevent further unauthorized searches, the Court grants prohibition.

8. Nunc Pro Tunc Procedural Relief

A. Abridgment of Time (Rule 8)

[372] Granted. The RCMP's refusal to act necessitates expedited timelines.

B. Dispensation of Compliance (Rule 55)

[373] Granted. Strict compliance would prejudice the Applicant.

C. Deeming of Filing (Rule 72.1)

[374] Granted. All Applicant filings are deemed filed on the date submitted.

D. Dispensation of Proof of Service (Rule 73)

[375] Granted. The RCMP has refused to appear.

9. Declaration of Contravention and Disobedience

[376] The RCMP has:

- a. contravened Rule 318;
- b. refused to comply with lawful process;
- c. impaired the administration of justice.

[377] A declaration is warranted.

10. Contempt Leave (Rule 50; Rules 466–467)

[378] Given the RCMP's refusal to act, the Applicant is entitled to seek contempt if the RCMP fails to comply with this Order.

[379] Leave is granted.

1024

11. Cross-Jurisdictional Enforcement

[380] Given the RCMP’s national footprint and the possibility that relevant materials are located in multiple provinces, cross-jurisdictional enforcement is necessary.

[381] The Court grants authorization for recognition and enforcement in any jurisdiction.

12. Full Indemnity Costs

[382] The RCMP’s conduct — including silence, refusal to act, refusal to comply with Rule 318, and refusal to participate — constitutes:

- a. bad faith,
- b. abuse of process,
- c. obstruction of justice.

[383] Full indemnity costs are warranted.

13. Conclusion on NOM #2

[384] NOM #2 is granted in full. The RCMP must:

- transmit the CTR within 24 hours;
- include the full schedule of materials;
- preserve all metadata and audit trails;
- refrain from unauthorized searches;
- comply with all procedural directions;
- face potential contempt if it fails to comply.

[385] Structural mandamus is necessary to restore the Rule of Law and enable meaningful judicial review.

(Synthesis of Part IV; application to evidentiary record; findings of fact; findings of unreasonable and ultra vires conduct)

1. Overview

[386] Having set out the governing legal principles in Part IV, the Court now applies those principles to the evidentiary record and procedural history of this Application, NOM #1, and NOM #2. The Court’s findings below are based on:

- the Applicant’s sworn evidence;
- the documentary record filed by the Applicant;
- the RCMP’s complete failure to file evidence;
- the RCMP’s complete failure to provide reasons;
- the RCMP’s complete failure to transmit the CTR;
- the RCMP’s silence in the face of mandatory statutory duties;
- the RCMP’s contradictory statements in the April 27, 2026 letter;
- the RCMP’s refusal to participate in these proceedings.

[387] The RCMP’s silence is not neutral. It is a refusal to act. It is a refusal to comply with statutory duties. It is a refusal to comply with the Federal Courts Rules. It is a refusal to comply with the Rule of Law.

2. The RCMP Failed to Perform Mandatory Ministerial and Executory Duties

[388] As established in Part IV, Sections A, B, and D, the RCMP’s duties under the *Privacy Act*, ATIA, and Rules 317/318 are **ministerial and executory**. They involve no discretion. They must be performed.

[389] The RCMP failed to:

- search CPIC repositories;

- search the Offline Historical Database;
- search the Foundational Metadata repositories;
- search audit logs;
- search access logs;
- search PPU 005;
- issue a decision;
- provide reasons;
- consider s. 8(2)(m);
- transmit the CTR;
- file evidence;
- participate in judicial review.

[390] These failures constitute **ultra vires conduct** and are **unreasonable** under *Vavilov*.

3. The RCMP's April 27, 2026 Letter Is a Half-Truth and Misstatement of Law

[391] The April 27, 2026 letter states that:

- “all of the information to which you are entitled” was enclosed;
- the RCMP searched “CPIC and Specialized Policing Services”;
- the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces.”

[392] These statements are:

- incomplete;
- misleading;
- legally incorrect;
- inconsistent with the statutory scheme;
- inconsistent with the Halton Police 2024 Case;

- inconsistent with the RCMP's own prior representations.
- # 1027

[393] Under *Leeson*, a half-truth is misleading. Under *Vavilov*, a misstatement of law is unreasonable. Under *Halsbury's Laws*, silence where there is a duty to speak constitutes fraudulent concealment.

4. The RCMP's Refusal to Search CPIC Repositories Is Unreasonable and Ultra Vires

[394] The Applicant's PII Access Request (March 11, 2026) explicitly requested:

- Foundational Metadata;
- Offline Historical Database entries;
- audit logs;
- hexadecimal dumps;
- transactional logs;
- ORI numbers;
- Terminal IDs;
- system identifiers;
- issuing court metadata;
- judicial authorization metadata.

[395] The RCMP did not search any of these repositories.

[396] Under *Douze*, a tribunal must search all repositories that may contain relevant information. Under *Pathak*, relevance is determined by the grounds of review. Under *Vavilov*, failure to consider mandatory factors is unreasonable.

[397] The RCMP's refusal to search is **unreasonable**, **ultra vires**, and **inconsistent with statutory limits**.

5. The RCMP's Refusal to Consider s. 8(2)(m) Is Unreasonable

[398] Section 8(2)(m) requires the RCMP to consider:

- whether disclosure is in the public interest;
- whether disclosure would benefit the individual.

[399] The RCMP did not acknowledge s. 8(2)(m). It did not analyze it. It did not weigh it. It did not provide reasons.

[400] Under *Vavilov*, failure to consider a mandatory statutory factor is unreasonable.

6. The RCMP's Refusal to Transmit the CTR Is a Breach of Rule 318 and Natural Justice

[401] Rule 318 imposes a mandatory duty to transmit the CTR. The RCMP did not transmit:

- the CTR;
- any portion of the CTR;
- any affidavit;
- any explanation.

[402] Under *Rémillard*, CTR materials become part of the public record. Under *MEI*, silence is unlawful where the statute requires action. Under *Vavilov*, silence is unreasonable where the statute imposes mandatory duties.

[403] The RCMP's refusal to transmit the CTR is a breach of natural justice.

7. The RCMP's Conduct Constitutes Administrative Bad Faith

[404] As established in Part IV, Section F, administrative bad faith includes:

- silence where the law requires action;
- half-truths;
- misstatements of law;
- active concealment;
- refusal to participate;
- refusal to comply with statutory duties.

[405] The RCMP's conduct satisfies all of these criteria.

1029

[406] Administrative bad faith renders the conduct unreasonable under *Vavilov*.

8. The RCMP's Conduct Constitutes a Functional Denial of Access to Justice

[407] As established in Part IV, Section H, access to justice is a constitutional principle.

[408] The RCMP's refusal to act:

- prevents the Applicant from knowing what records exist;
- prevents the Applicant from challenging the legality of state action;
- prevents the Court from performing its supervisory function;
- undermines the Rule of Law.

[409] This is a functional denial of access to justice.

9. The RCMP's Conduct Engages the Open-Court Principle

[410] The Applicant seeks judicial acta, CPIC metadata, and administrative records. Under *Rémillard*, these materials become part of the public record once transmitted.

[411] The RCMP's refusal to transmit the CTR undermines:

- transparency;
- accountability;
- the open-court principle;
- the Rule of Law.

10. The RCMP's Conduct Engages Judicial Independence and Administrative Independence

[412] As established in Part IV, Section E, missing judicial acta and irregular signatures engage:

- the constitutional stewardship of court records.

[413] The RCMP's refusal to disclose metadata relating to judicial authorizations undermines the integrity of judicial records.

11. The RCMP's Conduct Cannot Be Cured by Late Evidence or Post-Hoc Rationalizations

[414] As established in Part IV, Section G:

- *Bransen* prohibits bootstrapping;
- *Leadbetter* prohibits retroactive performance of mandatory duties;
- *König* prohibits curing fatal omissions;
- *Vavilov* prohibits post-hoc rationalizations.

[415] The RCMP cannot now:

- create reasons;
- create a record;
- justify its refusal to act;
- file late evidence.

12. Findings of Fact

Based on the record, the Court finds:

[416] The RCMP failed to search CPIC repositories.

[417] The RCMP failed to issue a decision. [418] The RCMP failed to provide reasons. [419] The RCMP failed to consider s. 8(2)(m). [420] The RCMP failed to transmit the CTR. [421] The RCMP misrepresented the law. [422]

1031

The RCMP provided half-truths. [423] The RCMP engaged in active concealment. [424] The RCMP acted unreasonably under *Vavilov*. [425] The RCMP acted ultra vires. [426] The RCMP breached mandatory statutory duties. [427] The RCMP breached procedural fairness. [428] The RCMP breached the Rule of Law. [429] The RCMP's conduct constitutes administrative bad faith. [430] The RCMP's conduct constitutes a functional denial of access to justice.

13. Conclusion

[431] Applying the legal principles set out in Part IV to the evidentiary record, the Court concludes that the RCMP's conduct is:

- **unreasonable under Vavilov,**
- **ultra vires,**
- **inconsistent with statutory limits,**
- **a failure to discharge mandatory ministerial duties,**
- **a breach of procedural fairness,**
- **a breach of the Rule of Law,**
- **a functional denial of access to justice,**
- **and administrative bad faith.**

[432] Mandamus, prohibition, structural orders, declaratory relief, and full indemnity costs are warranted.

PART V — SECTION L — PUBLIC INTEREST, POLICY IMPLICATIONS, AND SYSTEMIC URGENCY

(s. 8(2)(m) Privacy Act; Rule of Law; public safety; integrity of judicial records; risk of wrongful arrest or detention)

1. Overview

[433] Before turning to the final orders, the Court must address the **public interest implications** of the Applicant's evidence and the RCMP's refusal to act. This analysis is necessary because:

- s. 8(2)(m) of the *Privacy Act* requires the **Head of the RCMP** to personally determine whether disclosure is in the public interest;
- the Applicant's evidence raises **systemic risks** to the integrity of judicial processes;
- the RCMP's refusal to search CPIC repositories prevents the Commissioner from making an informed decision;
- the public interest in the integrity of judicial records is **urgent and compelling**.

[434] The Court does not determine whether disclosure *must* occur under s. 8(2)(m). That is the Commissioner's statutory duty. The Court determines only that the Commissioner **must perform the duty**, and must do so **with reasons**.

2. The Public Interest in the Integrity of Judicial Records

[435] The Applicant's evidence raises concerns that:

- **Information Packages used in Ontario courts may have been falsified,**
- **judicial signatures may have been irregular or inauthentic,**
- **endorsements may be missing,**
- **warrants may not exist,**
- **court documents may not match CPIC entries,**
- **CPIC entries may have been altered post facto,**
- **or CPIC may contain the truth while court documents contain falsifications.**

[436] These concerns are not hypothetical. They are grounded in:

- the Applicant's production of two different "Information Packages,"
- the absence of judicial acta from the SCJ,
- the absence of warrants from TPS,
- the RCMP's refusal to search CPIC metadata,
- the RCMP's refusal to disclose audit logs,
- the RCMP's refusal to provide reasons.

[437] The integrity of judicial records is a **constitutional imperative**. As held in *Beauregard*, *Siwicki*, *Dugré*, and *Swaine*, judicial independence includes **administrative independence**, which requires:

1033

- accurate records,
- complete records,
- reliable records,
- preserved records.

[438] If judicial records have been falsified, altered, or manipulated, the consequences are profound:

- individuals may have been arrested without lawful authority;
- individuals may have been detained without lawful authority;
- individuals may have been convicted based on falsified documents;
- individuals may have been denied Charter rights;
- the Rule of Law may have been compromised.

3. The Public Interest in the Integrity of CPIC

[439] CPIC is the **national backbone** of criminal justice information in Canada. It is used by:

- police forces,
- prosecutors,
- courts,
- border agents,
- correctional institutions.

[440] If CPIC entries do not match court documents, or if CPIC entries have been altered to match falsified court documents, the consequences include:

- wrongful arrests;

- unlawful detentions;
- unlawful searches;
- unlawful seizures;
- miscarriages of justice;
- Charter violations;
- systemic risk to public safety.

[441] The Applicant's evidence suggests that:

- the "False Information Package" may have been generated using the Mescius/GrapeCity PDF SDK;
- the RCMP's Specialized Policing Services may have been involved;
- the Offline Historical Database may contain the authentic entries;
- the Foundational Metadata may reveal the truth.

[442] The public interest in determining whether CPIC has been compromised is **urgent**.

4. The Public Interest in Preventing Wrongful Arrests and Detentions

[443] If falsified Information Packages were used to obtain warrants, then:

- individuals may have been arrested unlawfully;
- individuals may have been detained unlawfully;
- individuals may have been denied bail unlawfully;
- individuals may have been convicted unlawfully.

[444] The Applicant's evidence suggests that:

- the warrant allegedly executed on October 2, 2024 may not exist;
- the Intake Court Endorsement may not exist;
- the judicial signature may be irregular;

- the SCJ has no record of the Information;
- the TPS had no copy of the warrant at the time of arrest;
- the RCMP may have been the originating agency.

[445] These concerns engage the **core of the criminal justice system**.

5. The Public Interest in Preventing Post-Facto Alteration of CPIC

[446] The Applicant raises the possibility that:

- CPIC entries may have been altered after the fact to match falsified court documents,
- or that court documents may have been falsified to match CPIC entries.

[447] The Offline Historical Database and Foundational Metadata are the only repositories capable of revealing:

- the original entries,
- the sequence of modifications,
- the timestamps,
- the ORI numbers,
- the Terminal IDs,
- the operator IDs,
- the ADD/MODIFY/CLEAR/CANCEL logs.

[448] The RCMP's refusal to search these repositories prevents the Commissioner from determining whether disclosure is in the public interest.

6. The Public Interest in Transparency and Accountability

[449] The public interest in transparency is heightened where:

- judicial records are missing,

- warrants are missing,
- endorsements are missing,
- CPIC entries are incomplete,
- metadata is withheld,
- audit logs are withheld.

[450] The RCMP's refusal to act undermines:

- transparency,
- accountability,
- public confidence,
- the Rule of Law.

7. The Commissioner Must Personally Consider s. 8(2)(m)

[451] Section 8(2)(m) requires the **Head of the RCMP** to personally determine:

- whether disclosure is in the public interest, and
- whether disclosure would clearly benefit the individual.

[452] The Commissioner cannot make this determination without:

- CPIC metadata,
- Offline Historical Database entries,
- Foundational Metadata,
- audit logs,
- system logs,
- administrative records.

[453] The RCMP's refusal to search prevents the Commissioner from performing his statutory duty.

8. The Commissioner Must Provide Reasons

1037

[454] Under *Vavilov*, the Commissioner must:

- provide reasons,
- justify the decision,
- demonstrate that statutory factors were considered,
- demonstrate that the public interest was weighed.

[455] The Commissioner cannot provide reasons without the underlying records.

9. The Public Interest Override Is Engaged

[456] The Applicant's evidence raises systemic risks that engage the public interest override in s. 8(2)(m):

- risk of wrongful arrest;
- risk of wrongful detention;
- risk of falsified judicial documents;
- risk of compromised CPIC entries;
- risk of post-facto alteration;
- risk of miscarriages of justice;
- risk to the integrity of the courts;
- risk to the Rule of Law.

[457] The Commissioner must therefore consider whether disclosure is required in the public interest.

10. Conclusion on Public Interest and Systemic Urgency

1038

[458] The Applicant's evidence raises urgent and compelling public interest concerns. The RCMP's refusal to act prevents the Commissioner from performing his statutory duty under s. 8(2)(m). The Court must therefore order the RCMP to:

- search the required repositories,
- produce the required metadata,
- transmit the CTR,
- and enable the Commissioner to make a reasoned decision.

[459] The Commissioner must then provide reasons explaining:

- whether disclosure is in the public interest, and
- why or why not.

PART V — SECTION M — SYSTEMIC POLICY OBLIGATIONS OF THE RCMP AS NATIONAL CUSTODIAN OF PERSONAL INFORMATION AND JUDICIAL METADATA

(31 Proactive Duties Triggered When the RCMP Has Notice of Potential Falsification, Mismatch, or Irregularity)

1. Overview

[460] The Applicant submits that the RCMP, as the national custodian of CPIC and related metadata repositories, owes a suite of **proactive, systemic obligations** when it has **notice** of potential:

- falsification of judicial documents,
- mismatch between CPIC entries and court documents,
- post-facto alteration of CPIC records,
- irregular judicial signatures,
- missing judicial acta,
- missing warrants or endorsements,

[461] The Court agrees that the RCMP's role as:

- **controller of CPIC,**
- **custodian of national criminal justice metadata,**
- **federal steward of inter-jurisdictional police information,**
- **holder of audit trails and foundational metadata,**
- **and recipient of statutory access requests**

imposes **heightened obligations** once it has notice of potential systemic irregularities.

[462] These obligations arise from:

- the *Privacy Act* (ss. 4, 6, 8, 10);
- the RCMP Act (s. 37 duties of integrity, diligence, and incorruptibility);
- the common law duty of candour;
- the Rule of Law;
- the open-court principle;
- the constitutional imperative of judicial independence;
- and the public interest in preventing wrongful arrest, detention, or conviction.

2. The RCMP's 31 Proactive Obligations Upon Receiving Notice of Potential Falsification or Mismatch

The Court sets out the following **31 systemic obligations** that arise when the RCMP has notice — as it does here — of potential falsification, mismatch, or irregularity in judicial or CPIC-related records.

These obligations are **not discretionary**. They flow from statute, constitutional principles, and the RCMP's institutional role.

A. Obligations Relating to Integrity of CPIC and Metadata (1–10)

1040

(1) Duty to preserve all CPIC entries The RCMP must immediately preserve all relevant CPIC entries, including historical versions.

(2) Duty to preserve Offline Historical Database records This includes ADD/MODIFY/CLEAR/CANCEL logs.

(3) Duty to preserve Foundational Metadata Including ORI, SID, Terminal ID, timestamps, operator IDs.

(4) Duty to preserve audit logs Including cryptographic audit trails.

(5) Duty to preserve access logs Including all queries, operators, and timestamps.

(6) Duty to preserve system exception logs Including any anomalies in PDF generation or metadata manipulation.

(7) Duty to preserve cross-jurisdictional ingestion logs Including TPS → RCMP transfers.

(8) Duty to preserve all administrative processing files Including ATIP and ATIA cross-linking.

(9) Duty to preserve all internal communications Including emails, instant messages, and briefing notes.

(10) Duty to preserve all judicial metadata Including issuing court, issuing authority, and judicial identifiers.

B. Obligations Relating to Accuracy and Verification (11–17)

(11) Duty to verify CPIC entries against original judicial acta Where court documents are missing or irregular, the RCMP must verify authenticity.

(12) Duty to verify whether CPIC was altered post-facto Including forensic comparison of historical logs.

(13) Duty to verify whether court documents were falsified Including comparison with CPIC's original entries.

1041
(14) **Duty to verify whether judicial signatures are authentic** Including cryptographic or handwriting analysis where appropriate.

(15) **Duty to verify whether warrants actually existed** Including cross-checking with court registries.

(16) **Duty to verify whether endorsements existed** Including Intake Court Endorsements.

(17) **Duty to verify whether the RCMP was the originating agency** Including ORI analysis.

C. Obligations Relating to Transparency and Disclosure (18–23)

(18) **Duty to disclose to the Applicant all personal information used for administrative purposes** As required by s. 10(1)(a) of the *Privacy Act*.

(19) **Duty to disclose all personal information retrievable by identifier** As required by s. 10(1)(b).

(20) **Duty to disclose administrative metadata** Including ORI, Terminal ID, SID, timestamps.

(21) **Duty to disclose judicial metadata** Including issuing authority and court level.

(22) **Duty to disclose audit trails** Where they relate to the Applicant's personal information.

(23) **Duty to disclose whether CPIC entries were modified** Including the sequence of modifications.

D. Obligations Relating to Public Interest and s. 8(2)(m) (24–27)

(24) **Duty to consider whether disclosure is in the public interest** This duty is personal to the Commissioner.

(25) **Duty to consider whether disclosure would benefit the individual** Also personal to the Commissioner.

(26) **Duty to provide reasons** Under *Vavilov*, reasons must be intelligible, justified, and responsive.

(27) **Duty to consider systemic risks** Including risk of wrongful arrest, detention, or conviction.

(28) **Duty to act with integrity, diligence, and incorruptibility** As required by s. 37 of the RCMP Act.

(29) **Duty to avoid conflicts of interest and institutional bias** Including avoiding reliance on SPS where SPS may be implicated.

(30) **Duty to cooperate with judicial review** Including compliance with Rules 317 and 318.

(31) **Duty to prevent spoliation and ensure preservation of evidence** Including prohibition on alteration, deletion, or migration.

3. These Obligations Are Triggered Because the RCMP Has Notice

[463] The Applicant’s evidence — including the two divergent Information Packages, missing judicial acta, missing warrants, irregular signatures, and unexplained CPIC anomalies — constitutes **formal notice** to the RCMP of potential systemic irregularities.

[464] Once the RCMP has notice, these 31 obligations are triggered.

[465] The RCMP’s refusal to act is inconsistent with:

- the *Privacy Act*,
- the RCMP Act,
- the Federal Courts Rules,
- the duty of candour,
- the Rule of Law,
- and the public interest.

4. These Obligations Justify Structural Orders

1043
[466] The Court's structural orders — including mandatory CTR transmission, preservation orders, prohibition orders, and contempt leave — are justified because:

- the RCMP has failed to discharge these obligations;
- the RCMP has refused to act;
- the RCMP has refused to participate;
- the RCMP has refused to provide reasons;
- the RCMP has refused to search;
- the RCMP has refused to disclose;
- the RCMP has refused to comply with Rule 318.

[467] Structural orders are necessary to restore the Rule of Law.

5. Conclusion on Systemic Policy Obligations

[468] The RCMP's role as national custodian of CPIC and judicial metadata imposes **31 proactive obligations** once it has notice of potential falsification or mismatch. The RCMP has failed to discharge these obligations. Structural orders are necessary to ensure compliance, protect the public interest, and enable the Commissioner to perform his statutory duty under s. 8(2)(m).

Court File No. T-2448-26

FEDERAL COURT

The Honourable Acting Chief Justice of the Federal Court of Canada

Tuesday, June 30, 2026

(Court Seal)

BETWEEN:

KEVIN ALEXANDER McLEAN

Applicant

ROYAL CANADIAN MOUNTED POLICE, COMMISSIONER MICHAEL DUHEME,
ATTORNEY GENERAL OF CANADA, and HIS MAJESTY THE KING IN RIGHT OF
CANADA

Respondents

ORDER

THE APPLICANT’S NOTICE OF MOTION NUMBER ONE, NUMBER TWO AND APPLICATION, made by the Applicant for the relief sought in those motions and in the Applicant were heard this Tuesday, June 30, 2026, in Toronto or Ottawa.

UPON reading the Applicant’s Notice of Application, Notice of Motion #1, Notice of Motion #2, the supporting affidavits and documentary evidence, and the Respondent having filed no Notice of Appearance, no Certified Tribunal Record, no evidence, and no submissions;

AND UPON the Court finding that the Respondent has failed to comply with its mandatory statutory duties under Rules 317 and 318 of the *Federal Courts Rules*, the *Privacy Act*, and the principles of procedural fairness, natural justice, and the Rule of Law;

AND UPON the Court concluding that structural relief is necessary to restore legality, ensure access to justice, and enable the Commissioner of the RCMP to perform his statutory duty under s. 8(2)(m) of the *Privacy Act*;

THE COURT ORDERS AND DECLARES THAT:

A. PROCEDURAL RELIEF (NUNC PRO TUNC)

1. **Abridgment of Time (Rule 8):** All timelines relating to this Application and the Applicant’s motions are abridged nunc pro tunc.
2. **Dispensation of Compliance (Rule 55):** Strict compliance with any procedural rule is dispensed with nunc pro tunc where necessary to give effect to this Order.
3. **Deeming of Filing (Rule 72.1):** All documents submitted by the Applicant are deemed filed on the date they were submitted to the Registry.
4. **Dispensation of Proof of Service (Rule 73):** The Applicant is not required to provide further proof of service upon the Respondent.

B. DECLARATORY RELIEF

5. **Ultra Vires Conduct:** It is declared that the RCMP acted outside statutory limits, failed to discharge mandatory ministerial and executory duties, and acted unreasonably within the meaning of *Vavilov*.

- 1046
6. **Contravention of Rule 318:** It is declared that the RCMP contravened Rule 318 by failing to transmit the Certified Tribunal Record.
 7. **Breach of Procedural Fairness:** It is declared that the RCMP breached procedural fairness and natural justice.
 8. **Administrative Bad Faith:** It is declared that the RCMP engaged in administrative bad faith, including silence where the law required action, half-truths, misstatements of law, and active concealment.
 9. **Denial of Access to Justice:** It is declared that the RCMP's conduct constitutes a functional denial of access to justice.
 10. **Public Interest Engagement:** It is declared that the Applicant's evidence raises urgent and compelling public interest concerns requiring the Commissioner's personal consideration under s. 8(2)(m) of the *Privacy Act*.
 11. **Systemic Obligations:** It is declared that the RCMP is subject to the 31 proactive obligations set out in these Reasons when it has notice of potential falsification, mismatch, or irregularity in judicial or CPIC-related records.

C. MANDAMUS

12. **Mandatory Search Order:** The RCMP shall conduct a full search of all repositories containing the Applicant's personal information, including but not limited to:
 - CPIC Foundational Metadata;
 - CPIC Offline Historical Database;
 - ADD/MODIFY/CLEAR/CANCEL logs;
 - audit logs;
 - access logs;
 - hexadecimal dumps;
 - PPU 005;
 - cross-jurisdictional ingestion logs;
 - administrative processing files;
 - all internal communications relating to file P-2025-16999.
13. **Mandatory s. 8(2)(m) Consideration:** The Commissioner of the RCMP shall personally consider whether disclosure is required under s. 8(2)(m) of the *Privacy Act*.
14. **Mandatory Reasons:** The Commissioner shall provide written reasons explaining:
 - whether disclosure is in the public interest;
 - whether disclosure would benefit the Applicant;
 - the statutory analysis;
 - the factual basis;
 - the public interest considerations.

D. CERTIFIED TRIBUNAL RECORD (RULE 318)

15. **24-Hour Deadline:** The RCMP shall transmit the complete Certified Tribunal Record to the Registry and to the Applicant **within 24 hours** of this Order.
16. **Required Contents:** The CTR shall include all 18 categories of materials enumerated in the Schedule to NOM #2, including:
 - administrative files;
 - system logs;
 - audit trails;
 - metadata;
 - judicial acts;
 - warrants;
 - endorsements;
 - communications;
 - ingestion logs;

- and all other materials specified therein.

1047 **E. PROHIBITION AND PRESERVATION**

17. **Preservation of Metadata:** The RCMP is prohibited from deleting, altering, migrating, sanitizing, obfuscating, or archiving beyond rapid retrieval any metadata, logs, or audit trails relating to the Applicant.
18. **Prohibition Against Unauthorized Searches:** The RCMP is prohibited from conducting searches outside the scope of the Applicant's PII Access Request for the purpose of responding to that request.

F. JUDICIAL OVERSIGHT

19. **Court Seized:** The Court remains seized of this matter to supervise compliance, address issues arising from execution, and adjudicate any contempt proceedings.

G. CONTEMPT LEAVE

20. **Leave for Contempt:** The Applicant is granted leave to bring a motion for contempt under Rule 50 and Rules 466–467 if the RCMP fails to comply with this Order.

H. CROSS-JURISDICTIONAL ENFORCEMENT

21. **Enforcement Authorization:** The Applicant is authorized to seek recognition and enforcement of this Order in any court, tribunal, or administrative body in Canada.

I. COSTS AND INTEREST

22. **Costs:** Costs are awarded to the Applicant on a **full indemnity basis**, payable forthwith by the Respondent.
23. **Interest:** Pre-judgment and post-judgment interest are awarded on all costs.

J. RESIDUAL RELIEF

24. **Residual Authority:** The Court grants such further and other relief as may be just and equitable to give full effect to this Order.

SIGNED at Ottawa, Ontario, this ____ day of _____, 2026.

_____ *A Judge of the Federal Court*

TAB 29

Federal Court



Cour fédérale

180 Queen St. W, Suite 200
Toronto, Ontario
M5V 3L6

Via email

Applicant:

Kevin Alexander McLean
mclean@searchandseizure.ca

Respondent:

Nick Continelli / Jake Norris
Department of Justice, Ontario Regional Office
nick.continelli@justice.gc.ca / jake.norris@justice.gc.ca

June 24, 2026

RE: T-2448-26 - Kevin Alexander McLean v. Royal Canadian Mounted Police

Please find below the Direction issued Associate Judge Crinson dated June 24, 2026:

“The following documents have been placed before me for directions under R.72:

Submitted June 3 – Letter dated June 3, 2026, Application Record and Memo of Fact and Law

Submitted June 19 – Letter dated June 19, 2026 and Requisition for Hearing

Submitted June 22 – Bill of Costs and Draft Decision

Submitted June 22 – Updated and Amended Application Record

Submitted June 22 – Letter dated June 22, 2026

Submitted June 23 – Letter dated June 23, 2026

The Notice of Appearance submitted by the Respondent on June 3, 2026 cannot be accepted for filing absent an Order granting an extension of time to file the Notice of Appearance. Pursuant to Rule 145 of the Federal Courts Rules the Applicant is not required to serve any further documents on the Respondent unless and until there is a properly filed Notice of Appearance. They are however required to file documents in a timely fashion. This means that any supporting affidavits were required to be filed, or proof of their service filed, by June 14, 2026. If the submitted Applicant's Record contains supporting affidavits that have not been previously filed it may not be accepted for filing until those affidavits have been filed.

The Applicant must comply with R.306 and file supporting affidavits before other steps in the proceeding may be taken, time for doing so is hereby extended to 30 days from the date of this direction. Subsequent documents are not accepted for filing until R.306 filing of the Applicant's supporting affidavits is complete.

This direction will also address the letter dated June 23 which identifies a hearing date of June 30. The Motion Record submitted under Rule 369 therefore will be determined in writing."

Regards,

Alice Prodan Gil
Senior Registry Officer

TAB 30

June 25, 2026

1053

Via "Delivery Filing" (to the Local Office of the Toronto Office of the Federal Court of Canada) at first instance

TO:

Chief Administrator

Federal Court of Canada

c/o Toronto Registry
180 Queen Street West,
Suite 200
Toronto, Ontario
M5V 3L6

COPIED TO, FORWARDED TO AND TO THE ATTENTION OF:

The Honourable Chief Justice of the Federal Court of Canada (acting) and the ACJ of the Federal Court of Canada
Madam Justice St. Louis

Courts Administration Service
Registries of the Federal Courts
90 Sparks Street, 5th Floor
Ottawa, Ontario K1A 0H9

Fax: 613-952-3653

RE: MCLEAN V. ROYAL CANADIAN MOUNTED POLICE COURT FILE NO. T-2448-26

APPLICANT'S RESPONSE TO DIRECTION OF ASSOCIATE JUDGE CRINSON (JUNE 24, 2026) —

**PROCEDURAL CLARIFICATION RE: RULE 306 TO RULE 307, LOCUS STANDI, AND NOTICE OF MOTION
#2 ET AL**

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

1. I write further to the Direction issued by Associate Judge Crinson dated June 24, 2026. I thank you for a copy of the same.
2. This correspondence is respectfully filed by **Delivery Filing** on the denoted date above, will be included as Tab 30, with enclosures to ensure to ensure the completeness of the Court's record and to clarify several procedural matters arising from the Direction, particularly as they relate to: (a) the applicability of Rule 306 in circumstances where no Notice of Appearance has been accepted for filing; (b) the Respondents' lack of *locus standi*; and (c) the status of the Applicant's *Notice of Motion* #2, returnable June 30, 2026.

2. The Applicant acknowledges and appreciates the Direction confirming that:
 - (a) "The Notice of Appearance submitted by the Respondent on June 3, 2026 cannot be accepted for filing absent an Order granting an extension of time."
 - (b) "Pursuant to Rule 145...the Applicant is not required to serve any further documents on the Respondent unless and until there is a properly filed Notice of Appearance."
3. These findings confirm that the Respondents presently have **no locus standi** in this proceeding. They are not parties, cannot be served, cannot participate, cannot file materials, cannot seek cross-examinations, cannot oppose motions, and cannot be heard.
4. Accordingly, all future correspondence, consistent with previous correspondence, will be transmitted and filed to the Registry and, where appropriate, to the Chief Administrator, **without service upon the Respondents**, consistent with Rule 145 and the aspect of the Direction that is consistent with the Federal Courts Rules.
5. This reinforces that Rules 306 through 308 are **inapplicable**, as they presuppose reciprocal service and the existence of a responding party(ies) with standing.
6. To the extent the Respondents may seek **leave** to file a late Notice of Appearance, the Applicant confirms that such leave will be **opposed**. The delay is now nearly four times the prescribed period under Rule 305, and **costs cannot cure** the prejudice arising from:
 - (a) the Respondents' total procedural default;
 - (b) their failure to transmit the Certified Tribunal Record under Rule 318; and
 - (c) their failure to file any objection under Rule 318(2).

II. THE RULE 306 PARADOX: NO SERVICE POSSIBLE → NO PROOF OF SERVICE → RULE INOPERATIVE

6. The Direction references Rule 306 and extends time for filing "supporting affidavits". Respectfully, clarification is sought, in the extant and to be decided, consistent with the Federal Courts Rules, required, as Rule 306 is a **service-based rule based upon the immediately foregoing Rule 305**, not an evidentiary requirement.
7. Rule 306 provides:

"Within 30 days after issuance of a notice of application, an applicant shall **serve** its supporting affidavits and documentary exhibits and **file proof of service**. The affidavits and exhibits are deemed to be filed when the proof of service is filed in the Registry."
8. Given Associate Judge Crinson's finding that: (a) no Notice of Appearance has been accepted for filing; (b) the Applicant is not required to serve the Respondents; and (c) service is legally impossible, it follows that: (d) **no proof of service can be filed**; (e) the deeming provision cannot operate; and (f) Rule 306 is **inoperative** in these circumstances.

s 306–308 presuppose: (a) a participating Respondent; (b) reciprocal service of affidavits; and (c) the possibility of cross-examination. Where no Respondent appears, these Rules cannot apply.

III. CANADA EVIDENCE ACT: DOCUMENTARY EVIDENCE IS ADMISSIBLE WITHOUT AFFIDAVITS

10. The *Canada Evidence Act*, a federal statute, governs the admissibility of documentary evidence in this proceeding. Sections 29 through 36 expressly contemplate the admissibility of business records, public documents, electronic records, and certified copies **without the necessity of a supporting affidavit**.
11. As a matter of statutory hierarchy, the *Canada Evidence Act* supersedes any contrary implication that might be drawn from the *Federal Courts Rules*. Accordingly, the Applicant’s documentary record is fully admissible without recourse to Rule 306. As such, the initial Application Record (June 3, 2026), the first updated Application Record (June 22, 2026) and the combined Motion Record/2nd Updated Motion Record are, as a matter of law, deemed Delivery Filed on the date they were “Delivery Filed” to the Local Office (Toronto).

IV. FORM 301: “MATERIAL” IS NOT SYNONYMOUS WITH “AFFIDAVITS”

12. Form 301 expressly states: “*This application will be supported by the following **material**.*”
13. The Form does **not** mandate affidavits. The term “material” is broader and naturally encompasses: (a) documentary evidence; (b) statutory materials; (c) certified records; and (d) the Certified Tribunal Record itself.
14. This drafting choice reflects the reality that judicial review is a **record-based proceeding**, and that the Tribunal’s own record — not affidavit evidence — is the primary evidentiary foundation.
15. This interpretation is reinforced by the Supreme Court of Canada’s decision in *Ontario (Energy Board) v. Ontario Power Generation Inc.*, 2015 SCC 4, per Rothstein J. for the SCC, which articulates the three-part test governing tribunal participation. A tribunal that does **not** appear cannot file evidence, cannot expand the record, and cannot introduce affidavit material. Respectfully, the same is applicable to an Applicant pursuant to the Keeprite Standard as per the partially self-eponymous named case (i.e. no filing of affidavit material that was not before the Tribunal at the time of the decision by the tribunal).
16. There is a distinction between standing and participation. The Tribunal had the right to appear but chose not to.

V. RULE 317: DEFINITION OF “MATERIAL” AND THE CTR FAILURE

16. Rule 317 authorizes a party to request that the tribunal transmit **any material** relevant to the application that is in possession. “Material” is not defined in the *Federal Courts Rules*, the *Federal Courts Act*, or the *Interpretation Act*.
17. As set out in the Applicant’s Rule 317 Request, “material” must therefore be interpreted **purposively**, consistent with: (a) the open court principle; (b) the record-based nature of judicial review; and (c) the statutory duty of tribunals to transmit the Certified Tribunal Record.
18. The RCMP Tribunal has: (a) not transmitted the Certified Tribunal Record; (b) not filed any objection under Rule 318(2); (c) not sought an extension; and (d) not complied with its statutory obligations.
19. This failure is independent of any Notice of Appearance. Rule 317 binds the Tribunal **as a tribunal**, not as a litigant.

VI. MCINERNEY V. MACDONALD POLICY SYMMETRY

20. The Supreme Court of Canada in *McInerney v. MacDonald*, [1992] 2 S.C.R. 138, emphasized that access to personal information regimes exist to **avoid unnecessary litigation** and ensure efficient resolution of disputes.
21. Rule 317 serves a parallel function: by compelling the Tribunal to transmit the Certified Tribunal Record into the open court record, it preserves judicial resources and avoids duplication of proceedings.
22. This policy symmetry reinforces that Rule 317 is not optional, discretionary, or exploratory. It is a prescribed duty.

VII. STATUS OF NOTICE OF MOTION #2 (RETURNABLE JUNE 30, 2026)

23. The Direction does not reference *Notice of Motion #2*, which was: (a) filed by Delivery Filing on June 22, 2026; and (b) with the Motion Record, Delivery Filed, on June 23, 2026.
24. NOM #2 seeks: (a) the self-assignment to the Chief Justice or Acting Chief Justice; and (c) consolidation of outstanding issues for determination in writing, including the Application itself considering it will be outstanding for some 45 days as of June 30, 2026.
25. Given that NOM #1 is now confirmed to proceed in writing although its returnable date was June 17, 2026, the Applicant respectfully notes that NOM #2 must also proceed in writing under Rule 369.

VIII. MATERIALS FILED CONCURRENTLY OR TO BE FILED CONCURRENTLY (TABS 29–31)

26. To complete the record for NOM #2 and the Applicant, the Applicant is filing: (a) **Tab 29** — Direction of Associate Judge Crinson (June 24, 2026); (b) **Tab 30** — This correspondence; and (c) **Tab 31** — Email from Mr. Jeff Ball (RCMP) dated May 19, 2026 and *IPC Order MO-1672*. Tab 31 underscores the complete provision to this Honourable Federal Court of Canada of the positions

IX. THIS PROCEEDING IS A CHIEF JUSTICE'S CASE

27. As set out in the Delivery Filed *Notice of Motion #2* and the Second Updated Application Record, it is the Applicant's position — now further reinforced by the Direction — that this Proceeding is properly a **Chief Justice's case**, as defined in the jurisprudence arising from the doctrine of *primus inter pares*.
28. Since the Supreme Court of Canada's decision in *Ruffo v. Conseil de la magistrature*, [1995] 4 S.C.R. 267, as cited in *Baldovi*, the doctrine of *primus inter pares* has evolved into a substantive recognition that a Chief Justice of a s. 96 Court possesses inherent responsibilities not dependent on statutory conferral. These responsibilities (the "13 Chief Justice Duties") include: (a) **Ultimate Jurisdiction** — final authority over adjudicative and administrative functions; (b) **Constitutional Trust Stewardship** — safeguarding the constitutional trust vested in the judiciary; (c) **Imperviously Influenced Mandate** — remaining insulated from external pressures (*Faber c. R.*, 2015 QCCS 12, at para. 111); (d) **Master of the Roster** — exclusive authority over judicial scheduling; (e) **Self-Assignment Power** — authority to seize matters of institutional significance; (f) **Administrative Stewardship** — oversight of registry and clerical functions; (g) **Institutional Reputation Guardian** — protection of the Court's integrity; (h) **Efficiency Operation Duty** — ensuring the seamless operation of the Court; (i) **Ethical Compliance Guarantee** — ensuring adherence to judicial ethics; (j) **Complaint Laying Power** — authority to initiate complaints against colleagues; (k) **Puisne Judge Removal Power** — authority to reassign judges during inquiries; (l) **Moral Barometer** — setting the ethical tone for the institution; (m) **Moral Authority** — guiding puisne judges through institutional leadership.
29. A precise reading of the current Chief Justice of Manitoba's articulation of the doctrine in *Baldovi* (2016) confirms that the test for a Chief Justice's case is met where: (a) challenges exist; (b) controversies exist; (c) the high profile nature of a case; and (d) the integrity of the Court is engaged.
30. As *Baldovi* states at paragraph 72:

“From time to time, a case presents as ‘a Chief’s case’. Such a case may be defined by its challenges, its controversy and/or its high profile nature. Such a case may also present as one whose circumstances place the focus on the integrity of the court.”
31. The present Proceeding meets this test. (a) **Challenges** exist, including unprecedented procedural irregularities and the Respondents' total default. (b) **Controversies** exist between the Applicant and the Respondents, including the failure to transmit the CTR. (c) **Integrity issues** arise because the Direction raises a national question of whether

X. CONTEMPT RISK NECESSITATES CHIEF JUSTICE OVERSIGHT (AN INTEGRITY AND PUBLIC INTEREST ISSUE)

32. A further and determinative factor confirming that this Proceeding is a Chief Justice's case arises from the **law of contempt**. Rule 50 of the *Federal Courts Rules* expressly provides that **Associate Judges cannot hear or determine contempt motions**. Only a judge of the Federal Court may adjudicate contempt.
33. Rule 466 of the *Federal Courts Rules* defines contempt broadly. A person is guilty of contempt of Court who: (a) fails to maintain a respectful attitude at a hearing; (b) disobeys a process or order of the Court; (c) acts in such a way as to interfere with the orderly administration of justice or impair the authority or dignity of the Court; (d) is an officer of the Court and fails to perform his or her duty; or (e) is a sheriff or bailiff who fails to execute a writ or return thereof.
34. The Direction issued by Associate Judge Crinson, while correct in confirming that the Respondents are not entitled to service under Rule 145, simultaneously creates a **procedural paradox**: (a) If the Applicant proceeds **without filing an affidavit**, consistent with Rule 306 being inoperative, the Applicant risks being accused of "impairing the authority of the Court" under Rule 466(c). (b) If the Applicant files an affidavit, the Respondents may use that affidavit to argue that prejudice is cured and seek leave to file a late Notice of Appearance, thereby undermining the Applicant's procedural rights. (c) If the Applicant serves an affidavit on the Respondents, this would contradict the Direction and Rule 145, creating a risk of contempt under Rule 466(b). (d) If the Applicant does **not** serve an affidavit, the Applicant risks contempt under Rule 466(c) for allegedly failing to comply with the Direction.
35. This paradox places the Applicant in a position where **any course of action risks a contempt allegation**, and only a judge — not an Associate Judge — has jurisdiction to resolve or prevent such a risk. This alone requires that the matter be seized by the Chief Justice or Acting Chief Justice.
36. Moreover, the contempt risk is not theoretical. It directly engages the institutional integrity of the Court because the Direction, if interpreted literally, would require the Applicant to: (a) serve affidavits on a Respondent who has no standing; (b) file proof of service that cannot exist; (c) comply with a Rule (306) that cannot operate; (d) expose himself to contempt for following the Direction; or (e) expose himself to contempt for not following the Direction.
37. No Associate Judge or Toronto-Region judge can adjudicate this issue without exceeding their jurisdiction under Rule 50. Only the Chief Justice or Acting Chief Justice may determine whether the Direction creates a contempt risk and whether Rule 306 is inoperative.

XI. UNPRECEDENTED CHALLENGES AND CONTROVERSIES

38. The **challenges and controversies** in this Proceeding are unprecedented. As set out at pages 10–11 of the Second **1059** Submitted Application Record, which is in the Form 301, the Applicant is the first individual in Canadian legal history — by any reported decision — to have an entire Criminal Code Information Package **manipulated post facto** using PDF modification software, filed in a transferee courthouse, and prosecuted for 18 months without withdrawal — albeit upon his extensive forensic investigations into the same leading to its inevitable conclusion that it was void ab initio from the time of the filing of the “false document” (as defined under the Criminal Code).
39. The jurisprudential distinctions between subfacial deficiencies and absolute nullities, as articulated in *R. v. Schertzer*, 2015 ONCA 259, *R. v. Hansen*, 2018 ONCA 46, and the *R. v. Silva* decisions (2021 QCCS 4627; 2021 QCCS 4131), demonstrate that the misconduct in this case transcends mere irregularity. It constitutes **absolute fabrication of judicial process ab initio**.
40. In *Schertzer* and *Hansen*, the courts addressed subfacial defects — misleading notes, misstatements, and improper grounds. In *Silva*, the misconduct involved the temporary misappropriation of a judicial stamp to forge a warrant in the context of apprehending a violent fugitive. Even in that extreme context, the fabrication was treated as noble-cause corruption.
41. The present case is more severe. It involves: (a) the manipulation of an entire Information Package; (b) the use of PDF manipulation software *post facto*; (c) the filing of the manipulated package in a transferee courthouse; (d) the continuation of prosecution for 18 months; (e) the failure of the RCMP Tribunal to comply with Rule 318; and (f) the Respondents’ refusal to appear or transmit the CTR.
42. These circumstances satisfy — and exceed — the *Baldovi* criteria for a Chief Justice’s case: (a) **Challenges**: unprecedented procedural and evidentiary anomalies; (b) **Controversies**: ongoing disputes between the Applicant and Respondents; (c) **Integrity**: the Direction raises a national question of whether Rule 306 requires service of affidavits on a non-appearing Respondent.
43. Accordingly, no Judge or Associate Judge of the Toronto Region should adjudicate NOM #1 or NOM #2. The issues must be determined by the Chief Justice or Acting Chief Justice for the benefit of the entire country.
44. The Applicant will provide a slightly revised Draft Order and Draft Reasons for Order/Judgment seeking a declaration that Rules 306–308 are inoperative where no Notice of Appearance has been filed, and that the matter is properly sub judice before the Chief Justice.

XII. TRANSMISSION TO PRINCIPAL OFFICE AND THE OFFICE OF THE CHIEF JUSTICE

45. This letter is therefore copied and will be forwarded to the **Office of the Chief Justice of the Federal Court of Canada**.
46. The Applicant also reminds the Toronto Local Office of its obligation under section 17 and section 25 of the *Federal Courts Rules* to transmit Delivery Filed documents to the Principal Office **without delay**.

47. Section 25 of the *Federal Courts Rules* provides that when a document is filed in paper copy at a local office, the Administrator shall: (a) transmit that paper copy, without delay, to the Principal Office; (b) keep a certified copy of the document at the local office; and (c) transmit a copy of the document to any other local office where a copy is required for the business of the Court.
48. Given the unprecedented issues raised herein — including the Rule 306 paradox, the contempt risk under Rule 466, the Respondents’ lack of *locus standi*, the failure to transmit the Certified Tribunal Record under Rule 318, and the national-level institutional integrity questions — the Applicant respectfully confirms that this correspondence must be transmitted to: (a) the **Principal Office** of the Federal Court of Canada; and (b) the **Office of the Chief Justice of the Federal Court of Canada**, the Honourable Madam Justice St. Louis.
49. The Applicant will, in accordance with the *primus inter pares* doctrine and the jurisprudence in *Baldovi*, *Ruffo*, and *Faber*, provide a slightly revised Draft Order and Draft Reasons for Order/Judgment seeking a declaration that Rules 306–308 are inoperative where no Notice of Appearance has been filed, and that the matter is properly **sub judice** before the Chief Justice or Acting Chief Justice.
50. The Applicant reiterates that no judge or Associate Judge of the Toronto Region should adjudicate *Notice of Motion #1* or *Notice of Motion #2*, as doing so would: (a) risk exceeding jurisdiction under Rule 50 (contempt); (b) risk placing the Applicant in contempt under Rule 466; (c) risk creating inconsistent or unenforceable procedural obligations; (d) risk undermining the integrity of the Court; and (e) contradict the institutional principles articulated in *Baldovi* and the 13 Chief Justice Duties.
51. In summary, I am appreciative of Associate Judge Crinson taking the time to issue such a direction to ensure that outstanding submitted filings did not require proof of service since June 1, 2026. However, public interest, challenges, controversies and court integrity issues arise because of this wording being incorrect, from an enactment interpretation and doctrinal standpoint:
- “Any supporting affidavits were required to be filed, or proof of their service filed, by June 14, 2026.”
52. Based on the indisputable premises and rudimentary enactment interpretation, This is legally impossible because:
- Proof of service is the filing.
 - Proof of service cannot exist without service.
 - Service cannot occur without a Notice of Appearance.
 - A Notice of Appearance does not exist.
53. Therefore, Rule 306 cannot operate.
54. And yet the Direction implies:
- I must file affidavits,
 - I must serve affidavits,
 - I must file proof of service,
 - and if you do not your record “may not be accepted.”

1061 55. I also draw this Court's attention to section 32 of the Interpretation Act, federal of course, regarding the validity of the prescribed form.

56. For these reasons, and consistent with the jurisprudential framework governing Chief Justice cases, the Applicant confirms that this Proceeding — and the issues raised in NOM #1 and NOM #2 — must now be adjudicated by the Chief Justice or Acting Chief Justice of the Federal Court of Canada.

57. The final document for the NOM #2/2nd Updated Application Record will follow as a standalone document when it has been properly and precisely drafted to include said relief with the necessary factual underpinnings in Tab 32.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'K. McLean', with a stylized flourish at the end.

Mr. Kevin A. McLean (BA, JD, CIM)

Applicant (Self-Represented)

mclean@searchandseizure.ca

TAB 31

McLean v. RCMP - Federal Court of Canada - file number to be assigned by the FCC

4 messages

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>

Fri, May 15, 2026 at 1:01 AM

To: Michael.Duheme@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Tanya.Mirsky@rcmp-grc.gc.ca, rborland@justice.gc.ca, carla.lyon@justice.gc.ca

Date: May 15, 2026

Classification: Private and Confidential

Subject: privilege including informant privilege

Sending method: Via Email

Your litigation file number: Unassigned

To:

Royal Canadian Mounted Police

Attention: Head of the Government Institution (RCMP)

Attention: Chief Legal Counsel

Attention: Mr. Jeff Ball

Attention: Mr. Stefane Brisson

Attention: Mr. Robert Borland (Department of Justice Canada)

Attention: Ms. Carla Lyon (Department of Justice Ontario Regional Office)

Email: Michael.Duheme@rcmp-grc.gc.ca; Jeff.ball@rcmp-grc.gc.ca; stephane.brisson@rcmp-grc.gc.ca; Tanya.Mirsky@rcmp-grc.gc.ca; rborland@justice.gc.ca; carla.lyon@justice.gc.ca

CC: mclean@searchandseizure.ca

Subject I: Advance Service of Unissued Notice of Application (Federal Court) – Compulsion of Statutory Search

Subject II: Proposal for Expedited Consent Resolution and Avoidance of Multiplicity of Proceedings

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I write regarding the above.

I attach the following documents for purposes herein. I have also copied my email utilized for the access requests under the Privacy Act and ATIA for ease of reference and security along with my passport in scanned form for security purposes and solely for purposes herein.

PART I: INTRODUCTION AND THE SERVICE OF UNISSUED PROCESS

1. It is formally submitted that the enclosed, duly executed, albeit unissued, notice of application (the "**Notice of Application**") is hereby served upon the Royal Canadian Mounted Police (the "**Respondent**") strictly as a professional courtesy. The formally issued and financially perfected iteration of this judicial instrument shall be provided to the Respondent in exceedingly short order. Out of an abundance of caution, physical reproductions of both the unissued and subsequently issued iterations shall concurrently be transmitted via postal service.

This comprehensive documentation is deliberately furnished in advance to meticulously articulate the material facts and the complex legal syllogisms underpinning the severe jurisdictional nullity presently contaminating the administrative record. The comprehensive nature of the drafting is designed to ensure that the Respondent is placed upon absolute, incontrovertible notice of the material facts and legal arguments prior to the commencement of expedited judicial interventions.

PART II: PROPOSAL FOR CONSENT RESOLUTION AND THE AVOIDANCE OF PROTRACTED LITIGATION

3. It is proposed that the Respondent consent to a formalized, binding agreement, or alternatively, a consent order (the "**Consent Order**"), to be entered seamlessly into the formal court record. This instrument must unequivocally establish strict timelines for the immediate execution of a comprehensive search of the foundational metadata (the "**Foundational Metadata**") and the offline historical database (the "**Offline Historical Database**").
4. Furthermore, the aforementioned agreement must strictly compel the provision of incontrovertible evidentiary proof that the mandated search was flawlessly conducted, alongside the explicit legal position of the Respondent concerning the statutory entitlement of the applicant (the "**Applicant**") to the extracted data and the specific application of any purported statutory exemptions.

PART III: EXIGENCY AND TEMPORAL CONSTRAINTS

5. The Respondent is strictly required to provide formal consent to the aforementioned resolution no later than the close of the current business day. Should this temporal deadline expire entirely devoid of a binding commitment, highly expedited judicial interventions, encompassing urgent motions for extraordinary prerogative writs, shall proceed immediately and without further localized notice.
6. The failure to secure such consent shall ipso facto precipitate a catastrophic escalation in compensatory issues and punitive costs, both strictly within the ambit of this immediate proceeding and comprehensively across external, collateral litigation.

PART IV: ANTICIPATORY REBUTTALS AND THE INAPPLICABILITY OF STATUTORY EXEMPTIONS

7. To preemptively neutralize any anticipated, albeit legally deficient, counter-arguments suggesting that the Respondent lacks statutory control over data ostensibly inputted by extraneous municipal constabularies, strict reliance is placed upon the supreme jurisprudence articulated in Canada (Information Commissioner) v. Minister of National Defence, 2011 SCC 25. This binding authority unequivocally establishes that overarching administrative dominion over a national database fundamentally constitutes absolute custody and control. The legal maxim *qui facit per alium facit per se* (he who acts through another does the act himself) is forcefully invoked to demonstrate that the systemic architecture orchestrated by the Respondent cannot be artfully bifurcated to shield localized data manipulation.
8. Should the Respondent attempt to advance the proposition in limine that the present application is procedurally premature due to a purported failure to exhaust administrative remedies via the Office of the Privacy Commissioner pursuant to the Privacy Act, such a postulate is categorically repudiated. A deliberate, institutional refusal to execute a search entirely transcends a mere discretionary refusal of access, constituting an *ultra vires* abdication of a non-derogable public duty. This severe omission perfectly crystallizes the jurisdiction of the superior tribunal to issue a writ of mandamus, compelling the restoration of the status quo ante.
9. Moreover, the profound, unyielding legal maxim *Fraus et jus nunquam cohabitant* (fraud and justice never dwell together) strictly dictates that the systemic circumvention of proper court jurisdiction via illicit technological machinations cannot be shielded by the passive invocation of generalized privacy exemptions. The public interest in the structural integrity of the justice system vastly eclipses any constructed administrative privilege. Where an administrative irregularity morphs into a direct contravention of an explicit statute, regulation, or equitable principle, it is definitively classified as an absolute nullity *ab initio*, rendering the entire proceeding *coram non iudice*.
10. Consequently, any reliance upon standard administrative exemptions to shield the transaction logs of a fabricated warrant is a *prima facie* misapplication of the law, fundamentally offensive to the administration of justice, and subject to immediate judicial quashing.

PART V: EVIDENTIARY ATTACHMENTS AND THE SEVERITY OF THE DOCUMENTARY FORGERY

11. For immediate ease of reference, and in the highly probable event that the Respondent's legal directorate has not yet scrutinized the most egregious and sophisticated documentary falsification within the annals of Canadian legal history, the purportedly authorizing instrument is appended hereto. This fabricated artifact profoundly eclipses the documented malfeasance adjudicated in *R. v. Hamilton*, 2004 CanLII 5549 (ON CA), *R. v. Scherzer*, 2014 ONSC 1234, and even the circumstances of *R. v. Silva*, 2010 ONSC 4752, involving the conduct of Officer G. Jolly—conduct which, albeit unlawful, was arguably animated by a misguided perception of noble cause.
12. The foundational presumption of administrative regularity—*omnia praesumuntur rite et solemniter esse acta* (all acts are presumed to have been done rightly and regularly)—is violently and entirely rebutted upon a mere facial examination of the appended instrument. It is an axiomatic, universally acknowledged procedural reality that a standard Adult Common Information Package strictly mandates a six-page architecture. The instrument currently

PART VI: JUDICIAL COMPLICITY AND THE PRIMUS INTER PARES

13. Following an exhaustive, highly sophisticated twenty-month forensic investigation, the precise identity of the presiding judicial officer has been incontrovertibly deduced. The individual implicated in authorizing this jurisdictional nullity is the departing Chief Justice of the Superior Court of Justice and President of the Divisional Court, officially vacating said office no later than 5:01 p.m. upon the date of their imminent departure.
14. It is formally averred that the ex parte in camera hearing precipitating this falsification transpired clandestinely within the judicial chambers of the aforementioned primus inter pares of the Ontario Superior Court of Justice, conspicuously and deliberately devoid of statutorily mandated recording apparatuses. While arguably tangential to the strict mandamus relief beseeched herein, the systemic failure of this judicial officer to safeguard the public interest—both within these specific proceedings and collateral litigation involving the Applicant—necessitates formal articulation. It remains the profound expectation of the Applicant that the Department of Justice and the Prime Minister of Canada shall henceforth execute appointments to the office of the primus inter pares more befitting of that solemn constitutional designation.

PART VII: THE PUBLIC INTEREST OVERRIDE AND SETTLEMENT PRIVILEGE

15. Notwithstanding the aforementioned judicial malfeasance, the statutory duty imposed upon the Respondent to execute a comprehensive search remains absolute, unequivocal, and entirely unassailable. The establishment of factual reality to a threshold of absolute certainty, far superseding the mere civil standard of a balance of probabilities, is fundamentally requisite.
16. It remains entirely opaque whether the Applicant constitutes a singular, isolated victim of this highly sophisticated technological subversion, or whether a broader, systemic contagion exists. Ergo, it is strictly demanded that the Head of the Government Institution immediately execute their mandatory statutory discretion to ascertain whether a public interest disclosure notice must be promulgated pursuant to the Privacy Act to alert other citizenry who may have been subjected to analogous deprivations of liberty.
17. Should the Respondent or its delegated counsel desire to engage in substantive discourse upon a strictly without prejudice basis, such communications shall be fully honored and enveloped by absolute settlement privilege, whether executed orally or in writing. However, it is explicitly declared that the Applicant shall not initiate such overtures. The collective, highly coordinated institutional misconduct sustained over the preceding eighteen to twenty months portended catastrophic, existential prejudice to the physical vitality and liberty of the Applicant; the mere reality that the Applicant neutralized these existential threats through superior jurisprudential acumen fundamentally aggravates the severity of the institutional malfeasance.

PART VIII: LEGAL REPRESENTATION, COMMUNICATION PROTOCOLS, AND PRESERVATION DEMANDS

18. Notice is hereby formally provided that two prominent senior general legal counsel, historically associated with the Royal Canadian Mounted Police in analogous jurisprudential matters and frequently tasked with assigning themselves or alternate specialized counsel, have been explicitly included within the distribution of this correspondence. It is formally requested that absolute confirmation of receipt be transmitted forthwith. Furthermore, the Respondent is entirely at liberty to seamlessly integrate any supplementary legal counsel into this electronic correspondence matrix.
19. Should the Respondent or its delegated legal representatives desire to engage in substantive telephonic discourse concerning these exigent matters, kindly advise so that an appropriate teleconference may be facilitated. Absent such discourse, it is respectfully submitted that the jurisprudential principles underpinning the requisite mandamus relief are fundamentally rudimentary, and the foundational material facts remain entirely incontrovertible and beyond substantive dispute.
20. Given that the requisite evidentiary corpus and documentary exhibits intended for deployment at any prospective motion or the substantive hearing of this Application—should the matter remain unresolved via antecedent motion—are fundamentally incontrovertible and not subject to substantive dispute, the formulation of a Joint Book of Documents is formally welcomed. Furthermore, it is advised that an exhaustive Application or Motion Record has been effectively finalized and shall be provided to the Respondent forthwith.
21. The paramount objective animating these proceedings remains the strict, unyielding adherence to the rule of law, effectuated exclusively through the immediate execution of the statutorily mandated offline searches. It is a profound institutional tragedy that scarce governmental resources must be aggressively consumed by such remedial litigation; however, the persistent administrative intransigence exhibited to date has strictly compelled the invocation of these extraordinary judicial remedies.
22. Finally, while it is established architectural reality that Foundational Metadata and hexadecimal data dumps—irrespective of whether they were subsequently amended via CLEAR, CANCEL, ADD, or MODIFY transactions—cannot be irrevocably purged from the offline historical repositories absent supreme, system-wide executive authorization, the Respondent is hereby strictly commanded to provide formal, written attestation confirming that

said architectural data points have absolutely not been subjected to unauthorized algorithmic alteration, manual sanitization, or systemic spoliation in any manner whatsoever.

23. In the alternative, and strictly as an interim measure demonstrative of institutional *bona fides*, should a licensed legal practitioner representing the Respondent, or the Commissioner of the Royal Canadian Mounted Police acting in their capacity as the Head of the Government Institution, elect to furnish a comprehensive summary of the Personal Information encapsulated within the Foundational Metadata and the Offline Historical Database via electronic transmission, the Applicant is amenable to the receipt thereof. It is strictly mandated that any such summary must explicitly enumerate the nomenclature of any and all judicial officers implicated, alongside the precise Originating Agency Identifiers (the "**ORIS**") of the entities responsible for the initiation of the frivolous, utterly meritless, and presently defunct charges.
24. The paramount objective animating these exhaustive efforts remains the unyielding pursuit of the truth-searching function. The optimal methodology for the safeguarding of the Applicant's fundamental rights, as enshrined within the *Canadian Charter of Rights and Freedoms*, shall be dictated entirely by the degree to which the Respondent adheres to the inviolable dictates of the Rule of Law. Furthermore, it is explicitly declared that the Applicant unreservedly reserves the absolute right to rely upon any and all correspondence not expressly demarcated as 'without prejudice' in subsequent judicial proceedings; it is formally noted that the present correspondence is emphatically not tendered upon a 'without prejudice' basis.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)

Enclosures

--

Best regards,

Mr. Kevin A. McLean (BA (MCL), JD, CIM)

Email: mclean@searchandseizure.ca

Phone: 647.370.9354

Fax: upon request

NOTA BENE: This email is for dispute resolution and litigation purposes only. Without prejudice communication so denoted invokes settlement privilege.

CONFIDENTIALITY NOTICE: This email and any attachments are confidential and may contain privileged information. It is intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution, or reliance upon the contents of this email is strictly prohibited. If you have received this communication in error, please immediately notify the sender by replying to this email and permanently delete the original message and any attachments from your system.

3 attachments

 **Form 301 - Notice of Application - McLean v RCMP et al - Applicant - KAM (BA JD CIM) - 14-MAY-2026 - DIGITAL SIGNATURE - ADOBE - MR MCLEAN.pdf**
786K

 **Information Package 4810 998 24 48129169-00 (4).pdf**
329K

 **ADULT-COMMON-INFORMATION-FORM-WITH-HIGHLIGHTED-CHANGES - LINCOLN COUNTY LAW ASSOCIATION.pdf**
215K

1067

Michael.Duheme@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Tanya.Mirsky@rcmp-grc.gc.ca, rborland@justice.gc.ca, carla.lyon@justice.gc.ca
Cc: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Date: May 15, 2026

Classification: Private and Confidential

Subject: privilege including informant privilege

Sending method: Via Email

Your litigation file number: Unassigned

To:

Royal Canadian Mounted Police

Attention: Head of the Government Institution (RCMP)

Attention: Chief Legal Counsel

Attention: Mr. Jeff Ball

Attention: Mr. Stefane Brisson

Attention: Mr. Robert Borland (Department of Justice Canada)

Attention: Ms. Carla Lyon (Department of Justice Ontario Regional Office)

Email: Michael.Duheme@rcmp-grc.gc.ca; Jeff.ball@rcmp-grc.gc.ca; stephane.brisson@rcmp-grc.gc.ca; Tanya.Mirsky@rcmp-grc.gc.ca; rborland@justice.gc.ca; carla.lyon@justice.gc.ca

CC: mclean@searchandseizure.ca; mcleansettlement@gmail.com

Subject I: Supplemental Transmission – Confirmation of Delivery, Evidentiary Attachments, and Contextual Exigency

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I write strictly in furtherance to the antecedent correspondence transmitted earlier this day.

PART I: CONFIRMATION OF DELIVERY AND SUPPLEMENTAL ATTACHMENTS

1. It is formally confirmed that the primary electronic transmission, encompassing the unissued Notice of Application and the comprehensive proposal for consent resolution, has been successfully routed and delivered to all designated recipients, entirely devoid of any automated rejection or delivery failure notifications.
2. Furthermore, to rectify an inadvertent administrative omission within the primary correspondence, the requisite biometric identification—specifically, a highly secure, digitized reproduction of the passport belonging to the Applicant—is appended hereto. This documentation is furnished strictly for security verification protocols and solely for the purposes enumerated within these specific proceedings.
3. Additionally, as formally undertaken, the electronic address mcleansettlement@gmail.com has been successfully integrated into the carbon copy distribution matrix of this transmission for ease of reference and heightened security. Sincere apologies are tendered for the initial oversight regarding these specific inclusions.

PART II: MEDICAL EXIGENCY AND THE NECESSITY OF PROCEDURAL FASTIDIOUSNESS

4. Strictly as a professional courtesy, and to provide profound context regarding the exacting, highly accelerated, and meticulous nature of these ongoing proceedings, formal notice is hereby provided concerning impending, severe medical interventions scheduled for the Applicant.
5. Specifically, a conclusive magnetic resonance imaging (MRI) procedure is scheduled to transpire imminently within the ensuing hours. Subsequently, the Applicant is slated to undergo highly invasive medical treatments, encompassing direct spinal injections and allied therapeutic protocols.

It is a medically anticipated reality that these profound interventions may precipitate a period of significant physical incapacitation, effectively sidelining the Applicant for an indeterminate duration. Consequently, this impending, unavoidable unavailability severely underscores the absolute necessity for the rigorous, fastidious, and immediate crystallization of the administrative and judicial records prior to the commencement of said medical treatments.

PART III: HISTORICAL CONTEXT AND THE IMPERATIVE OF PROCEDURAL VIGILANCE

7. To further contextualize the absolute necessity for the uncompromising procedural vigilance exhibited herein, supplementary evidentiary exhibits are appended to this transmission. These documents delineate a profound, historical privacy transgression perpetrated by the Law Society of British Columbia (the "**LSBC**") and its retained legal counsel, originating in June 2014 and surfacing via chronological disclosures in late 2021.
8. The aforementioned malfeasance involved the execution of a clandestine, non-consensual, and wholly undisclosed Random Access Memory (RAM) extraction—a highly intrusive, covert maneuver fundamentally distinguishable from a standard, judicially authorized forensic digital replication. This unauthorized extraction precipitated a seven-year trajectory of institutional obfuscation, effectively misleading judicial tribunals, regulatory bodies, and the public apparatus, thereby validating the jurisprudential axiom that systemic concealment invariably eclipses the severity of the antecedent transgression.
9. While the capacity to effectuate comprehensive public exposure of this quasi-criminal conduct was fully retained, deliberate restraint was exercised. The paramount focus was consciously restricted to the overarching truth-searching function, actively eschewing the mere public excoriation of a regulatory body amidst active litigation.
10. Fortuitously, this sustained exposure to sophisticated technological subterfuge has necessitated the acquisition of an advanced, highly specialized technological acumen by the Applicant. Consequently, this historical matrix fundamentally dictates the present, absolute intolerance for any administrative delay, procedural deflection, or statutory non-compliance.
11. The aggressive mobilization of substantial resources is deliberately undertaken not merely for the pursuit of individual vindication, but to engender a profound, systemic public benefit by strictly ensuring absolute, unyielding fidelity to the Rule of Law by those entities entrusted with its administration.

Yours truly,

Mr. Kevin A. McLean (BA, JD, CIM)

Enclosures:

1. Scanned Passport Copy
2. Lockhart (LSBC counsel at material times and responding on its behalf to FIPPA requests in 2021) - October 18, 2021 Correspondence (RAM Capture)
3. Lockhart (LSBC counsel at material times and responding on its behalf to FIPPA requests in 2021) - October 25, 2021 Correspondence (RAM Capture Link)

[Quoted text hidden]

3 attachments



Lockhart-October 18 letter-RAM capture.PDF

81K



Lockhart-RAM letter-with link-clickable for Organizations.pdf

96K



Kevin A McLean - Canadian Passport - 2023 - 10 Year validity.pdf

142K

Mr. Kevin Alexander McLean <mclean@searchandseizure.ca>
To: Michael.Duheme@rcmp-grc.gc.ca, Jeff.ball@rcmp-grc.gc.ca, stephane.brisson@rcmp-grc.gc.ca, Tanya.Mirsky@rcmp-grc.gc.ca, rborland@justice.gc.ca, carla.lyon@justice.gc.ca
Cc: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Mon, May 18, 2026 at 5:22 PM

Date: May 18, 2026

Classification: Private and Confidential

Sending method: Via Email

Subject I: Service of the Applicant's *Rule 317 (Federal Courts Rules)* Request, "Material from Tribunal"

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I. TRANSMISSION OF EXIGENT LEGAL INSTRUMENTS

1. Enclosed herewith, effectuated by means of formal electronic service, is the comprehensive written requisition articulated pursuant to *Rule 317* of the *Federal Courts Rules* (the "**Rule 317 Request**"). As delineated therein, exhaustive prophylactic measures have been deployed *in limine* to preemptively extinguish any anticipated objections, thereby optimizing judicial economy, preserving the public fisc, and strictly circumscribing the adjudicative temporal resources of the Federal Court of Canada.

II. STATUTORY COMPULSION AND PRODUCTION DIRECTIVES

2. Pursuant to the strictly construed operational mandates delineated within *Rule 318(1)* of the *Federal Courts Rules*, a compulsory directive is hereby effectuated, commanding the RCMP Tribunal to transmit the original or, in the alternative, a properly certified duplicate of the eighteen (18) distinct taxonomic categorizations of materials identified in the comprehensive schedule (the "**Schedule**").
3. The aforementioned statutory transmission must indispensably encompass all unprocessed hexadecimal enumerations (the "**Raw Hexadecimal Dumps**"), sequential operational chronologies (the "**Transaction Trails**"), and foundational information technology procurement data (the "**Core IT Procurement Data**"). Delivery thereof to the Federal Court Registry and the Applicant is strictly mandated within the prescribed twenty (20) day statutory limitation period, commencing on the juridical day following the present statutorily recognized holiday, thereby restoring the *status quo ante* of operational timelines.
4. Notification of the issued Notice of Application (the "**Application**") shall be remitted upon its formal issuance by the Registry; however, unequivocal confirmation is hereby furnished that the requisite financial remunerations necessary for filing have been fully discharged, as evidenced by the confirmation sequence heretofore transmitted.

III. EXTRAPOLATION OF EVIDENTIARY POSSESSION

5. It remains an unassailable legal postulate, absent any countervailing substantive rebuttal, that the Royal Canadian Mounted Police operated as the instigating law enforcement apparatus, contrary to extraneous assertions attributing involvement to ancillary constabularies. Consequently, it is an irrebuttable presumption that the RCMP Tribunal retains possession, custody, or control of the original and duplicate iterations of the *Criminal Code* Form 2 Information (the "**Form 2 Information**"), the authentic informational compendium (the "**Authentic Information Package**"), and ancillary juridical endorsements, comprising the September 23, 2024 endorsement (the "**Intake Court Endorsement**"), alongside any foundational warrant initialized at first instance. For the purposes of the operationalization of *Rule 317* of the *Federal Courts Rules*, possession is *prima facie* established, rendering any assertions to the contrary a nullity *ipso facto*.

IV. PRODUCTION DEFAULTS AND STATUTORY NULLITIES

6. Notwithstanding the purported guidelines delineated within the *Ministry of Attorney General Court Services Division Court Information Access Guide (2019)* (the "**MAG Access Guide**"), the legal mandate of a court of record, as constituted under section 96 of the *Constitution Act, 1867*, necessitates the retention of endorsed warrants within the originating judicial repository. Any administrative failure by the originating court office (the "**Originating Court Office**") to properly have in its court file said warrants constitutes not a mere procedural irregularity, but rather an absolute legal nullity, effectuated in direct contravention of fundamental constitutional and equitable principles. Nonetheless that is not at issue herein but for context purposes and that which I do not have in my possession per se. Consequently, the RCMP Tribunal remains strictly bound by the compulsory production mandates of *Rule 317*, necessitating the transmission of a certified duplicate of the arrest warrant, irrespective of ancillary administrative derelictions.

V. PRIVACY ACT EXEMPTIONS AND EQUITABLE REMEDIES

7. It is further asserted that the RCMP Tribunal's reliance upon extraneous informational repositories, devoid of explicit invocation of a designated statutory exemption under section 18 of the *Privacy Act*, is fundamentally *ultra vires*. Insofar as the RCMP Tribunal cited paragraph 19(1)(d), paragraph 22(1)(b), and section 26 of the *Privacy Act*—wholly omitting the requisite subparagraph 22(1)(a)(ii)—any assertion regarding an inability to execute a search of "files" is rendered legally hollow and devoid of substantive merit. The aforementioned search obligations are now entirely subsumed by the overarching statutory directives of *Rule 317* and remain subject to the equitable remedies of *mandamus* and prohibition.

8. Notwithstanding the undeniably tortuous and protracted procedural trajectory necessitated to secure the aforementioned evidentiary materials and correspondingly enshrine them within the public repository, such complications are inextricably linked to the administrative obfuscation and systemic recalcitrance exhibited by the Office of the Chief Justice (Ontario) (the "**Office of the Chief Justice**"). Said bureaucratic evasion pertains directly to records to which unquestionable entitlement exists *de jure* absent the imposition of pecuniary levies, and to which the broader public maintains an inviolable statutory right of access contingent solely upon the remittance of prescribed tariffs. Nevertheless, while such egregious institutional deviations from administrative mandates warrant severe judicial scrutiny, these procedural impediments remain ultimately ancillary, and thus legally tangential, to the substantive foundational issues currently at bar.

ALL OF WHICH IS RESPECTFULLY SUBMITTED,

Mr. Kevin A. McLean (BA, JD, CIM) The Applicant

[Quoted text hidden]



Rule 317 Requist - McLean v. RCMP - Applicant - Mr McLean - 18-May-2026 - Electronically Signed - Served - Filed.pdf
664K

Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>

Tue, May 19, 2026 at 10:44 AM

To: "Mr. Kevin Alexander McLean" <mclean@searchandseizure.ca>, "Brisson, Stéphane (RCMP/GRC)" <Stephane.Brisson@rcmp-grc.gc.ca>, "Mirsky, Tanya (RCMP/GRC)" <Tanya.Mirsky@rcmp-grc.gc.ca>, "rborland@justice.gc.ca" <rborland@justice.gc.ca>, "carla.lyon@justice.gc.ca" <carla.lyon@justice.gc.ca>
Cc: "mcleansettlement@gmail.com" <mcleansettlement@gmail.com>

Mr. McLean,

I would like to extend my apologies for the delay in responding to your email from last week. I was looking into your request myself and if I understand correctly you are seeking from the RCMP, the ORI within CPIC, relevant to your request 2025-16999.

After looking into your request for the ORI, we have noted some precedence that has been set to protect the ORI number from disclosure. I've taken the liberty of attaching the ruling from the Ontario Information and Privacy Commissioner that noted this decision (specifically on pages 5 of the attached).

The following is an extract from page 5 of the PDF (page 4 if you exclude the cover page) from the Information and Privacy Commissioner of Ontario:

"Previous orders of this office have found ORI Numbers to qualify for exemption under section 8(1)(l) (for example, Orders M-933, MO-1335, MO-1428). In Order MO-1335, Senior Adjudicator David Goodis stated that "Where information could be used by any individual to gain unauthorized access to the CPIC database, an important law enforcement tool, it should be considered exempt under section 8(1)(l)." As in these previous orders, I find that disclosing the ORI Numbers in this appeal could reasonably be expected to facilitate the commission of an unlawful act. Accordingly, the ORI Numbers qualify for exemption under section 8(1)(l)."

Now that being said, even though we are closing and concluding your request 2025-16999, I do want to remind you that you can file a complaint with the Office of the Privacy Commissioner of Canada, who can investigate the RCMP's ATIP Branch decisions and provide direction and guidance to us to improve on this request as well as recommend and guide broader institutional changes, if they find an issue while investigating your complaint.

The following is an extract from the [OPC website](#) to that effect: *"We consider the impact on both the complainant and the public. For example, when a complaint raises important systemic issues that affect large numbers of individuals, it may be given a higher priority and greater resources. This enables our Office to best serve the public interest by responding effectively to privacy matters of the greatest or emerging concern."*

I want to also take a moment to acknowledge that in the pursuit of information, a refusal of access to that information can be frustrating and erode confidence in public services. I do acknowledge any frustrations you may be experiencing in your pursuit of that information. We commit to working closely with the Office of the Privacy Commissioner, if a complaint is investigated, to ensure we are accountable and responsible in our execution and delivery of ATIP services under the legislative framework for which they fall.

Lastly, I want to thank you once again for writing to us and for your ongoing pursuit and demand for accountability.

Jeff Ball

Director Privacy

Access to Information and Privacy Branch

Digital Program

Royal Canadian Mounted Police

Jeff.Ball@rcmp-grc.gc.ca

Cell: 343-571-6721

Jeff Ball

Directeur protection des renseignements personnels

Sous-Direction de l'accès à l'information et la protection des renseignements personnels

Programme Numérique

Gendarmerie royale du Canada

Jeff.Ball@rcmp-grc.gc.ca

Céll: 343-571-6721

[Quoted text hidden]



32_MO_1672.pdf
178K

1072



Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

ORDER MO-1672

Appeal MA-020331-1

Toronto Police Services Board



80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9195
TTY: 416-325-7539
<http://www.ipc.on.ca>

NATURE OF THE APPEAL:

The requester made a request to the Toronto Police Services Board (the Police) under the *Municipal Freedom of Information and Protection of Privacy Act* (the Act) for access to the following information:

All the records pertaining to both of the July 10th, 2002 interactions at [a specified address], all records covering all of the conversations on July 10th, 2002 and any and all documents/records that pertain to these incidences [sic].

The Police identified 18 pages of records as being responsive, either wholly or in part, to the request. These records consist of entries in two police officers' notebooks, a "Record of Arrest," a "Supplementary Record of Arrest" and two "Event Details Reports."

The Police initially issued a decision letter to the requester granting partial access to the records. The Police denied access to portions of the records on the basis that they qualified for exemption under section 38(a) (discretion to refuse requester's own information) in conjunction with section 8(1)(l) (facilitate commission of an unlawful act or hamper the control of crime), and section 38(b) (invasion of privacy) with specific reference to section 14(3)(b) (compiled and identifiable as part of an investigation into a possible violation of law). The Police also indicated that they had severed portions of the police officers' notebooks on the basis that they were not responsive to the request.

The requester (now the appellant) appealed the Police's decision to deny access.

During mediation, the appellant indicated that she was not pursuing access to the non-responsive portions of the police officers' notes, and the parties agreed that pages 1 and 5 are no longer at issue in this appeal.

Also during mediation, the Police issued a revised decision and claimed section 38(a) in conjunction with section 8(1)(l) for portions of pages 14 and 18 that they had originally claimed were not responsive to the request. In addition, the Police decided to disclose to the appellant additional information on pages 6, 12, and 16.

Mediation did not resolve this appeal, and the file was transferred to adjudication. This office sent a Notice of Inquiry to the Police, initially, outlining the facts and issues and inviting the Police to make written representations. The Police submitted representations in response to the Notice. This office then sent a Notice of Inquiry to the appellant, together with a copy of the non-confidential portions of the Police's representations. The appellant provided brief representations in response, stating that "My only goal is to obtain all the personal information as per the definition in [the Act] pertaining to me."

In this appeal I must decide whether the exemptions claimed by the Police apply to the records.

RECORDS:

Of the 18 pages of records initially identified by the Police, nine remain at issue. They are the undisclosed portions of the following pages: two police officers' notebook entries (Pages 2-4 and Page 6, respectively); a "Record of Arrest" (Page 8); a "Supplementary Record of Arrest" (Page 10); and two "Event Details Reports" (Pages 12, 14 and Pages 15, 16, 18).

BRIEF CONCLUSION:

For the reasons set out in this order, I find that the records are exempt from disclosure under sections 38(a) and 38(b) of the *Act*.

DISCUSSION:**PERSONAL INFORMATION**

The first issue I must decide is whether the records contain personal information, and if so, whose.

Under section 2(1) of the *Act*, personal information is defined, in part, to mean recorded information about an identifiable individual, including the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual (section 2(1)(h)).

The Police submit:

The personal information contained within the records includes the names, dates of birth, telephone numbers, addresses and officer's comments about, as well as comments made by, individuals other than the appellant.

In claiming section 38(b) of the *Act*, which applies to information relating to the appellant, the Police also raise as an issue whether the records contain the appellant's personal information.

I find that all the pages at issue contain the personal information of both the appellant and other individuals. All the pages relate to incidents occurring on July 10, 2002 involving the appellant and these other individuals. The personal information includes the names, addresses, telephone numbers and age, as well as other personal information, of these individuals.

LAW ENFORCEMENT

Section 36(1) of the *Act* gives individuals a general right of access to their own personal information held by an institution. Section 38 provides a number of exemptions from disclosure that limit this general right.

The Police have claimed section 38(a) in conjunction with section 8(1)(l) to deny access to some of the information in the records. These sections read:

38. A head may refuse to disclose to the individual to whom the information relates personal information,
- (a) if section 6, 7, **8**, 9, 10, 11, 12, 13 or 15 would apply to the disclosure of that personal information;
8. (1) A head may refuse to disclose a record if the disclosure could reasonably be expected to,
- (l) facilitate the commission of an unlawful act or hamper the control of crime.

Under section 38(a), where a record relates to the requester but section 8 (law enforcement) would apply to the disclosure of personal information in the record, the institution may refuse to disclose that personal information to the requester.

Because section 38(a) is a discretionary exemption, even if the information falls within the scope of this section, the institution must nevertheless consider whether to disclose the information to the requester.

The Police rely on sections 38(a) and 8(1)(l) to support their denial of access to:

- “ten-codes” appearing in the officers’ notes (Pages 3 and 4); and
- ORI Numbers in the “Event Details Reports” (Pages 14 and 18).

“Ten-codes” are used by OPP officers in their radio communications with each other. The Police submit that ten-codes provide law enforcement with “an effective and efficient means of conveying a specific message without publicly identifying its true meaning,” and that divulging the codes would compromise their effectiveness. They contend that revealing the codes could enable those engaged in criminal activity to circumvent police detection or prevent police from responding to situations, thereby posing a risk of harm to the police and the public. The Police also state that disclosing the codes could enable those engaged in criminal activity to hamper the control of crime by monitoring police radio transmissions to determine when the police do not have any available officers. Finally, the Police submit that disclosing the ten-codes in the context of the records at issue in this case could easily reveal their meaning, thereby compromising the security of those codes.

This office has consistently found that section 8(1)(l) applies to “ten-codes” (for example, Orders M-393, M-757, PO-1665). Based on these earlier orders and my review of the records and the Police’s representations, I find that disclosing the ten-codes at issue could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime. As

Adjudicator Laurel Cropley stated in Order PO-1665, “disclosure of the ‘ten-codes’ would leave ... officers more vulnerable and compromise their ability to provide effective policing services as it would be easier for individuals engaged in illegal activities to carry them out and would jeopardize the safety of ... officers who communicate with each other on publicly accessible radio transmission space.” I therefore find that the ten-codes qualify for exemption under section 8(1)(l).

“ORI Numbers” are also known as “CPIC access codes.” The Police submit that “the release of transmission access codes for the CPIC system could facilitate the commission of an unlawful act or hamper the control of crime.”

Previous orders of this office have found ORI Numbers to qualify for exemption under section 8(1)(l) (for example, Orders M-933, MO-1335, MO-1428). In Order MO-1335, Senior Adjudicator David Goodis stated that “Where information could be used by any individual to gain unauthorized access to the CPIC database, an important law enforcement tool, it should be considered exempt under section 8(1)(l).” As in these previous orders, I find that disclosing the ORI Numbers in this appeal could reasonably be expected to facilitate the commission of an unlawful act. Accordingly, the ORI Numbers qualify for exemption under section 8(1)(l).

INVASION OF PRIVACY

The Police rely on section 38(b) in conjunction with section 14 to support their denial of access to the remaining information at issue (the undisclosed portions of Pages 2-4, 6, 8, 10, 12 and 15-16).

More specifically, the Police rely on the “presumed unjustified invasion of personal privacy” at section 14(3)(b) and the factors favouring privacy protection at sections 14(2)(e) and (h). These sections read:

- 38. A head may refuse to disclose to the individual to whom the information relates personal information,
 - (b) if the disclosure would constitute an unjustified invasion of another individual’s personal privacy;
- 14(2) A head, in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy, shall consider all the relevant circumstances, including whether,
 - (e) the individual to whom the information relates will be exposed unfairly to pecuniary or other harm;
 - (h) the personal information has been supplied by the individual to whom the information relates in confidence; ...

- (3) A disclosure of personal information is presumed to constitute an unjustified invasion of personal privacy if the personal information,
- (b) was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation;

As noted above, section 38 provides a number exemptions from disclosure that limit the general right of access under section 36(1) to one's own personal information held by an institution.

Under section 38(b), where a record relates to the requester but disclosure of the information would constitute an unjustified invasion of another individual's personal privacy, the institution may refuse to disclose that information to the requester.

Like section 38(a), section 38(b) is a discretionary exemption. Even if the requirements of section 38(b) are met, the institution must nevertheless consider whether to disclose the information to the requester. In this case, section 38(b) requires the Police to exercise their discretion in this regard by balancing the appellant's right of access to her own personal information against other individuals' right to the protection of their privacy.

Sections 14(1) through (4) of the Act provide guidance in determining whether disclosure would result in an unjustified invasion of an individual's personal privacy under section 38(b). Sections 14(1)(a) through (e) provide exceptions to the personal privacy exemption; if any of these exceptions apply, the information cannot be exempt from disclosure under section 38(b).

Section 14(2) provides some criteria for determining whether the personal privacy exemption applies. Section 14(3) lists the types of information whose disclosure is presumed to constitute an unjustified invasion of personal privacy. Section 14(4) lists the types of information whose disclosure does not constitute an unjustified invasion of personal privacy.

The Divisional Court has ruled that once a presumption against disclosure has been established under section 14(3), it cannot be rebutted by either one or a combination of the factors set out in section 14(2). A section 14(3) presumption can be overcome, however, if the personal information at issue is caught by section 14(4) or if the "compelling public interest" override at section 16 applies [*John Doe v. Ontario (Information and Privacy Commissioner)* (1993), 13 O.R. (3d) 767].

If none of the presumptions in section 14(3) applies, the institution must consider the factors listed in section 14(2), as well as all other relevant circumstances.

Based on my review of the records, I have concluded that none of the exceptions at sections 14(1)(a) through (e) applies in this case.

With respect to the section 14(3)(b) presumption, the Police submit:

In this instance, the police responded to a complaint of an assault, a criminal code offence. Whether or not criminal charges were ever laid in relation to this incident, does not negate the applicability of this section.

In order for section 14(3)(b) to apply, the information must have been compiled and must be identifiable as part of an investigation into a possible violation of law.

I have reviewed the records. The two sets of police officers' notes were created when the officers responded to incidents that occurred on July 10, 2002. Similarly, the "Record of Arrest" and "Supplementary Record of Arrest" document an arrest on that date arising from these incidents. The two "Event Details Reports" contain information about telephone calls made to the police. These records were all clearly compiled as part of an investigation into a possible violation of law, and I am satisfied that they fall within the section 14(3)(b) presumption. The presumption is not rebutted by section 14(4) or the "compelling public interest" override at section 16, which was not raised in this case. I therefore find that disclosing the information would constitute an unjustified invasion of personal privacy under section 38(b).

SEVERANCE

Section 4(2) of the *Act* requires the Police to disclose as much of any responsive record as can reasonably be severed without disclosing information that is exempt from disclosure. I am satisfied that in the circumstances, the Police have made a reasonable effort to sever the records and they have disclosed as much information to the appellant as possible.

POLICE'S EXERCISE OF DISCRETION

Where appropriate, institutions have the discretion under the *Act* to disclose information even if it qualifies for exemption under any of the *Act's* discretionary exemptions.

Because sections 38(a) and 38(b) are discretionary exemptions, I must also review the Police's exercise of discretion in deciding to withhold the information. The Police have made representations on this issue for both sections 38(a) and 38(b), including representations which, because of their confidential nature, I am not at liberty to disclose in this order.

I find that the Police properly exercised their discretion in refusing to disclose the information at issue under both sections 38(a) and 38(b) in this case. They took into account and appropriately balanced relevant considerations, including the appellant's right of access, the interests section 8(1)(l) seeks to protect, and other individuals' right to privacy. The Police provided the appellant with partial access to the information she requested, and they disclosed additional information during mediation conducted by this office. I am satisfied that they properly exercised their discretion in withholding the remaining information.

ORDER:

I uphold the Police's decision.

Original signed by _____
Shirley Senoff
Adjudicator

July 30, 2003

TAB 32



Royal Canadian Mounted Police
Gendarmerie royale du Canada

Royal Canadian Mounted Police

[RCMP.ca](#) › [About the RCMP](#) › [Access to Information and Privacy](#)

Access Granted: Restoring Trust in the RCMP Access to Information and Privacy Program

On this page

- [Commissioner's foreword](#)
- [Introduction](#)
- [Rising to the challenge now and into the future: our vision for ATIP](#)
- [Pillar one: Our people](#)
- [Pillar two: Our tools](#)
- [Pillar three: Our procedures](#)
- [Accountability, risk mitigation and assessing achievement](#)

▼ Alternate formats

[Access Granted: Restoring Trust in the RCMP Access to Information and Privacy Program \(PDF, 947 KB\)](#)

▼ List of acronyms and abbreviations

ATIA

Access to Information Act

Access to Information and Privacy

IM

Information management

NHQ

National Headquarters

OIC

Office of the Information Commissioner

OPI

Offices of Primary Interest

RCMP

Royal Canadian Mounted Police

PA

Privacy Act

SOP

Standard operating procedures

TBS

Treasury Board Secretariat

Commissioner's foreword

Access by the public to government information is a core value of our democracy. Accordingly, compliance with the *Access to Information Act* and the *Privacy Act* is crucial for government departments and agencies like the RCMP. Making sure the public has timely access to information,

In particular how and why the RCMP makes decisions and challenges we face, is key to maintaining and strengthening Canadians' trust and confidence in the RCMP – we simply cannot operate without it.

That is why I consider the 2020 review by the Office of the Information Commissioner (OIC) to be so important as it identified a number of challenges in our Access to Information and Privacy (ATIP) program. I am committed to modernizing our ATIP program to help ensure that it meets the expectations of Canadians. We also have the support we need to proceed from the Minister of Public Safety who has highlighted his commitment to supporting the organization to resolving the challenges, specifically through the development and implementation of a strategy and action plan.

I am proud to present this strategy to the Minister. It addresses the Information Commissioner's recommendations, as well as outlines a goal to fully modernize the program and change how we approach access to information. As we modernize, we will be accountable not only to the Minister and Government of Canada partners, but to the Canadian public and will be fully transparent in this process along the way. Our public website will be updated quarterly with information on our plan, and, importantly, our progress.

I am personally committed, as I know that all RCMP employees are, to implementing these changes and am confident this strategy will elevate the RCMP's ATIP program to the high standard that is expected by Canadians.

Brenda Lucki

1084 Introduction

Canadians must have access to information in a timely and well-organized manner in order to have trust in their public institutions – it is a central tenet of our democracy. One of the primary means that the Government of Canada ensures this is through the access to information and privacy (ATIP) request process under the *Access to Information Act* and the *Privacy Act*.

As Canada's national police service, the Royal Canadian Mounted Police (RCMP) works every day in communities from coast-to-coast-to-coast to keep Canadians safe. To do our work successfully, the RCMP depends on the trust, confidence and support of Canadians, who need to have an understanding of our services, as well as the challenges we face and the decisions we make.

Learn more:

- [Access at issue: The need for leadership](#) – Information Commissioner's report

Challenges in meeting our legislated responsibilities

Over the past decade, the RCMP has faced major challenges in responding to ATIP requests. While there are no excuses, there is an explanation: the program has remained largely the same size, while the number of requests have increased, and the tools we use are outdated. In essence, we have not kept pace with change, resulting in a program that is unable to meet expectations and its obligations. This situation was outlined in detail in two recent reviews: the 2019 RCMP internal *Audit of Access to Information and Privacy*; and, the 2020 Office of the Information Commissioner (OIC) *Access at Issue: The Need for Leadership*.

Broadly, the 2019 Audit calls for updates to policies and guidance, including on the roles and responsibilities of employees in the ATIP process and enhancing quality assurance. Similarly, the OIC urges action to address: tasking; policies and procedures; training; electronic systems; and, insufficient resources within the program.

On February 10, 2021, the Minister of Public Safety issued the *Ministerial Directive to the Royal Canadian Mounted Police on Access to Information*, outlining the importance of resolving the issues identified by the Information Commissioner, and directing the organization to develop a concrete strategy addressing how it aims to undertake this effort.

Did you know?

In Canada, two main pieces of legislation outline the government's responsibility in regards to informing the public and the protection of privacy.

- The *Access to Information Act* (ATIA) provides a right to access information contained in records under the control of government institutions. This is under the principle that government information should be available to the public and that exceptions to the right of access should be limited and specific.
- The *Privacy Act* (PA) outlines how government organizations must handle the personal information of individuals, including how individuals can access that information.

Created in 1983, the RCMP ATIP Branch serves as the central contact point for all matters arising from both the ATIA and the PA, and ensures that any exemptions applicable under the Acts are applied before information is released publicly.

On the horizon: emerging trends and technology

We acknowledge and accept both reviews, and recognize that the RCMP must go even further. Technology is evolving at an extremely rapid rate. Canadians expect timely digital service including accessing government services from their computer or from their phone, and not the mail. New technology is introduced every day that has enormous benefits to law enforcement, but often raise significant privacy and information management concerns.

These trends compound our current challenges, requiring us to look to the future and fully **modernize** the way the RCMP approaches access to information and privacy requests, with a focus on digital ATIP services for Canadians requesting and receiving information. Our program must also be proactive – ensuring that privacy and information considerations are at the core of our decision making and information management processes to help the RCMP process requests quickly, efficiently and transparently.

The impact of COVID-19

The COVID-19 pandemic has created challenges for all Canadians – the RCMP has been no exception. We pivoted quickly to a posture that allowed us to maintain front-line and critical services to keep Canadians safe, but the ATIP program has faced unique challenges. For instance, the RCMP still relies heavily on physical records. As Canada's national police service, we also have access to highly sensitive material that must be protected. As such, while most of our work could be completed remotely, some could not. The RCMP continues to work on innovative solutions, and is using this opportunity to leverage lessons from the

pandemic as part of the modernization effort, for instance, by examining how the organization can continue to leverage remote work and enhance digital collaboration.

Supporting change

Efforts are already underway, but reform will not occur overnight; rather our vision requires transformational change over the next five years. As such, it is crucial that the RCMP monitors and tracks modernization efforts, in order to communicate success and adapt to unforeseen challenges. That is why the RCMP also developed:

- **A Modernization Action Plan** that outlines the initiatives we are undertaking to modernize with clear timelines, which will be supported by a Change Management Plan to help identify and mitigate implementation challenges
- **A Communications Strategy** outlining how we will engage with not only our personnel, but Canadians at large, to ensure full transparency

Efforts to date

Our efforts began once the RCMP received its 2019 audit. We took concrete steps to improve the program, including: introducing mandatory training for ATIP employees; developing new policies and procedures; and, contracting support personnel to reduce our backlog.

Rising to the challenge now and into the future: our vision for ATIP

Our goal is to develop a modern program to enable Canadians to make requests quickly, effectively and digitally, and to be fully transparent in our process.

Further, we will develop internal policies and procedures that are clear, accessible and straightforward to increase efficiency, allowing for the rapid completion of requests while ensuring our front line personnel have more time to keep Canada and Canadians safe.

This proactive program will aim to make information available to the public before a request is made through the proactive disclosure of commonly-requested information, and ensure programs and policies are designed at the outset with privacy and access to information in mind.

A focus on privacy

While the Ministerial Direction's primary focus is on responding to the Information Commissioner's 2020 systemic review, our modernization effort provides us with an opportunity to reinforce the RCMP's commitment to protect the private information of individuals. From the unique protections afforded to private information, to the need to assess new technologies and programs with privacy in mind, the RCMP is also committed to make privacy a cornerstone of its modernization strategy.

A vision for Access to Information and Privacy

The RCMP's modern ATIP program is a core business that ensures a transparent RCMP by being:

- **Efficient and expedient** in the processing of requests by the public

Proactive in the release of information

- **Rigorous** in the applications of policies and procedures that meet the highest standards
- **Invested** in its dedicated professionals, who work in a culture that embraces information and privacy considerations, using state-of-the-art technologies

The ATIP program at NHQ and positions across the country will be staffed with highly-trained professionals, using state-of-the-art technologies. Employees will be recruited for their skills and retained by the rewarding work and advancement opportunities in an organization that embraces information and privacy as a fundamental element of its business.

The modernization strategy: enabling success

We know that our future vision is far from what is in place today, but it is not out of reach. We know what must be improved, and how it must be done. To this end, our efforts will be organized across three pillars:

Our people

Includes our efforts to identify investments to expand the program, sustained by robust recruitment, development and training efforts. It also includes promoting organizational change to enhance employee commitment to information and privacy.

Our tools

Includes our efforts to ensure we are using state-of-the-art technology, from modernized case management software to effective technologies in the field to help organize and process requests.

Our procedures

Includes our efforts to bring outdated policies up to date and are regularly maintained, while eliminating redundant ones.

ATIP modernization: a phased approach

The RCMP's ATIP modernization efforts will require a long-term commitment as we will be implementing this strategy over three phases:

Phase 1 (0 to 3 months)

Initial groundwork phase with a focus on establishing the modernization team, consultation groups and strategies. This phase will ensure we have a strong foundation on which to build our long-term implementation efforts.

Phase 2 (3 to 12 months)

Efforts to implement change that can be accomplished internally, such as developing new policies and guidance material, as well as conducting the necessary analysis to determine what additional staffing and technological tools are required to achieve success.

Phase 3 (12 to 36 months)

Long-term implementation efforts, such as the introduction of new recruitment campaigns and operational functions. Procurement and introduction of new software and staffing elements.

Pillar one: Our people

Like all organizations, people are at the core of what we do: whether on the frontlines or in the back office, every RCMP employee helps keep Canadians safe.

Today's ATIP program

At its core, the RCMP's ATIP program is made up of dedicated employees within National Headquarters (NHQ) who perform a large portion of the work to process ATIP requests: from the initial receipt and public engagement; to reviewing material for potential exemptions; and, sending the completed product to the requester. They also work with the

Office of the Privacy Commissioner (OPC) and the OIC to resolve complaints made by the public, maintain operational policies and procedures, and advise on the RCMP's responsibilities under both Acts. This core team is supported by personnel in the divisions across the country. The ATIP liaison officers across the country help coordinate the collection of requests; this function is in addition to their main duties. Additionally, all employees across the country have a responsibility to support the ATIP program through the identification and review of materials subject to requests in their role as Offices of Primary Interest (OPIs).

Actions at a glance

People are at the very core of our modernization efforts – that is why the RCMP will:

- establish a program to attract and develop new talent and provide them with a clear career path
- develop and action a human resource strategy to guide recruitment and retention efforts
- clearly outline the roles and responsibilities of all employees, supported by clear performance standards
- enhance training and delivery to increase awareness of the *Access to Information Act* and the *Privacy Act*, and advance core leadership, digital and communications skills

Our challenges

These dedicated professionals work diligently to ensure that we meet our obligations, under the Acts and to the public. However, they face numerous challenges:

Workload

Over the past two decades, digitization has not only increased public expectations of service, but the size of our own information holdings. This has resulted in an increase in the number of requests, and the size of the responses. Despite this, our program has largely remained the same size and we do not have sufficient employees to meet the growing demand.

Recruitment and retention

ATIP is a unique field, and there continues to be a limited number of applicants who seek ATIP as a career path, which results in a significant demand across the Government of Canada for ATIP professionals, especially in the National Capital Region. This recruitment challenge, combined with an increased retirement rate, has led to vacancies in the RCMP and across the government.

Training and skill development

The reviews recommended that we address a lack of awareness of employee obligations under both Acts. However, while training in relation to these obligations is crucial, it is not enough as there are gaps in other core competencies, such as providing supervisors and managers with advanced leadership and supervisory training and digital skills training.

Culture change

More needs to be done to ensure that all RCMP employees embrace their responsibilities under both Acts as a core part of business, be they a new employee or a seasoned professional.

Our actions

Ensuring that the RCMP has the dedicated resources required, in NHQ and in divisions, supported by robust leadership and training is necessary to modernize the program. That is why the RCMP must adopt a holistic approach to the recruitment and retention of personnel and lead

the transition toward a digital workforce in line with the expected results of the *Policy on Service and Digital*. Some of the actions the RCMP will take include:

Creating a developmental program and recruitment campaign

Based on best practices from other government agencies, in particular Treasury Board Secretariat (TBS), we will put in place a developmental program that attracts new talent from across Canada, and helps us retain employees by providing them with a clear career path.

Expanding our training curriculum

We will introduce mandatory training on both Acts. We will also create a clear, responsibility-based program for ATIP employees that will identify additional competency training, from advanced digital skills to leadership training. This will improve our retention by helping employees advance their careers and manage the pressures of the increasing workload.

Developing a human resource strategy

A modernized ATIP program requires not only additional analysts, but key supporting functions such as dedicated training, policy and quality-assurance personnel. Further, a modern ATIP program requires more management and leadership positions to ensure that there is robust capacity to not only influence RCMP decision-making, but to develop and lead personnel. We will build a strategy to outline both our staffing needs, as well as a plan on how we will fill these positions.

Engaging with stakeholders

ATIP cannot be examined within the context of NHQ alone - front-line employees must have the support they need to meet their obligations. We will work with divisions to identify resource, training and technology needed for success. We will also enhance leadership accountability in the divisions to promote culture change and ensure timely and complete responses.

Examining our resource base

We will do all we can to improve the program within existing funds, but new investment for technology and staff will be necessary. We will work with TBS to examine the resource base of the ATIP program, including potential reallocation of existing RCMP resources or a request for new resources.

Pillar two: Our tools

Technology is crucial to the effectiveness of a modern police organization. Just as the latest technologies assist us in preventing and investigating crime, technology is also crucial to the proper functioning of the ATIP program.

ATIP's current toolset

By their very nature, ATIP requests require processing records. Members of the public submit a request to the RCMP, either through a digital portal or by mail, which is reviewed to identify where the records may be held, and then tasked out appropriately. Assembled records are then collected, reviewed by OPIs, and submitted for assessment and possible exemptions under both Acts. A request could involve a single page, or thousands of multipage documents.

To help manage this process, the RCMP uses a number of technological tools. Our case management software allows personnel to manage requests, keep track of tasks, and collate and redact records. The ATIP program also relies on a broad range of related technologies. For example, physical documents, both in terms of incoming requests as well as records, must be scanned and digitally stored. Public requests often involve video or audio formats, which requires additional software to review and process.

Actions at a glance

Technology is critical to our success – Canadians expect timely and accessible digital services. That is why the RCMP will:

- evaluate and procure user-friendly digital technologies to enhance the public's ability to make and track requests
- evaluate and procure innovative new case management software to facilitate our processing of requests and ensure interoperability with other systems
- identify technology gaps in divisions that create inefficiencies or delays in collecting records
- support broader RCMP efforts to modernize our information management practices to help ensure the RCMP is a more transparent and data-driven organization

Our challenges

Outdated and inefficient tools have created challenges for the efficient functioning of the ATIP program.

Interfacing with the public

While Canadians are able to make requests through an online portal, our website does not emphasize this feature. The RCMP also lacks the necessary tools to allow Canadians to track their online requests, or to learn more about the RCMP's ATIP program.

Antiquated case management software

Our case management system is over a decade old. It lacks many of the necessary features required to streamline processes, handle digital records, and provide necessary business intelligence.

Information management

The RCMP's overall information management (IM) capabilities require significant enhancement – we are too dependent on paper-based processes. This creates enormous challenges, as digitizing records is extremely time consuming.

Additionally, various software products that are currently being leveraged for digital record keeping are not always compatible with our ATIP case management software.

Tools of the trade

Not all employees have access to the tools they need. For example, aging computers have impacted employees working and engaging from home during the COVID-19 pandemic.

Spotlight on information management modernization

The ATIP Program will be collaborating with its IM/IT colleagues on key elements of enterprise IM modernization. The ATIP program will directly benefit from enhancement to various IM services and solutions, including: electronic document management; information and data governance; information architecture; open government; data analytics; and, an enterprise policy hub.

Our actions

Ensuring that our personnel have modern software and technical tools to conduct their activities is critical to a modern ATIP program. That is why the RCMP will be:

Interfacing with the public

Canadians expect to engage digitally with us. As such, we will be introducing a range of improvements, including: updating our external website to be more intuitive and accessible; evaluating and introducing a new digital request portal with the assistance of TBS; and, identifying a

user-centric approach by which the public can monitor and track their request as it is processed.

Procuring of new case management software

With the assistance of TBS, we will explore a number of new case management software options with a goal of ensuring that it is fully compatible with our existing IM software to enhance the efficiency of retrieving and processing records. We will also be evaluating what additional software could benefit the ATIP program, such as innovative technology to process other types of digital media like video and audio.

Analysing hardware requirements

We will also examine whether additional hardware tools are required in both NHQ and the divisions to ensure employees are well equipped to process requests and to reduce technology-related delays.

Pillar three: Our procedures

Policies and procedures are at the core of how we operate. Employees rely on policies and procedures to guide their actions and to understand the organization's expectations of them. They rely on official policies through the Operational Manual, and standard operating procedures (SOPs) drafted within individual units to guide them in their daily activities.

The challenge: finding the right policies at the right time

Outdated and inefficient policies and procedures are creating challenges in meeting our obligations:

Out-of-date policies

Some policies are out of date and refer to processes that are no longer in place. In other cases, they need to be modernized; for example, current policies do not expressly outline the accountability of senior personnel in

the divisions in the ATIP request process, which represents a significant gap.

Policies are difficult to locate

Employees often have to search for these policies and procedures—they are not accessible in a standardized location. This can create delays, or worse, result in inconsistent application of policies in the conduct of ATIP activities.

Need for standardized forms

We lack standardized, digital forms which can help reduce delays resulting from incomplete requests. For instance, the OIC specifically outlines the need for OPIs to indicate how they searched for records – something which could be streamlined through user-friendly, and data-driven digital forms.

Actions at a glance

A modern, efficient ATIP program cannot be successful without clear, transparent and easily-accessible policies and procedures. That is why the RCMP will:

- conduct a robust review of all policies and procedures at every step in the ATIP program with the assistance of a business consultancy firm
- update guidance materials for ATIP personnel in the divisions and NHQ that clearly identifies the mandates, information holdings and points of contact of RCMP business lines
- introduce new digital forms and checklists to help guide OPIs in their collection of records, and help to identify incomplete responses
- update out-of-date operational policies and SOPs to ensure that personnel can have the most up to date guidance on how to proceed
- leverage technology to create central repositories for ATIP related policies and procedures

Our actions

Ensuring that official policies and procedures are available and understood by employees, and that processes are in place to continuously review and improve these procedures, are essential to modernization. Recognizing this, the RCMP will be:

Conducting an efficiency exercise

Review all existing policies and procedures to identify efficiencies where possible, with a goal of reducing the overall number of steps in the ATIP process and enhancing overall quality assurance and accountability.

Updating the core policy and SOP suite

Efforts have already begun to update the official policy and ATIP SOP suite, but these efforts will be expanded to address all identified areas for improvement. We will ensure this effort is continuous, so that policies and procedures remain up to date as other initiatives are implemented. This will help ensure that our decisions are data-driven and based on evidence, and that we have robust quality assurance mechanisms in place. Further, this will help us identify what information Canadians commonly request, and develop the means by which to release this information proactively. This will help us be more transparent with Canadians while helping to reduce the number of requests received.

Going digital

Develop new, data driven, user-friendly digital forms and guidance tools to help our employees respond to requests. For instance, we will create a new digital OPI checklist and examine new, digital tools to help intake personnel appropriately task requests.

Developing a Big Book of Answers

We will make policies easy to locate and accessible for all ATIP employees by making them available at a click of a button in a central location. As part of the Our People pillars' training curriculum, training materials will

be updated to ensure employees are aware of the location of the policy and procedure suite.

Accountability, risk mitigation and assessing achievement

This strategy outlines an ambitious plan to modernize the ATIP program. Implementation will not be without its challenges – that's why it is crucial that our modernization efforts are fully accountable, anticipate and mitigate risks, and have clear indicators for success.

Governance and accountability

The RCMP is developing a robust governance framework to identify various accountability mechanisms to guide our efforts and ensure success. For instance, internal governance will be ensured through a number of oversight bodies such as the Senior Management Team, supporting management committees and the RCMP Management Advisory Board.

External to the RCMP, structures such as the Government of Canada Enterprise Architecture Review Board will be leveraged to ensure that efforts to modernize our software and digital services are fully informed by the latest guidance and direction from the Government of Canada, and are innovative and user friendly. This will also help ensure that the RCMP adheres to TBS policies and directives such as the Policy on Access to Information; the Policy on Privacy Protection; Policy on Service and Digital; the Directive on Service and Digital policies; and the Directive on Open Government, to help meet the government's commitments to transparency, accountability and service and digital transformation. We

will continue to seek support and guidance from TBS in the implementation of this strategy and through the ongoing leadership and support TBS provides to the entire ATIP community.

Ultimately, this modernization effort is about improving our services to Canadians. That is why the RCMP is committed to remaining accountable to the Canadian public through quarterly progress updates on our website to identify not only our successes, but any challenges we may encounter.

Risk identification and mitigation

The RCMP will work to identify innovative solutions to modernize the ATIP program. As with any effort to modernize, it will not be without risk – initiatives could fail, or have the opposite affect to that desired. We will not shy away from being innovative just because there is risk – we must pursue well considered risk in order to achieve success, and accept that there may be mistakes or missteps. When outcomes do not meet our expectations, we will analyse them to discover what did not work, and modify our approach accordingly. Initiatives will be piloted before being put in place to identify and address potential concerns and mitigate them early. Further, initiatives will be fully consulted and reviewed continuously to identify, evaluate and, where possible, mitigate potential risks.

Assessing performance

The RCMP will track our progress through the informed and descriptive indicators outlined in the Modernization Action Plan, which includes clear timelines. Through this formal approach, supported by the robust accountability and governance structure, we will ensure that implementation remains on track, and supported by senior management

and employees alike. To evaluate the outcomes of initiatives, and through consultation sessions with employees, we will monitor impacts on our compliance rates. Through the development of clear performance metrics, we will be able to relate longer-term impacts of modernization initiatives, providing a more accurate indication of the success of the approach. Ultimately, the success of this strategy will be measured in a gradual increase in compliance rates, as well as a steady decrease in public complaints.

Conclusion

We are responsible under the *Access to Information Act* and the *Privacy Act* to provide Canadians with timely access to information and are confident that this strategy will signal the commitment in meeting those responsibilities. Canadians expect the best from us and we must meet their expectations.

Major changes in modernizing culture and fundamental practices do not occur overnight – we are in this for the long-term. However, we will also be making every effort to identify immediate and impactful solutions to increase our compliance rate and address the recommendations by the Information Commissioner and our own internal audit, as well as necessary improvements to enhance our compliance under the *Privacy Act*. We are confident that this strategy and plan puts us on the right path, and we are committed to keep momentum going until, and even after, the RCMP ATIP program is fully modernized and responsive to the needs of all Canadians.

We won't stop until access to information and our obligations under the *Privacy Act* move to the forefront of our actions and becomes rooted in our culture.

Date modified:

2022-02-17

TAB 33

Resources

Home > Access at issue: The need for leadership

Access at issue: The need for leadership

Systemic investigation of the RCMP

Special Report to Parliament from the Information Commissioner of Canada

November 17, 2020

Download PDF version

Submit a complaint



"Change is needed now. Access officials must have the resources and tools they need to respond efficiently and effectively to access requests. The culture of secrecy must end. The right of access must be upheld."

Submit a complaint

Information Commissioner of Canada

Introduction

I initiated an investigation into systemic issues in the Royal Canadian Mounted Police's (RCMP, ~~(Royal Canadian Mounted Police)~~) ability to provide timely access to information given my growing concern about:

- Complaints to the Office of the Information Commissioner (OIC, ~~(Office of the Information Commissioner of Canada)~~) that indicated that the RCMP is persistently unable to meet statutory timeframes under the *Access to Information Act* for responding to access requests.
- The consistent failure of the RCMP to provide representations to the OIC during delay complaint investigations.

This report is tabled in Parliament several months into a global pandemic that has profoundly impacted the right of access – not just in Canada – but around the world. I would like to stress that the situation at the RCMP is critical and may soon be past the point of no return, unless senior leaders within the organization take action immediately. It is vital that the Minister of Public Safety and Emergency Preparedness, who has responsibility for the RCMP, ensure that the necessary resources, processes and tools are in place so that the RCMP can start meeting its obligations under the Act.

The RCMP asserts it has implemented many strategies to improve response times under the Act. However, my investigation revealed that the strategies implemented to date have failed to improve the RCMP's performance. I believe that the RCMP will continue to fail in effectively managing access requests if leaders do not do more to improve the internal culture, along with the current processes and access to information program infrastructure.

I must also report that I was disappointed by RCMP's lack of responsiveness during this investigation. I received no communication that would convince me that the RCMP is truly ready to address these problems.

The following presents a synopsis of the issues and recommendations made at the conclusion of the investigation. A copy of the findings and the 15 recommendations I made to the Minister of

Public Safety, as well as his response, are included as appendices. The final report of this systemic investigation is found [here](#).

Ultimately, this special report illustrates the disappointing facts associated with the review of the RCMP's access to information program, facts which support my contention that there is an urgent requirement to address six problem areas. There is clear evidence that the RCMP's inability to meet statutory timeframes under the Act is the norm, not the exception.

On more than one occasion in recent months, I have signaled that the Government of Canada must develop a new vision for the access system, which otherwise is in danger of collapse. Modernization must centre on innovation, new technology, and adequately resourced and equipped access units across government. There is no need to wait for legislative review to address deficiencies that are operational in nature. Leaders within government institutions must address the fact that they have not taken all appropriate measures to ensure that they properly uphold access rights, as required by the law as it currently stands. They are letting Canadians down.

The RCMP Commissioner and the Minister both appear to accept the *status quo* and are only prepared to commit to minimal improvements without a clear plan of action or timelines. In the current context, this is simply insufficient.

Canadians rightfully expect that the police force for Canada, in charge of enforcing Canadian law, will itself comply with it. The gravity of the situation at the RCMP calls for bold and comprehensive action to turn the tide.

I want Canadians to know that I will continue in my efforts to pursue meaningful change across the federal access system through various means. These include investigations of other government institutions with a view to encouraging compliance and operational improvements, and using the order-making powers granted to me in the June 2019 amendments to the Act.



Caroline Maynard
Information Commissioner of Canada

 Submit a complaint 

"I often say that leadership is key to ensuring the access to information regime is open and transparent. Strong leaders within the public service are essential to implementing the measures required to live up to these principles."

-Statement by the Information Commissioner on
International Right to Know Day



ACCESS REQUESTS completed in under 30 days:

2016-2017

Submit a complaint
2,249

2018-2019

1,101

Percentage decrease:

↓-51%

The RCMP Systemic Investigation

The RCMP is a large and complex organization of more than 20,000 police officers and nearly 10,000 civilian employees in over 700 detachments in 150 communities across Canada. It also provides policing services in more than 600 Indigenous communities. Interest in its activities is significant and historically it has received a high volume of access to information requests.

The OIC reviewed statistical evidence about requests and complaints, and interviewed members of the RCMP Access to Information and Privacy (ATIP (Access to Information and Privacy)) Branch in order to understand how the flow of access requests is normally managed. Training materials available to staff were also assessed.

The OIC sent its letter of notice to the RCMP about initiating an investigation into its access to information operations on January 21, 2019. In February 2019, the RCMP confirmed that it had

4,532 active access to information requests of which 4,179 (92 percent) were beyond the statutory due date to respond.

Table 1 from the RCMP's own report to Parliament about its access to information activities shows that, despite its efforts, it takes the RCMP significantly more time to respond to access requests now when compared to the performance reported three years ago. The report indicates that the RCMP completed 55 percent fewer access requests in less than 30 days in 2018–2019 when compared to its performance two years before.

Table 1: Completion time for access requests, 2016–2017 to 2018–2019 – Annual Report to Parliament 2018-2019 on the *Access to Information Act* and the *Privacy Act*

	2016– 2017	2017– 2018	2018– 2019	Percentage increase/decrease (2016–2017 to 2018–2019)
1 to 15 days	1,017	397	545	-46%
16 to 30 days	1,232	493	556	-55%
31 to 60 days	775	516	633	-18%
61 to 120 days	481	650	522	9%
121 to 180 days	142	341	273	92%
181 to 365 days	148	389	942	536%
More than 365 days	63	181	705	1,019%

"This is clear evidence that the RCMP's inability to meet statutory timeframes under the Act is the norm, not an exception."

– Information Commissioner to Minister of Public Safety



ACCESS REQUESTS
carried over to the next year:

2015-2016

Submit a complaint
224

2018-2019

3,688

Table 2 shows the number of requests the RCMP carried over from one fiscal year to the next grew from 224 at the end of 2015–2016, to 3,688 outstanding requests by the end of 2018-2019. This increase is despite an overall drop in the number of requests received. Between 2016-2017 and 2018-2019, the number of requests that remained unanswered in 365 days rose by over 1000 percent.

Table 2: Access to information caseload, 2016–2017 to 2018–2019 – Annual Report to Parliament 2018-2019 on the *Access to Information Act* and the *Privacy Act*

	2016–2017	2017–2018	2018–2019
Outstanding requests from previous year	224	1,192	3,428
Requests received	4,826	5,203	4,436

	Submit a complaint	2016–2017	2017–2018	2018–2019

1114

Requests closed	3,858	2,967	4,176
Deemed refusals	1,336	2,047	2,979
Requests carried over to next year	1,192	3,428	3,688

Information Commissioner's recommendations

This review identified six issues of concern that have an impact on the RCMP's ability to respond to access requests in a timely manner.

Tasking

1

Procedures

2

Training

3

4

Electronic Systems

5

Insufficient Resources

6

Comprehensive strategy to meet access obligations and reduce the backlog

The RCMP and the Minister did not disagree with the Commissioner's focus on these six issues and have asserted that the strategies implemented have been effective at improving timelines. This assertion is not supported by the evidence obtained through the OIC's investigation.

SIX ISSUES

Text version



Submit a complaint



1. Tasking – The trigger for Offices of Primary Interest to search for and produce records related to an access request

The first step for all government institutions responding to an access to information request is to “task” or assign certain officials within the organization with finding the relevant documents that will constitute the official response. This tasking procedure is a critical step that begins with the in-house ATIP (Access to Information and Privacy) Office. It requires knowledge of the organization and an ability to identify the Office of Primary Interest (OPI (Office of Primary Interest)) - and there may be more than one - most likely to hold those documents.

At the RCMP, poor task assignment has led to many requests being bounced around from one OPI to another, sometimes producing a NIL response (i.e. “we have no records”). When a requester suspects that additional records exist, they may complain to the OIC. In one instance, a requester sought records related to a high-profile shooting in Nova Scotia for which the RCMP had been given jurisdiction to investigate. The RCMP responded that it had no relevant records even though it was obvious that such a response made no sense. The requester complained and ultimately, thousands of responsive records were identified, but only after the OIC started investigating.

This investigation found that the RCMP's tasking processes are generally ineffective and inadequate and, in turn, do not ensure accurate responses to requests.

Commissioner's Recommendations

- Review tasking processes to identify what impedes the processing of records and delays in responding to requests
- Implement measures to reduce or eliminate these problems (e.g., facilitate the ATIP Intake Unit's ability to identify the relevant and correct OPIs when tasking):
 - Require OPIs returning NIL responses to provide details about the search they conducted
 - Require OPIs to develop and provide an evergreen reference document to the ATIP Intake Unit, in a consistent format, that explains their programs, mandate and

information holdings, and the electronic and/or paper information management systems they use

Submit a complaint

Identify best practices for tasking and share them with the ATIP Intake Unit regularly

Response from the Minister of Public Safety and Emergency Preparedness

The RCMP's ATIP Branch will review and update their current OPI template to expand the reference to knowledge, roles and OPI responsibilities, which will facilitate tasking to the proper location in the first instance.

There are plans to prepare a checklist for OPIs, as well. However, the RCMP did not commit to ensuring that search parameters be documented when an OPI replies with a NIL response.

Despite the OIC's findings, the Minister did not commit the RCMP to ensuring that search parameters be documented when an OPI replies with a NIL response. Nor did he commit the RCMP to implementing a process that will ensure its tasking processes remain evergreen.

The Minister's response on tasking is not satisfactory, as it does not address two out of three recommendations. Improvements generated by the revision of templates and implementation of a checklist are unlikely to be sustained over time, given there is no commitment to ongoing process review.

"...an institution must, within the 30-day period or an extended period, register the request, task program officials with searching and retrieving responsive records, scan and process the records, apply appropriate exemptions or exclusions, and issue a final response to the requester." – Information Commissioner to RCMP Commissioner



2. Procedures – Documented, consistent and auditable procedures are more likely to produce reliable results in a timely manner

When institutions receive access requests, they must process all responsive records under their control, regardless of format, and apply necessary and limited severances to that information, as permitted by the Act. Documented, consistent and auditable procedures are more likely to produce reliable, timely results.

Government institutions that manage access requests in a timely and efficient manner have clear protocols that delineate each step in their internal process. And they regularly check back to see

that those processes are working.

The OIC investigation found that the RCMP does have Standard Operating Procedures (SOP (Standard Operating Procedures)s) related to processing and responding to access requests, which can be found in training materials, checklists and email communications. Unfortunately, we found no evidence that these SOPs are consistently applied across the organization or audited for effectiveness. As a result, staff lack knowledge of standardized procedures (and related skills) that would contribute to the effective management of requests.

Commissioner's Recommendations

- Review and keep SOPs introduced in 2017 evergreen and relevant
- Regularly share updated procedures with those across the RCMP involved in responding to access requests
- Implement a process for access staff to monitor the implementation of SOPs across the RCMP

Response from the Minister of Public Safety and Emergency Preparedness

The RCMP committed to implementing a cyclical review process for their SOPs to ensure they remain up to date.

The Minister did not commit the RCMP to implementing an audit capacity to ensure that SOPs are implemented consistently across the organization and over time.



3. Training – Employees who receive adequate training are better able to perform in their role

1119 Training are better able to perform in their role. Training lays the foundation for setting expectations in an organization.

Treasury Board of Canada Secretariat policies require institutions to ensure employees are properly informed of their responsibilities under the Act and receive adequate training.

Training lays the foundation for setting expectations in an organization and builds knowledge, skills and abilities to meet the standard set. Proper training ensures that employees are aware of their obligations under the Act and the standards the organization has set for its own access to information program.

The OIC's systemic review looked closely at the RCMP's approach to training for those with some responsibility for responding to access requests. While the investigation found the RCMP offered in-classroom and hands-on training to Intake Unit officers and ATIP analysts, this training was not mandatory, nor was there any evidence of plans to make it compulsory.

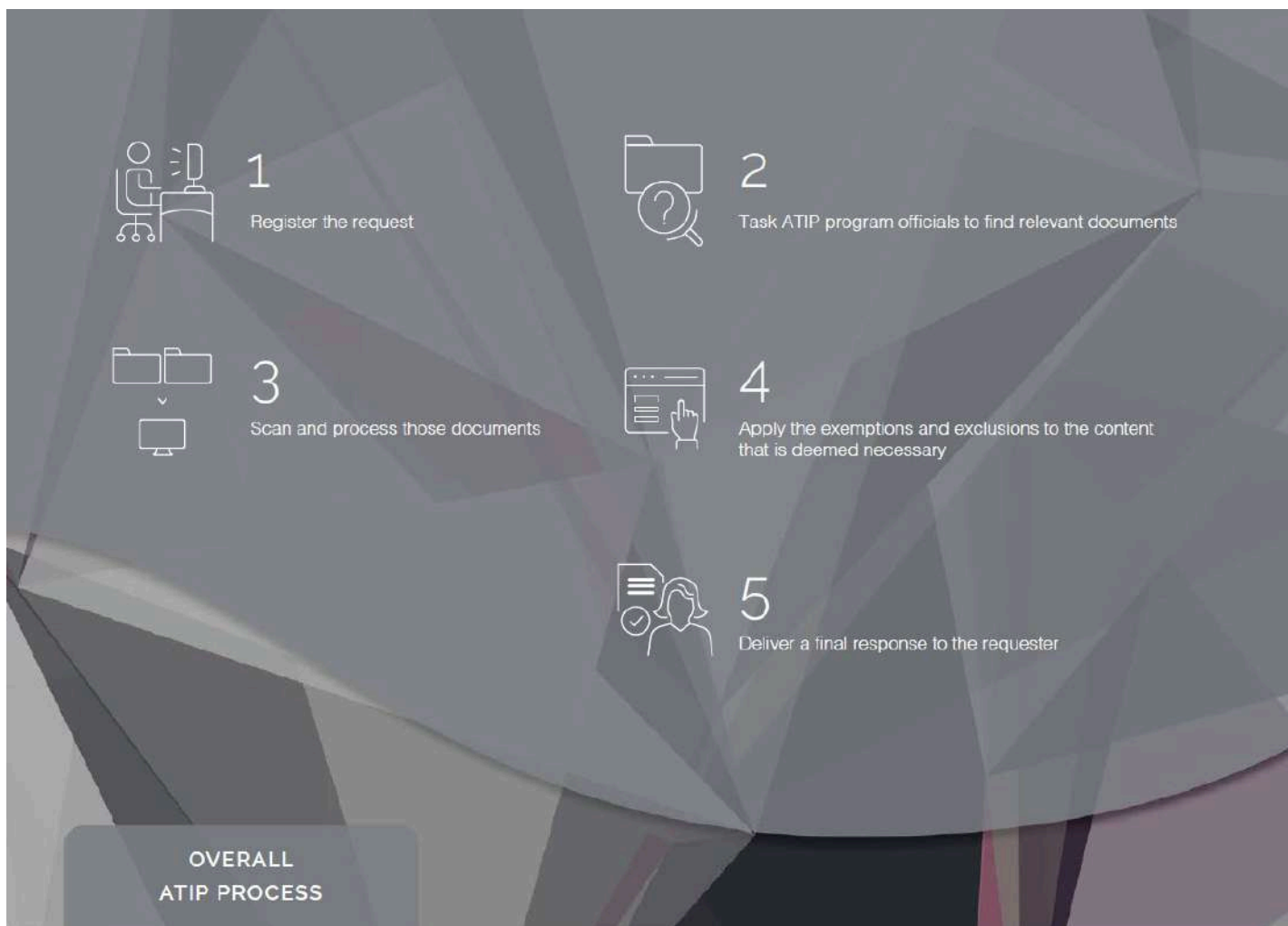
Commissioner's Recommendations

- Continue to develop the training program for ATIP Branch staff and make attendance mandatory
- Hold more information sessions for RCMP employees across Canada and make attendance mandatory
- Develop training for individuals across the RCMP with primary and/or secondary ATIP responsibilities and make attendance mandatory
- Address the specific training needs of OPIs, taking into account the complexity of the organization and the regional dispersion of employees

Response from the Minister of Public Safety and Emergency Preparedness

The RCMP committed to providing yearly, mandatory information sessions for Liaison Officers, developing online training modules for employees with primary and secondary ATIP responsibilities, and continuing to liaise with OPIs. However, the RCMP has not committed to offering mandatory training to these employees.

The Minister's response is disappointing because it only partially addresses the recommendations on training. The Minister has only committed to mandatory information sessions rather than making a full commitment to mandatory training. Yet, based on the findings of the investigation, only a mandatory training program for ATIP staff and employees across the RCMP with primary or secondary ATIP responsibilities is likely to produce significant improvement. Training is what is required to effectively inculcate the knowledge and skills needed to efficiently manage requests.



Text version

Submit a complaint



4. Electronic Systems – Canadians expect efficient, streamlined and digital services

The RCMP is badly served by the archaic information management systems that support its ATIP operations. Intake officers need an inordinate amount of time to manually upload and import records from operational systems into redaction software. And there is a limit to how much data can be uploaded at one time. More worrisome is the fact that these systems regularly crash, the maintenance contract for the redaction software expired years ago, the database is not being regularly serviced, and the RCMP still has not identified a new system administrator. Finally, the current software is not capable of gathering data and producing regular reports or analysis via an in-house dashboard.

The investigation also revealed that while the RCMP has an online portal for receiving access requests it is not integrated with its case management software. As a result, Intake officers must enter all data related to requests into the system manually, increasing the risk of data entry errors and data integrity, and taking time.

The situation could hardly be worse. The RCMP's electronic systems are inadequate to support timely access to information, but there is little evidence of a comprehensive plan to address this situation.

Commissioner's Recommendations

- Upgrade and integrate the digital tools and systems used to process access requests, keeping in mind the need to address the geographic dispersion of RCMP units and employees
- Adopt innovative and efficient digital practices to better serve requesters
- Invest in digital skills development for staff

Response from the Minister of Public Safety and Emergency Preparedness

The RCMP agrees that its current electronic systems are inadequate and cause challenges. It has committed to upgrading digital tools and exploring the possibility of reducing paper-based

records. The RCMP confirmed that it has not yet joined the Treasury Board Secretariat Online Request Service.

The Minister of Public Safety has not committed the RCMP to implementing or adopting more innovative digital approaches or investing in digital skills development for staff. The RCMP will continue to fail at making progress without bolstering its electronic systems and giving its staff access to modern technology.

"The ability to access government information allows citizens to shine a light on government decision-making."

 [Submit a complaint](#) – Statement by the
Information Commissioner on



5. Insufficient resources – Human and financial resources must match the volume of incoming requests and longstanding backlog of open requests

Interviews conducted by the OIC revealed that the RCMP has insufficient human and financial resources to meet its access request workload, which includes both the high volume of incoming requests and a longstanding backlog of open requests.

Commissioner's Recommendations

- Secure adequate human and financial resources for the RCMP's ATIP program/function to allow it to meet its obligations under the Act

Response from the Minister of Public Safety and Emergency Preparedness

Improving compliance with obligations under the Act is a high priority for the RCMP and will inform funding allocation decisions.

Despite the fact that the Government of Canada has recently provided additional funding to the RCMP, it appears that there is still no targeted plan to channel some of those new resources to its ATIP program.



6. Comprehensive strategy to meet access obligations and reduce the backlog

More often than not, over the last three years, when the OIC receives a complaint against the RCMP it usually relates to a delay, meaning that the RCMP has not responded within the statutory timeframe.

The strategy the RCMP has put in place to improve response times involves the hiring of consultants. Unfortunately, the RCMP's own access to information annual statistics (see Table 1) proves that this strategy has been ineffective.

Commissioner's Recommendations

- Implement a detailed strategy that covers each of the six areas of concern highlighted in this report
- Adopt any other measures the RCMP determines would effectively help the RCMP meet its legislated obligations and reduce its backlog of open requests

Response from the Minister of Public Safety and Emergency Preparedness

The RCMP committed to hiring up to twelve consultants.

The RCMP still lacks a comprehensive strategy to address the persistent problems identified by the OIC. Consultants are not a cure-all for the backlog that the RCMP is facing. Without a better plan, the RCMP's efforts to meet its statutory requirements will continue to fall short.

The RCMP's failure to provide representations during delay complaint investigations.

The OIC's investigation mainly focussed on the RCMP's inability to respond to requests within statutory timelines. However, the lack of representations from the RCMP is also an issue. Clearly, the RCMP, like every institution, must deploy limited ATIP resources judiciously, in order to respond to access requests, while simultaneously dealing with the OIC when requesters choose to avail themselves of their recourse mechanism by way of complaint.

That said, as required by the Act, the Commissioner has made it clear that she will continue to seek representations from government institutions under investigation. When they fail to respond, she will not hesitate to conclude any investigation and issue recommendations and orders, when she finds the complaint is well-founded.

"Canadians deserve bold and decisive actions."

-Statement by the
Information Commissioner on
International Right to Know Day

Conclusion

By nearly every measure, the RCMP is failing in terms of its obligation to ensure that Canadians have access to information about its operations and decision-making. While some of the information under its control is sensitive and may justifiably be withheld when personal details are involved or if the matter is before the courts, my investigation found many examples of mismanagement and lack of attention at various step of its handling of access requests. It would appear that the RCMP gives little or no priority to its access to information requirements.

The RCMP's processes and procedures must be tightened and audited, to produce more reliable results. The entire digital infrastructure that underpins the RCMP's access operations is essentially an impediment to those who handle access requests. Funding, training and staffing are significant issues. The size of the request backlog is shocking.

Most worrisome is the lack of action on the part of RCMP leadership. There is no evidence that the solutions put forward to date to address chronic delays and poorly managed processes really made any difference at all. None of the commitments made by the Minister have timelines associated with them. Without a comprehensive plan of redress and clear, targeted completion dates, following through on any of these individual action items could be indefinitely delayed by the various pressures facing an already overwhelmed ATIP team.

The response I received from the Minister falls short on many fronts, particularly when it comes to commitments to improve transparency and timely responses. He has ignored most recommendations and appears unconcerned by the failings identified within the RCMP's ATIP operations.

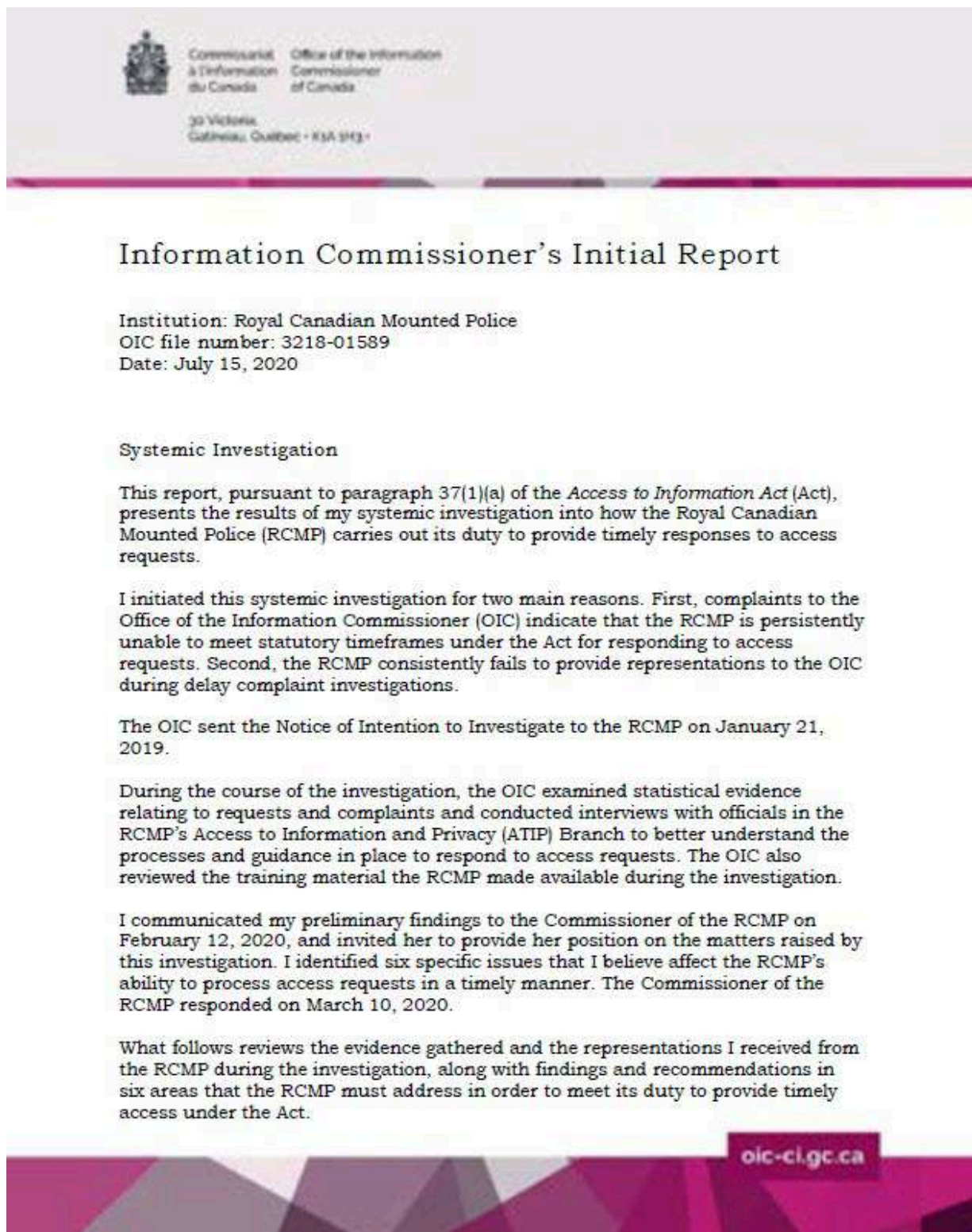
This report offers suggestions about how the RCMP can begin to address the long-standing issues that have hindered its ability to manage its access obligations. But it will take leadership

and commitment to improve on a track record that is sadly not up to the standard that Canadians expect.

Annexes

Annex 1.1

Submit a complaint



Initial Report of the Information Commissioner regarding the Royal Canadian Mounted Police dated July 15, 2020, that conveys the results of the systemic investigation of the department's ATI processes.

Submit a complaint

Information commissioner's initial report

Institution : Royal Canadian Mounted Police

OIC file number: 3218-01589

Date: July 15, 2020

Systemic Investigation

This report, pursuant to paragraph 37(1)(a) of the *Access to Information Act* (Act), presents the results of my systemic investigation into how the Royal Canadian Mounted Police (RCMP (Royal Canadian Mounted Police)) carries out its duty to provide timely responses to access requests.

I initiated this systemic investigation for two main reasons. First, complaints to the Office of the Information Commissioner (OIC (Office of the Information Commissioner of Canada)) indicate that the RCMP is persistently unable to meet statutory timeframes under the Act for responding to access requests. Second, the RCMP consistently fails to provide representations to the OIC during delay complaint investigations.

The OIC sent the Notice of Intention to Investigate to the RCMP on January 21, 2019.

During the course of the investigation, the OIC examined statistical evidence relating to requests and complaints and conducted interviews with officials in the RCMP's Access to Information and Privacy (ATIP (Access to Information and Privacy)) Branch to better understand the processes and guidance in place to respond to access requests. The OIC also reviewed the training material the RCMP made available during the investigation.

I communicated my preliminary findings to the Commissioner of the RCMP on February 12, 2020, and invited her to provide her position on the matters raised by this investigation. I identified six specific issues that I believe affect the RCMP's ability to process access requests in a timely manner. The Commissioner of the RCMP responded on March 10, 2020.

What follows reviews the evidence gathered and the representations I received from the RCMP during the investigation, along with findings and recommendations in six areas that the RCMP

must address in order to meet its duty to provide timely access under the Act.

Investigation

Data on the RCMP's processing of access requests between 2016–17 and 2018–19 sheds light on the increasing problems the RCMP is having in responding to access requests in a timely manner.

The RCMP's report to Parliament on its access to information activities in 2018–19 shows that between 2016–17 and 2018–19, the RCMP took significantly longer to respond to access requests. As Table 1 shows, the RCMP completed considerably fewer access requests in less than 30 days and more than 1000% more in more than 365 days.

Table 1: Completion time for access requests, 2016–17 to 2018–19

	2016–17	2017–18	2018–19	Percentage increase/decrease (2016–17 to 2018–19)
1 to 15 days	1,017	397	545	-46%
16 to 30 days	1,232	493	556	-55%
31 to 60 days	775	516	633	-18%
61 to 120 days	481	650	522	9%
121 to 180 days	142	341	273	92%
181 to 365 days	148	389	942	536%
More than 365 days	63	181	705	1,019%

Second, and also according to the RCMP's 2018–19 report, the number of requests the RCMP carried over from one fiscal year to the next grew from 224 at the end of 2015–16 to 3,688

requests at the end of 2018–19—this is despite an overall drop in the number of requests received (see Table 2).

Table 2: Access to information caseload, 2016–17 to 2018–19

	2016–17	2017–18	2018–19
Outstanding requests from previous year	224	1,192	3,428
Requests received	4,826	5,203	4,436
Requests closed	3,858	2,967	4,176
Deemed refusals	1,336	2,047	2,979
Requests carried over to next year	1,192	3,428	3,688

Third, in 2017–18 the RCMP responded to 31 percent of access requests within the statutory timeframes. By the next year, that figure had dropped to 29 percent. The Act sets out 30 days as the response time, unless an institution validly extends the time to process and respond to the request.

This is clear evidence that the RCMP's inability to meet statutory timeframes under the Act is the norm, not an exception.

The RCMP agrees that it is challenged to respond to access requests within statutory time frames, noting that these challenges relate to and are compounded by the geographical dispersion of 30,000 employees, the large volume of requests and the diverse policing activities it undertakes. The RCMP also states that much of its policing related information is paper-based and spread across various systems rather than in one repository, making it sometimes difficult to retrieve records. The RCMP also contends that the Public Safety portfolio is not only complex but also different from other parts of the public service, especially as it relates to sensitive investigative information that should not be released to the public.

While all this may be true, it does not fully explain the RCMP's delays in responding to requests, particularly since other geographically dispersed agencies within the Public Safety portfolio are

able to meet their obligations under the Act in this regard. This includes the Canada Border Services Agency, which responded to 94 percent of requests on time in 2018–19.

With this context in mind, the OIC also examined a number of aspects of the RCMP's access operations and processes to determine what factors are contributing to delays and what needs to be addressed to rectify the problems.

Tasking

Tasking refers to the process by which staff in the Intake Unit of the RCMP's ATIP Branch notify offices of primary interest (OPI (Office of Primary Interest)) that an access request has been made, and ask OPI representatives to retrieve all the responsive records they have. The Intake Unit relies on a list of all OPIs within National Headquarters and a list of liaison officers for the divisions located across Canada in order to direct its tasking requests.

Previous OIC investigations have revealed that access requests are sometimes tasked to the wrong OPI which produces a NIL response. OPIs will then redirect tasking requests to other parts of the organization, which causes delays. In some cases, it is only when an ATIP analyst begins to process the retrieved records that they realize that the wrong OPI was tasked. In these cases, the tasking process is restarted once again, causing further delay.

The RCMP confirmed that there is a high turnover of employees in the RCMP's ATIP Branch, predominantly at the junior levels. Training is offered regularly and was specifically given to Intake Unit employees in April 2018 and March 2019. To further augment junior employees' capabilities, senior staff mentor members of Intake Unit. Formal standard operating procedures for activities such as tasking have been in place since the summer of 2017.

The RCMP undertook a pilot project in January 2019 to determine whether efficiencies could be gained by having Intake Unit staff review electronic operational records relevant to access requests housed in the Police Reporting Occurrence System and the Police Records Information Management Environment rather than having to task OPIs for records in some instances. The RCMP did not state whether the pilot project was successful or whether it led to more efficiencies in the tasking process.

Based on what I learned about the RCMP's tasking processes, I find them to be inadequate for ensuring timely responses to access requests. Given with the errors in tasking and multiple tasking I learned about during the investigation, I also find that the standard operating procedures have proven ineffective in improving its tasking processes or reducing response times.

Submit a complaint

I recommend that the RCMP:

1. Review its tasking processes to determine the causes of failures that impede the processing of records and delay responding to requests;
2. Implement measures to reduce or eliminate these causes. In particular, facilitate the Intake Unit's ability to identify relevant OPIs when tasking, thereby reducing the need to redirect taskings:
 - Require OPIs returning NIL response to taskings to also provide the Intake Unit with details about the search they conducted;
 - Require all OPIs to develop and provide to the Intake Unit an evergreen reference document in a consistent format that explains their programs, mandate and information holdings, and the electronic and/or paper information management systems they use; and
3. Identify best practices with respect to tasking and share these with the Intake Unit regularly.

Procedures

When institutions receive access requests, they must process all responsive records under their control, regardless of format, and apply necessary and limited severances to that information. Documented, consistent and auditable procedures are more likely to produce reliable results in a timely manner.

As part of the investigation, the OIC examined the RCMP's procedures related to processing and responding to access requests. These procedures were found in training materials, checklists and emails.

The investigation revealed that the RCMP has some procedures for how to use the various electronic systems, checklists and reference guides available for processing and responding to request.

However, there was no evidence that the RCMP has any systematic follow-ups or audits to ensure staff are following the procedures.

In response to my preliminary findings, the RCMP told the OIC that it continually reviews its procedures, including the standard operating procedures introduced in 2017, to find efficiencies.

However, the RCMP did not comment on the lack of auditing processes the OIC identified in the investigation.

Based on what the investigation revealed about the RCMP's procedures for processing and responding to access requests, I find that the RCMP has not taken any steps to ensure that the procedures that do exist are being implemented consistently across the organization. This may mean that employees do not have the necessary knowledge and skills to process access requests in an efficient manner and may contribute to the RCMP's difficulty in providing timely access.

I recommend that the RCMP:

4. Review and keep evergreen the standard operating procedures introduced in 2017;
5. Regularly share updated procedures with access staff and individuals across the RCMP involved in responding to access requests; and,
6. Implement a process for access staff to monitor the implementation of standard operating procedures across the RCMP.

Training

Treasury Board of Canada Secretariat policies require institutions to ensure employees are properly informed of their responsibilities under the Act, and receive adequate training.

Employees who receive necessary training are better able to perform in their role. Training lays the foundation for setting expectations in an organization and builds knowledge, skills and abilities to meet those expectations. I view training as a critical component of transforming any business activity.

During the investigation, the OIC sought to confirm the training opportunities offered to access staff and other individuals across the RCMP responsible for responding to access requests.

The investigation revealed that the RCMP has offered in-classroom and hands-on training to new Intake Unit officers and ATIP analysts. RCMP employees across Canada can attend access to information sessions, and ATIP Branch staff have held engagement meetings with internal stakeholders. However, attendance at these sessions is not mandatory.

The RCMP asserts that it has one of the most thorough training programs for access staff of any Government of Canada institution and that it includes hands-on exercises. Further, the RCMP

noted that training for access staff and OPIs has resulted in improvements in the capacity of access to staff to review responsive records.

The RCMP did not comment on my preliminary finding about there being no mandatory training for all individuals who have access to information as a primary and/or secondary duty. The RCMP also did not provide the number of information sessions offered or the number of individuals who attended the information sessions.

I find that the RCMP's lack of mandatory training for OPIs and/or individuals who have access to information as a primary and/or secondary duty outside of the access office contributes to its inability to provide timely access to information.

I recommend that the RCMP:

7. Continue to develop its training program for ATIP Branch staff and make attendance mandatory;
8. Continue to hold information sessions for RCMP employees across Canada and make attendance mandatory;
9. Develop training for individuals across the RCMP with primary and/or secondary ATIP responsibilities and make attendance mandatory; and,
10. Continue to engage with OPIs to better understand and address their specific training requirements, given the complexity of the organization and the regional dispersion of the employees.

Electronic systems

During the investigation, the OIC learned that a large portion of Intake officers' time is spent uploading and importing records from operational systems into redaction software.

A maximum of 300 pages can be uploaded at a time. Beyond that, the system crashes. Further, at the time of the investigation, the maintenance contract for the redaction software had been expired for years, the database was not being serviced and the RCMP was seeking a new system administrator.

The investigation also revealed that, while the RCMP has an online portal for receiving access requests, it is not integrated with its case management software. As a result, Intake officers must

enter all data related to requests into the system manually, increasing the risk of data entry errors and data integrity, and taking time.

ATIP staff produce weekly dashboard-type reports for senior management, including on open requests. However, due to system limitations, these reports have to be generated manually. This means that as the reports get longer as the year goes along it takes more time to generate them. In addition, since exporting the information to Excel does not generate a useable table (the data is jumbled and impossible to sort) conducting any in-depth analysis of the data is near impossible.

The RCMP confirmed that it has encountered information technology challenges in the past and is now working with its information management group as well as the Treasury Board Secretariat and Public Services and Procurement Canada on the Request for Proposal for new government-wide ATIP software.

Based on what I learned during the investigation, I find that the RCMP's electronic systems are inadequate to support timely access to information. In addition, Canadians expect better, more efficient and streamlined digital services from their government.

I recommend that the RCMP:

11. Upgrade the digital tools it uses to process access requests, including to overcome the geographic dispersion of RCMP units and employees;
12. Adopt innovative and efficient digital practices to better serve requesters; and,
13. Invest in digital skills development for staff.

Insufficient resources

During the investigation, the OIC discussed resourcing issues with a number of ATIP Branch employees.

These officials indicated that the RCMP has insufficient human and financial resources to meet its access request workload—addressing its backlog of open requests and dealing with incoming access requests.

In its response to my preliminary findings, the RCMP acknowledged that resource challenges are inhibiting its capacity to meet its access obligations and stated that it agrees that increased resources would help it meet them.

Further, the RCMP indicated that a departmental review has led to recommendations to the government concerning resourcing requirements, including those of the ATIP Branch. The RCMP

also advised that it is collaborating with other institutions on collective staffing processes.

Based on what I learned during the investigation, I find that the RCMP does not have sufficient human and financial resources to provide timely access to information and meet its statutory obligations under the Act.

I recommend that the RCMP:

- 14. Secure adequate human and financial resources for its ATIP processes to allow it to meet its obligations under the Act.

Comprehensive strategy to meet access obligations and reduce the backlog

During the investigation, the OIC learned that the RCMP hired a team of experienced consultants as part of a three-year plan to reduce the backlog of open requests for which responses are overdue. And, while the RCMP reported in March 2020 that this team had reduced the backlog by 74 percent, it remained at more than 2,000 requests. In my view this is not acceptable. Moreover, the problems this

investigation revealed suggests that the backlog will grow again if the RCMP does not take effective steps to address it.

The magnitude of the problem is clear in the complaints the OIC receives concerning the RCMP (Table 3).

Table 3: Complaints against the RCMP, 2017–18 to 2019–20

			Registered				
Fiscal year	Delay	Time extension	Exemptions/exclusions	Missing / No records	Misc.	Total	Closed
2017-18	318	2	37	76	2	435	332
2018-19	272	4	43	41	6	366	361

			Submitted complaint				

Fiscal year	Delay	Time extension	Exemptions/exclusions	Missing / No records	Misc.	Total	Closed
2019-20	222	2	67	59	4	354	442
Total	812	8	147	176	12	1,155	1,135

Over each of the last three years, complaints about delays in responding to requests have accounted for at least 62 percent of the complaints the OIC has received against the RCMP (with a high of 74 percent in 2018–19). Canadians should be able to expect timely service from the RCMP under a legislated program but the complaints my office investigates against the RCMP suggest otherwise.

Based on all my above findings and the prevalence of delay complaints against the RCMP, I further find that the approaches the RCMP has been taking to date under its three-year plan have been ineffective in solving the problems that plague its processing of access requests and that a more concerted and strategic effort is required.

I recommend that the RCMP:

15. Implement a detailed strategy that covers each of the areas I find are impeding the RCMP's ability to respond to access requests in a timely

manner and any other measures the RCMP determines would be effective in helping the RCMP meet its legislated obligations and reduce its backlog of open requests.

Conclusion

The access to information system is key to safeguarding Canadians' trust in their government. I have publicly signalled several times recently that this system is in a critical phase and may soon be beyond repair if certain ongoing and developing issues remain unaddressed. This is also true for the RCMP, which persistently fails to meet its legal obligations under the Act.

The RCMP responded to my letter by highlighting the many strategies it had adopted in the past to improve response times under the Act. However, my investigation revealed that the strategies implemented by the RCMP to-date have failed to effectively make it possible for the RCMP to

provide timely responses to access requests. [Submit a complaint](#)

The recommendations I make in this report are some of the steps the RCMP can take to address this. As Minister of Public Safety and Emergency Preparedness, it is your responsibility to ensure that the necessary resources, processes and tools are in place so that RCMP officials, including the Commissioner, to whom you have delegated your authority as head of the RCMP under the Act, can start meeting their statutory obligations with regard to access.

In other words, it is incumbent on you to take any necessary actions to ensure that our Country's national police force complies with the law on your behalf. Canadians expect it and deserve no less.

Finally, I will also note for the record that, although I have not made findings and recommendations on the RCMP's ongoing failure to provide representations to my office, this practice compromises the OIC's ability to effectively investigate delay complaints. Providing representations is the RCMP's opportunity to explain the particular reasons for the delays and would allow me to better understand the situation and better inform the recommendations and/or orders I make.

I will therefore continue to ask for representations in each and every case that I investigate, as required by the Act. I will, however, not hesitate to finalize any investigation by issuing my recommendations and orders directly to you, even when the RCMP chooses not to take the opportunity to submit representations.

Please inform me by August 10, 2020, as to whether you intend to implement my recommendations and the action you intend to take to do so. If not, please provide me with the reasons why you will not be taking the recommended action. I also urge you to propose any additional actions that could allow the RCMP to improve its response times and reduce its backlog.

Should you wish to discuss any aspect of this matter, please do not hesitate to communicate with me at 819-994-0001.

Caroline Maynard
Information Commissioner of Canada



AUG 25 2020

Caroline Maynard
Information Commissioner of Canada
30 Victoria Street
Gatineau, Quebec K1A 1H3

Dear Commissioner Maynard:

Thank you for providing a copy of your July 15, 2020, Initial Report on how the Royal Canadian Mounted Police (RCMP) processes access to information requests.

I am assured that the RCMP will examine each recommendation carefully and, where appropriate, articulate a way forward, including the identification of best practices to determine the root causes of the challenges outlined in your document and find efficiencies to minimize the delays in responding to requests.

The RCMP is fully committed to meeting its responsibilities under the *Access to Information Act* (Act) and ultimately to being transparent with Canadians.

The RCMP's responses to your recommendations, per theme, are outlined below.

1. Tasking

The RCMP Access to Information and Privacy (ATIP) Branch will review and update their current Office of Primary Interest (OPI) template to expand the knowledge, roles and responsibilities of each OPI, which will facilitate tasking to the proper location in the first instance. In addition, an OPI guidance checklist will be developed for each OPI to complete and submit when returning relevant records with all pertinent details about the search conducted. The checklist will include:

- database, folders, etc. searched;
- parameters of the search used (e.g., key words, date ranges);
- individual responsible for conducting the search and the date of the search; and,
- whether any other areas may have holdings of the information (e.g., divisions, detachments).

Canada

Letter from the Minister of Public Safety and Emergency Preparedness to the Information Commissioner dated August 5, 2020, that responds to the

Commissioner's findings and provides a further update regarding RCMP (Royal Canadian Mounted Police) actions.

Caroline Maynard

Information Commissioner of Canada 30 Victoria Street
Gatineau, Quebec K1A 1H3

Dear Commissioner Maynard:

Thank you for providing a copy of your July 15, 2020, Initial Report on how the Royal Canadian Mounted Police (RCMP (Royal Canadian Mounted Police)) processes access to information requests.

I am assured that the RCMP will examine each recommendation carefully and, where appropriate, articulate a way forward, including the identification of best practices to determine the root causes of the challenges outlined in your document and find efficiencies to minimize the delays in responding to requests.

The RCMP is fully committed to meeting its responsibilities under the *Access to Information Act* (Act) and ultimately to being transparent with Canadians.

The RCMP's responses to your recommendations, per theme, are outlined below.

1. Tasking

The RCMP Access to Information and Privacy (ATIP) Branch will review and update their current Office of Primary Interest (OPI) template to expand the knowledge, roles and responsibilities of each OPI, which will facilitate tasking to the proper location in the first instance. In addition, an

OPI guidance checklist will be developed for each OPI to complete and submit when returning relevant records with all pertinent details about the search conducted. The checklist will

- database, folders, etc. searched;
- parameters of the search used (e.g., key words, date ranges);
- individual responsible for conducting the search and the date of the search; and,
- whether any other areas may have holdings of the information (e.g., divisions, detachments).

The above will help guide and assist both the RCMP ATIP Intake Unit and Liaison Officers (LOs) in identifying the relevant records to better respond to a request.

2. Procedures

The RCMP ATIP Branch will develop, communicate and implement a cyclical review process of their standing operating procedures to ensure they remain up-to-date. This will better inform employees and ensure consistency across the RCMP in the processing of access requests, and reduce the response time for providing relevant records.

3. Training

The RCMP will continue to provide and formalize access to information training to ATIP Branch staff and employees across the RCMP by:

- providing yearly mandatory information sessions to all LOs across the RCMP;
- continuing with the development of an ATIP 101 online course consisting of two modules, one for all RCMP employees who have primary and/or secondary ATIP responsibilities and one dedicated to the roles and responsibilities of all LOs across the RCMP;
- exploring the possibility of mandating this online course to all affected employees and requiring all new ATIP employees to take the Canada School of Public Service on-line course; and,
- continuing to liaise and engage regularly with all 750 OPs to continue addressing their training requirements.

This will ensure the enhancement of employee training and create efficiencies across the RCMP in providing timely access to information.

4. Electronic systems

[Submit a complaint](#)

The RCMP agrees that its current electronic systems are inadequate and cause challenges. The RCMP obtained a new virtual server in April 2019 that has led to efficiencies in processing time and reliability on its systems. Additional efforts include:

- continued work with the RCMP's Information Management branch to upgrade digital tools and explore the possibility of streamlining flow of information and reducing paper-based records that cause challenges in retrieving records;
- being part of the of the new ATIP online Request Service (AORS), in collaboration with the Treasury Board Secretariat. The new service will offer Canadians the ability to submit access to information requests, and to have those requests automatically re-distributed to a Responding Institution among the 240-plus Government of Canada institutions subject to Part 1 of the Act. The onboarding of this new initiative was scheduled for May 2020; however, due to the global pandemic, it has been delayed; and,
- planned AORS and new ATIP Software to assist staff in alleviating data entry errors, improving data integrity, reducing time delays and improving reporting capability.

In securing better technological solutions, the RCMP's digital environment will be enhanced.

"The RCMP is fully committed to meeting its responsibilities under the Access to Information Act (Act) and ultimately to being transparent with Canadians." – The Honourable Bill Blair, Minister of Public Safety and Emergency Preparedness to Caroline Maynard, Information Commissioner of Canada, August 25, 2020

5. Insufficient resources

The Government has just recently provided additional funding to the RCMP to take measures to address program integrity issues. Shoring up the ATIP program to improve compliance with obligations under the Act is a high priority for the RCMP and will inform allocations decisions regarding the new funding.

6. Comprehensive strategy to meet access obligations and reduce the backlog

The RCMP's ATIP Branch currently has nine consultants helping to reduce its backlog. The current contract ends on March 31, 2021; however, there is engagement with Public Services and Procurement Canada (PSPC (Public Services and Procurement Canada)) to allow for twelve consultants. The current contract has demonstrated that this initiative is helping reduce backlog.

In conclusion, I reiterate that the RCMP will take all measures to meet its responsibilities under the Act and is fully committed to providing Canadians with information in a timely manner.

Yours sincerely,

The Honourable Bill Blair, P.C. (Privy Councillor), C.O.M. (Commander of the Order of Merit of the Police Forces), M.P. (Member of Parliament)

c.c.:

Commissioner Brenda Lucki Royal Canadian Mounted Police

Alison Whelan

Chief Strategic Policy and External Relations Officer

Royal Canadian Mounted Police

Superintendent Richard Haye

Submit a complaint

Director, Access to Information and Privacy Branch

Royal Canadian Mounted Police

Date modified:

2021-12-02

 Submit a complaint 

TAB 34



Royal Canadian Mounted Police

[RCMP.ca](#) > [About the RCMP](#) > [Publications and manuals](#)

2024-2025 Annual Report to Parliament on the Administration of the *Access to Information Act*

On this page

- [Introduction](#)
- [Organizational structure](#)
- [Delegation order](#)
- [Performance for 2024-2025](#)
- [Training and awareness](#)
- [Policies, guidelines and procedures](#)
- [Initiatives and projects to improve access to information](#)
- [Summary of key issues and actions taken on complaints](#)
- [Proactive publication under Part 2 of the *Access to Information Act*](#)
- [Monitoring compliance](#)
- [Appendix A - Delegation order](#)

▼ Copyright information

2024-2025 Annual Report to Parliament on the Administration of the *Access to Information Act*

© His Majesty the King in Right of Canada, as represented by the Royal Canadian Mounted Police, 2025

- ~~ISSN (International Standard Series Number)~~ 2564-2766
- Catalogue number PS61-41E-PDF

▼ List of acronyms and abbreviations

ATIA
Access to Information Act

ATIP
Access to Information and Privacy

BWC
Body Worn Camera

GC
Government of Canada

information management

IRCC

Immigration, Refugee and Citizenship Canada

IT

information technology

LGBT

Lesbian, Gay, Bisexual, Transexual

LO

Liaison officer

OIC

Office of the Information Commissioner

OPC

Office of the Privacy Commissioner

OPI

Office of Primary Interest

PA

Privacy Act

PIA

Privacy Impact Assessment

RCMP

Royal Canadian Mounted Police

SEC

Senior Executive Committee

SOP

Standard operating procedure

TBS

Treasury Board of Canada Secretariat

▼ List of charts

- [Chart 1: Backlog Accumulation and Reduction](#)
- [Chart 2: End-of-year backlog reduction](#)
- [Chart 3: Projected impact of strategic measures on page processing](#)

▼ List of tables

- [Table 1: Compliance](#)
- [Table 2: Active requests from previous reporting periods](#)
- [Table 3: Completion time for closed ATIA requests](#)
- [Table 4: Completion times for consultation requests](#)

- [Table 6: Complaints](#)
- [Table 7: Proactive publication requirements](#)
- [Table 8: Schedule](#)

Introduction

The Royal Canadian Mounted Police (RCMP) is pleased to outline in this annual report details of the manner in which it discharged its responsibilities in relation to the *Access to Information Act* (ATIA) during the reporting period. The report is prepared and tabled in Parliament in accordance with section 94 of the *Access to Information Act*. The purpose of the ATIA is to enhance the accountability and transparency of federal institutions in order to promote an open and democratic society and to enable public debate on the conduct of those institutions. To further that purpose:

- Part 1 extends the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific, and that decisions about the disclosure of government information should be reviewed independently of government.
- Part 2 sets out the requirements for the proactive publication of information.

The 2024-2025 fiscal year marks the RCMP's fourth year of its five-year modernization plan for its Access to Information and Privacy (ATIP) program. The RCMP is pleased to report improvements to its performance and program overall and is proud of its ongoing collaboration with our employees across Canada, as well as our network of partnerships with other Government of Canada departments. These improvements are also a testament to the hard work and dedication of the ATIP Branch's employees.

Ensuring that Canadians have timely access to information—enabling them to understand the decision-making process and the challenges faced—is essential to building and maintaining trust in the organization. The RCMP takes these responsibilities seriously and is committed to meeting the expectations of Canadians while protecting the integrity of the investigations undertaken on their behalf. Canadians are encouraged to monitor our work through the public website at

<https://rcmp.ca/en/corporate-information/access-information-and-privacy/access-granted-restoring-trust-rcmp-access-information-and-privacy-program>.

Organizational structure

Royal Canadian Mounted Police (RCMP)

As a federal, provincial, territorial and municipal policing body, the RCMP provides federal policing services to all Canadians and policing services under contract to the three territories, eight provinces, and more than 150 communities delivered through more than 700 detachments across Canada, 600 Indigenous communities and three international airports.

The RCMP's mandate is multifaceted and includes preventing and investigating crime; maintaining peace and order; enforcing laws; contributing to national security; ensuring the safety of state officials, visiting dignitaries and foreign missions; and providing vital operational support services to other police and law enforcement agencies within Canada and abroad.

A Commissioner leads the RCMP and is supported by a Senior Executive Committee (SEC) made up of regular members, civilian members and public servants. The role of SEC is to develop, promote and communicate strategic priorities, strategic objectives, management strategies and performance management for the purpose of direction and accountability.

The organization is subdivided into 15 divisions (10 provinces, 3 territories, Depot Division and National Headquarters in Ottawa), each of which is under the direction of a Commanding Officer or Director General.

National Headquarters includes 10 business lines and is structured as follows: Federal Policing, Contract and Indigenous Policing, Specialized Policing Services, Corporate Management and Comptrollership, Human Resources, Internal Audit and Evaluation, Professional Responsibility Sector, Strategic Policy and External Relations, Reform Accountability and Culture, and Legal Services.

Access to Information and Privacy (ATIP) Branch

The RCMP established the ATIP Branch in 1983, as the central point of contact for all matters arising from both the ATIA and the *Privacy Act* (PA). The ATIP Branch reports through the Chief Digital Officer to the Deputy Commissioner of Specialized Policing Services. The IM/IT Branch was renamed the Digital Program in December 2024. The new Digital Program is responsible for leading the technological transformation of the RCMP,

Working with Analytics, Data and Information Management and the ATIP Branch. While this is not a common structure within government, it unites, Information Management (IM) and Information Technology (IT) with ATIP further enabling the modernization of the ATIP program. These benefits include a more high-profile role for the Branch in areas such as digital records management, open government, and the declassification of historical records.

The ATIP Branch's Director General acts on behalf of the head of the institution as the Departmental Access to Information and Privacy Coordinator. The ATIP Coordinator ensures compliance with both the spirit and the intent of the ATIA, as well as all associated regulations, policies and guidelines. The Director General position is also tasked with leading the program's broad modernization efforts. The ATIP Branch is made up of 122 employees and 11 consultants who work on requests under both the ATIA and the PA.

For a breakdown of the groups and positions responsible for meeting each applicable proactive publication requirement under Part 2 of the ATIA, see the section "Proactive Publication under Part 2 of the ATIA" below.

Access to Information Stream

Led by a Director, the Access Stream is responsible for responding to all formal and informal requests made under the ATIA. This stream is made up of four disclosure teams, each with an area of expertise. The first team focuses on the on-time requests, helping the RCMP meet its obligations under the Act. The second team specifically looks at the most dated backlog files in order to reduce the risk associated with these requests. A third team, made up of highly experienced analysts, is responsible for addressing the most sensitive investigations which may require extensive consultations or unique knowledge in order to process. The fourth team is responsible for reviewing and responding to complaints received through the Office of the Information Commissioner (OIC).

The Access Stream also leads the overall coordination of the proactive publication requirements of Part 2 of the ATIA for the RCMP and works collaboratively with stakeholders to monitor and ensure compliance. This Stream also works closely with partners in Communications, Parliamentary Affairs, the Commissioner's Office and the Minister's Office to ensure horizontal visibility on ongoing trends, including issues with implications to the department, public sentiment, and strategic planning with the view of sharing a common understanding of organizational priorities, and informing existing, or anticipated ATIP requests.

Privacy Stream

Led by a Director, the Privacy Stream is made up of two units—one responsible for processing formal personal information requests and the other supports compliance of the RCMP's program delivery with the provisions of the *Privacy Act* and the policies and directives of the Treasury Board of Canada Secretariat (TBS).

Privacy Disclosure Unit

This unit processes all formal requests received under the PA. This stream is made up of four disclosure teams, each with an area of expertise. The first two teams focus on the on-time requests, helping the RCMP meet its obligations under the *Privacy Act*. The third team specifically looks at the most dated backlog files to reduce the risk associated with these requests. The fourth team is responsible for reviewing and responding to complaints received through the Office of the Privacy Commissioner (OPC).

Privacy Management Division (PMD)

The Privacy Management Division is divided into three interrelated but distinct teams: Compliance and Advisory Services, Privacy Policy and Transparency, and Incident Management and Permissible Disclosures. These dedicated professionals provide policy advice and expertise to the RCMP on privacy-related issues, including: assessing risks and recommending mitigating measures during program development and modernization; supporting the drafting, review and approval of Privacy Impact Assessments (PIAs) and Privacy Impact Assessment Questionnaires (PIAQs); reviewing RCMP agreements and contracts (for example, Memorandums of Understanding, Information Sharing Agreements, Requests for Proposal); managing privacy breach reporting, complaints under sections 4 through 8 of the PA, and the informal review of requests under subsection 8(2) of the PA. In addition, the team provides awareness sessions and reviews and creates internal policies that reflect TBS policy, directives and guidance, as well as expectations from the OPC. The team works to ensure the RCMP is meeting its obligations as described in section 4.2 of TBS's Policy on Privacy Protection and the PA.

Operational Support Stream

Led by a Director, the Operational Support Stream oversees the preliminary phases of a request, provides internal reporting services and digitization of its processes. It consists of two teams: Lead Operations and Innovative Solutions. The Lead Operations team concentrates on the opening, triaging, tasking and importing of all incoming requests. Meanwhile, the Innovative Solutions team is tasked with creating robotic processes (bots) that automate repetitive tasks, thereby enhancing efficiency and optimizing workflows. Additionally, they play a vital role in the management and maintenance of the ATIP case management software and in supporting ATIP operations within the RCMP. They ensure the accuracy of data, manage user access, and provide statistical reports to bolster ATIP operations. The team also includes the Centre of

Excellence for all rich media requests, including those from the Body Worn Camera (BWC) initiative and BWC footage contained in operational files.

When tasking requests, the Lead Operations team works closely with divisional Liaison Officers (LOs) and record holders, known as the Office of Primary Interest (OPIs). Some responsibilities of the LOs and OPIs include:

Liaison Officers

LOs are responsible for forwarding all requests to the appropriate personnel (i.e. OPIs) within their business lines or divisions. Other responsibilities include tracking submissions to ensure responsive records are sent by OPIs to the ATIP Branch; ensuring responses are on time; and documenting and communicating internal RCMP ATIP processes to all who facilitate the processing of requests. In 2022, the RCMP Contract Management Committee was consulted on an initial pilot to expand its ATIP footprint in the divisions. At that time, National Head Quarters transferred funds to five divisions to support limited capacity to serve as a proof of concept and identify challenges. The initial results of this pilot have been extremely successful, with divisions reporting increased visibility and carriage of ATIP requests moving through the divisions. Due to conflicting priorities and increasing demands, as well as a of lack of funding, the pilot couldn't continue past the first year.

Office of Primary Interest

As the record holders, some of the OPIs' responsibilities include providing electronic copies of the responsive records; reviewing records for duplication; ensuring that the information falls within the scope of the request; notifying the ATIP Branch if records are voluminous; and advising the Branch or LO if an extension is required.

Delegation order

The Minister of Public Safety is responsible for administering requests made to the RCMP under both the *Access to Information Act* and the *Privacy Act*. In accordance with section 95(1) of the ATIA, the Minister delegates authority to departmental senior management, including the ATIP Coordinator, to carry out the Minister's powers, duties and functions under the Act in relation to formal requests. A copy of the signed Delegation Order is included in [Appendix A](#). Of note, this Delegation Order is currently being updated to reflect the current operating structure of both the ATIP Branch and the RCMP as a whole.

Performance for 2024-2025

This section provides an overview of the RCMP's performance with respect to records requested under the ATIA for the 2024-2025 reporting year.

During the 2024-2025 reporting period, the ATIP Branch remained operational and continued to work closely with its partners and stakeholders in finding solutions and reviewing processes to ensure that it responded to Canadians' requests in a satisfactory and timely manner. However, it continued to face challenges that resulted in response delays to requests submitted. Despite its legislative responsibilities, certain realities prevented the RCMP from responding on time, including:

- Operational requirements that called for RCMP members and employees to be redeployed on an urgent basis. This includes the National Wildfire response, police assistance at protest activities and security for major events and visits, to name a few.
- The RCMP still relies heavily on paper-based processes with many records that have not been digitized.
- The extensive search for records often required (more than 750 locations throughout Canada).
- The switch from the Immigration, Refugee and Citizenship Canada (IRCC) ATIP portal to the TBS portal in March 2023 continues to obligate the RCMP to seek clarification from the vast majority of requesters for information that was previously mandatory on the IRCC portal.
- Significant recruitment, training, awareness and retention efforts in the ATIP Branch continued in light of the lack of experienced ATIP analysts in the wider ATIP community. The Branch is working diligently to develop new analysts through a Professional Development Program, and these efforts will show results in the years to come.

The RCMP recognizes the importance of complying with legislated timelines and continues to overhaul its program and address these issues by:

- devoting resources to improve the timeliness of responses
- modernizing/streamlining policies and procedures within the program and across the organization to enhance operational efficiency
- expanding training and awareness campaigns for all RCMP personnel to ensure they understand the obligation to respond within legislated timeframes
- investing in new technologies and automation to increase efficiencies and decrease the total workload

Compliance and pages processed

In alignment with the Treasury Board Secretariat's (TBS) performance target of closing 90% of access requests within the legislated timelines, the ATIP Branch saw an increase in compliance for the number of access requests closed within the legislated time frame. In the 2024-2025 reporting period, compliance rose to 43% from 35% in the previous fiscal year.

The ATIP Branch's level of output for the number of pages processed under the ATIA during the 2024-2025 fiscal year remained constant, increasing by only 2.4% compared to the 2023-2024 fiscal year. It is interesting to note that while the number of pages remained consistent, the number of requests processed decreased by 34%. The decrease in the number of requests processed can be explained by multiple initiatives throughout the Branch such as improved triaging to distinguish genuine access to information requests from privacy-related ones at the point of intake; redirecting requests outside of the ATIP process where appropriate; diligently narrowing the scope of requests through effective triage allowing for more targeted reviews and better service to Canadians; and the automation of processes like deduplication bots.

Table 1: Compliance

Fiscal year	Compliance	Pages processed	Requests closed
2024-2025	43%	1,663,359	4,191
2023-2024	35%	1,624,587	6,374
2022-2023	42%	941,259	5,633
2021-2022	40%	1,006,354	5,085

Requests received and closed

The RCMP received a total of 2,223 new requests under the ATIA in 2024-2025. In addition, there were 3,336 requests outstanding from the previous reporting periods for a total of 5,559 requests. Of these, 4,191 requests were completed and 1,368 requests were carried over to the 2025-2026 fiscal year. Of the completed requests, 7.8% were fully disclosed and 50.1% were partially disclosed.

Generally, access requests cover a variety of topics and can include information about contracts/program costs and expenses; information related to security issues; operational file material; and the management of the RCMP. Of note, approximately 80% of the ATIA requests processed were related to matters of a personal nature.

In the 2024-2025 reporting period, the RCMP received 2,225 ATIA request, a significant decrease compared to the previous reporting periods: 5,510 in 2023 and 3,658 in 2023-2024. The decrease is a direct result of the Branch's efforts to educate requesters, including adding guidance to the TBS portal advising requesters to use the PA to request their own personal information. This has benefited requesters as the PA requests can be made free of charge, provide them with an expanded right of access, and grants requesters the right to correction, none of which exists under the ATIA. The decrease here is matched to an increase in requests made under the PA.

1156

Active requests from previous reporting periods

The significant work done to eliminate the backlog of requests can be seen in the numbers below. The legacy backlog has been reduced by approximately 30%, from 6.4 million pages to 4.6 million pages over the reporting period. The ATIP Branch made a significant effort to process and close all backlog files received prior to April 1, 2020. At the end of the reporting period 11 files remained open. At the time of this report, eight of those requests have already been closed, and the last three are nearly complete. As such, there will no longer be any decade-old files in the backlog. While there is still a backlog of requests to process, they are more recent, demonstrating the efforts made to improve the service the RCMP is providing to the public. At the conclusion of the 2024-2025 fiscal year, a total of 1,367 requests were outstanding which is a decrease of 44.9% compared to the previous reporting period. Of those outstanding, 15% were carried over within legislated timelines, and 85% were carried over beyond legislated timelines.

As shown in Table 2, at the end of the reporting period, the RCMP had 1,367 open requests from previous reporting periods. One third of the outstanding requests (32%) were received within the last two years.

Table 2: Active requests from previous reporting periods

Fiscal year open ATIA requests were received	Open requests that are within legislated timelines as of March 31, 2025	Open requests that are beyond legislated timelines as of March 31, 2025	Total
2024-2025	209	147	356
2023-2024	0	228	228
2022-2023	0	223	223
2021-2022	0	381	381
2020-2021	0	168	168
2019-2020	0	8	8
2018-2019	0	1	1
2017-2018	0	2	2
Total	209	1,158	1,367

Completion time

The ATIP Branch was able to complete a total of 953 (22.7%) requests in 30 days or less. During the reporting period, 848 (20.2%) requests were completed within 31 to 60 days, 356 (8.4%) were completed in 61 to 120 days and 2,034 (48.5%) were completed in more than 121 days. The noteworthy number of requests closed in more than 121 days can be attributed to the significant effort undertaken to close the most dated requests.

Table 3: Completion time for closed ATIA requests

Completion time	Number of requests closed	Percentage of requests closed
1 to 30 Days	953	22.7%
31 to 60 Days>	848	20.2%
61 to 120 Days	356	8.4%
121 to 180 Days	161	3.8%
181 to 365 Days	326>	7.7%
More than 365 Days	1,547	36.9%
Total	4,191	100%

Extensions

Section 9 of the ATIA allows institutions to extend the statutory time limits to respond to a request beyond 30 days.

For the requests closed during the 2024-2025 reporting period, the RCMP sought a total of 3,165 extensions under section 9(1)(a), which pertains to unreasonable interference with operations.

A total of 22 extensions under section 9(1)(b), which pertains to necessary consultations were taken.

One extension under section 9(1)(c) were taken for third-party consultation.

While the RCMP makes every effort to avoid extensions, the unique operational reality of the organization sometimes requires additional time to process requests. For example, during the wildfire season in British Columbia and Alberta, several detachments were structurally impacted at various levels, others had to close, and many were on Evacuation Alert. Extensions were therefore sought for requests in these affected areas.

Consultations for other institutions

During the reporting period, the RCMP completed 270 consultations, totalling 43,579 pages reviewed. Of the 270 completed consultations, 227 were received from other Government of Canada (GC) institutions and 43 were from other organizations. Of those, 112 (41%) consultations from GC institutions were completed within 30 days, and 29 (67%) consultations from other organizations were completed within 30 days.

The number of consultations received dropped by 24% this reporting period. More importantly, the number of pages received rose by 114% from the previous reporting period. The RCMP maintains a balanced

focus on consultations as a service to the ATIP community, consistent with the expectations of the OIC, ensuring they are not used to artificially prolong the processing time of requests.

Table 4: Completion times for consultation requests

Completion times	Number of requests
1 to 15 days	59
16 to 30 days	82
31 to 60 days	57
61 to 120 days	35
121 to 180 days	18
181 to 365 days	10
More than 365 days	9
Total	270

Active outstanding complaints from previous reporting periods

At the conclusion of the reporting period, a total of 196 complaints were outstanding. Table 5 shows the number of outstanding complaints by the fiscal year received.

Table 5: Active complaints from previous reporting periods

Reporting period	Number of complaints
Received in 2024-2025	104
Received in 2023-2024	37
Received in 2022-2023	27
Received in 2021-2022	17
Received in 2020-2021	3
Received in 2019-2020	7
Received in 2018-2019	0
Received in 2017-2018	0
Received in 2016-2017	0
Received in 2015-2016 or earlier	1
Total	196

Training and awareness

Continuous learning is a priority for the RCMP and the ATIP Branch is no exception. ATIP Branch staff are encouraged to seek out relevant courses and other learning opportunities to enhance their knowledge and to improve their skills.

In the 2024-2025 reporting period, the ATIP Branch instituted internal and information training curriculum called "A Slice of Learning." These monthly sessions provide an opportunity for all employees to learn about the inner workings of the Branch, along with a variety of topics intended to assist in their daily work. Topics this year included ATIP statistical reporting, how to prepare to be an affiant, summaries of the Canadian Access and Privacy Association (CAPA) and Canadian Bar Association (CBA) ATIP conferences, responding to complaints, data detox, and occupational health and safety.

The ATIP Branch had the opportunity to meet with the senior management of F Division (Saskatchewan) and Depot Division to speak about ATIP and the legal obligations of all employees to comply with the Acts. In person sessions such as this are invaluable as they provide a chance for both sides to ask questions and address issues unique to the Division. This visit also allowed for the ATIP Branch to meet with the curriculum development team for Depot and opened the conversation for updating the training received by all in-coming police officers. These updates will be developed over the next reporting period and are a key piece in the ATIP Branch's modernization efforts and in line with TBS guidance.

Ad-hoc training continued throughout the year with a total of nine sessions being delivered to 599 employees across the country. A highlight of these presentations was the E Division (British Columbia) Information Governance Days of Summer Sessions. Led by the E Division Information Governance group, this two-week program was open to all employees in the Division and touched on a wide variety of topics that affect information management and governance. As the biggest Division, and utilizing unique records management systems, the ATIP Branch relies on the expertise within the Division to ensure we can respond to requests in a timely manner. Other sessions included employees from Federal Policing, Corporate Reporting and Governance, Strategic Policy, and the Information Professionals Summit in Ottawa led by the RCMP for employees currently working in information management and governance.

Since joining the Digital Program in May 2023, the ATIP Branch has been incorporated into the student outreach program which liaises with post-secondary institutions to connect students to co-op placements and post-secondary recruitment. Three sessions were held this year in the National Capital Region, reaching students across the city with an interest in law enforcement and data.

The RCMP's *Access to Information and Privacy Fundamentals* online course is available to all RCMP employees through the organizations' online learning platform. In addition to increasing their knowledge of the ATIA

and the PA, this course also provides employees with a better understanding of their responsibilities when responding to information requests and best practices when managing personal information. In 2024-2025, 886 RCMP employees successfully completed the course.

Policies, guidelines and procedures

Throughout this reporting period, the ATIP Branch continued to modernize and update internal policies and procedures to ensure alignment with current reporting standards. These changes will continue to be developed and instituted in the 2025-2026 reporting period.

ATIP Modernization

In November 2020, the OIC released the results of a systemic investigation of the RCMP's ATIP program entitled *Access at issue: The need for leadership*. The report was highly critical of the RCMP's ATIP program and identified 15 recommendations for improvement. Subsequently, the Minister of Public Safety issued a Directive to the RCMP to action the recommendations of the OIC's review and submit a strategy outlining a way forward to be developed in consultation with TBS. In response, the RCMP developed a strategy entitled *Access Granted: Restoring Trust in the RCMP's Access to Information Program*, supported by an action plan outlining initiatives to modernize the program.

The RCMP began implementation of the strategy in the 2021-2022 reporting period and is committed to seeing it through over the course of a five-year period. Since then, the RCMP ATIP Branch undertook advancements in human resources, technology, policy and procedures. The objective being to increase compliance rates and enhance public transparency. The RCMP posted the strategy and is providing updates on the RCMP external website. We encourage all Canadians to visit the site and monitor our progress at <https://rcmp.ca/en/corporate-information/access-information-and-privacy/access-granted-restoring-trust-rcmp-access-information-and-privacy-program>.

Over the reporting period, the RCMP continued to make progress in implementing the strategy. While more details can be found on our external website, some key initiatives include:

Pillar One: Our People

To improve the internal services provided to the organization, the Privacy Management Division has been strengthened to ensure the RCMP is able to provide expert services in privacy policy and the management of personal information to all areas of the organization.

The Operations Stream has been bolstered to include system administrators who are responsible for the technical support of the ATIP case management software and analytics positions to interpret data and assist with long-term planning and process improvements.

The ATIP Branch strengthened its commitment to diversity and inclusion by partnering with LiveWorkPlay, a non-profit organization that supports neurodivergent talent, enabling the recruitment of individuals whose unique perspectives and skills enhance the organization's innovation, resilience, and inclusive culture. The ATIP Branch currently employs four individuals from LiveWorkPlay in a variety of roles throughout the Branch. As a result, the RCMP was awarded the LiveWorkPlay Inclusive Employer award for 2024-2025. Talks are underway to expand the program to other areas of the RCMP.

The Professional Developmental Program has begun to show successes. The first candidates have been assessed and are being promoted via the program criteria. This program is essential for the ATIP Branch to train and retain new analysts by demonstrating a career path and growth opportunities within the program and the RCMP.

Pillar Two: Our Tools

The RCMP worked closely with TBS on updates to the ATIP Online Request Portal. These updates, outlining required information in order to submit a request, have resulted in a savings of approximately \$80,000 since October 23, 2024. More than 1,000 incomplete requests have been closed immediately following opening, resulting in a reduction in work to task and review records where no consent or proper identification has been provided.

As the RCMP deploys BWC across the country to front-line officers, ATIP Branch has expanded its capabilities to review these new records along with other rich media formats. The deployment of video vetting software has allowed the RCMP to release more video than ever before as the tools to process it have been improved. Preliminary analysis indicates that processing BWC video files requires significantly more time than initially anticipated. As data remains limited, the full impact of BWC-related requests is not yet clear. The Branch will continue to monitor developments closely and adjust its strategy and resource planning as more accurate information becomes available.

Three automation processes (RPA) have been put into production within the ATIP Branch. The first bot addresses duplicate records. Eligible records are now deduplicated prior to being uploaded to our case management software. In the first four months of use, 18,000 pages of duplicates were located and removed. This has reduced analyst workload

and workloads for our OPIs on consultations since they are not looking through duplicate records. Two more bots have just come online and their effectiveness is currently being monitored.

The case management software used by RCMP ATIP Branch is at the end of its life and will no longer be supported after June 30, 2026. All institutions currently using this outdated software are now required to prioritize the modernization of their case management systems, begin onboarding a new platform by June 2025, and complete the full transition by June 2026. TBS has approved two new ATIP software solutions, both of which have been evaluated against criteria established by the ATIP community and meet all mandatory requirements. The current legacy system is obsolete, and its failure could lead to information loss and significantly disrupt or delay the processing of ATIP files. However, funding sources for the replacement and modernization of the existing system have yet to be identified and secured.

Pillar Three: Our Procedures

The Branch collaborated with the Canadian Firearms Program (CFP) to redirect information requests for firearms information that can be better addressed directly.

Website and client portal updates were implemented to guide clients on accessing information without submitting a formal ATIP request. These efforts led to a 24% reduction in ATIP taskings to the Specialized Police Service business line during this reporting period.

The Triage Team established a few years ago has made great strides. Over the last two years, employee retention and training on this team has allowed for these analysts to grow, and their work can be seen in the reduction of pages processed. This team regularly speaks with applicants to assist with properly scoping requests, understanding RCMP jargon and ensuring requests are completed prior to any tasking or review being done. This has reduced the workload both within the ATIP Branch but also with the OPIs who have clearer direction on what is being requested.

High-quality data is critical for enabling informed, data-driven decisions; identifying trends; and effectively managing workloads within the ATIP Branch. It also ensures accurate reporting to the Chief Digital Officer and RCMP senior management. To improve data integrity, three targeted training sessions on data entry and reporting standards were delivered early in the reporting period. As a result, data accuracy improved significantly—from 69% in November 2024 to 94% by February 2025.

The drafting of standard operating procedures (SOPs) remained a priority in this reporting period. To facilitate training and ensure consistency, SOPs have been drafted to address digital evidence, active police

investigations, and how to treat records related to investigative techniques and obscene material.

To support business continuity and the shortcomings of the current case management software, ATIP collaborated with IT to ensure a full backup of the database is in place should anything happen. As seen in other institutions, the volatility of the database is a key concern and is a leading factor in the evaluation of new software solutions.

As the original 5-year modernization strategy is set to conclude in the next reporting period, the ATIP Branch is looking to the future and how to continue building on the successes seen in the last four years. The four strategic priorities that the Branch will be focusing on are:

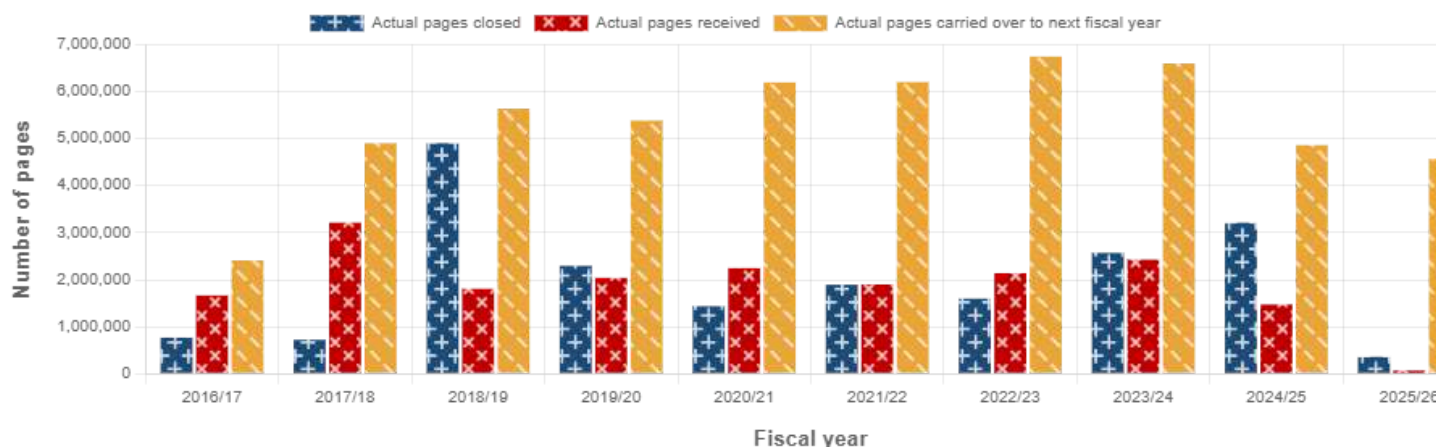
1. Clearing the legacy backlog
2. Disclosure oversight and improved compliance
3. Advancing modernisation initiatives
4. Providing robust privacy support services to the RCMP

Tackling the Legacy Backlog: A Strategic Success

To address the legacy backlog by 2029, the Branch adopted a targeted strategy: temporarily leveraging experienced and high-performing consultants to accelerate file processing. This approach is already delivering strong results—nearly 30% of the legacy backlog was cleared in 2024-2025, with the volume reduced from 6.4 million to 4.6 million pages over the fiscal year. Notably, the Branch successfully closed almost all backlog files received prior to March 1, 2020.

This progress allows indeterminate staff to focus on current and incoming requests, improving overall responsiveness and efficiency.

Chart 1: Backlog Accumulation and Reduction



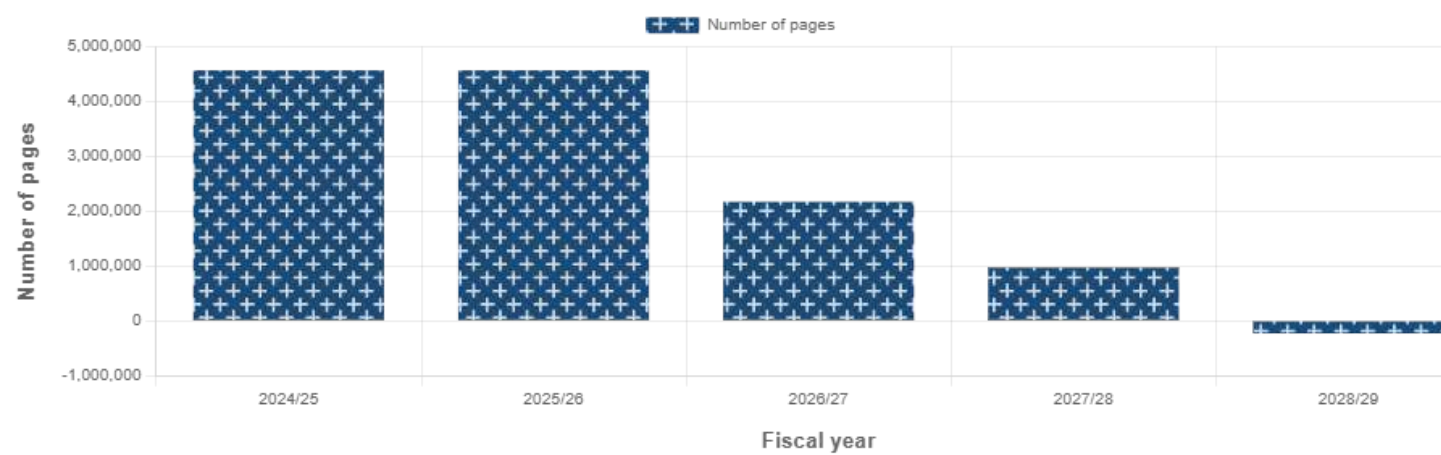
▼ Text version

Backlog accumulation and reduction

Fiscal year	Actual pages closed	Actual pages received	Actual pages carried over to next fiscal year
2016-2017	763,408	1,661,212	2,409,588
2017-2018	717,231	3,211,234	4,903,591
2018-2019	4,903,591	1,802,968	5,639,832
2019-2020	2,291,749	2,036,597	5,384,680
2020-2021	1,432,605	2,243,925	6,196,000
2021-2022	1,889,469	1,896,731	6,203,262
2022-2023	1,593,479	2,136,774	6,746,557
2023-2024	2,568,134	2,424,489	6,602,912
2024-2025	3,210,836	1,469,154	4,861,230
2025-2026	355,380	63,462	4,569,312

Based on current processing capacity, the ATIP Branch anticipates resolving the legacy backlog—comprised of outstanding files from 2020 to 2025—by the 2028-2029 fiscal year, as outlined in Table 7.

Chart 2: End-of-year backlog reduction



▼ Text version

End-of-year backlog reduction

Fiscal year	Number of pages
2024-2025	4,569,312
2025-2026	4,569,312
2026-2027	2,169,312
2027-2028	969,312
2028-2029	-230,688

Closing the Production Gap: A Sustainable Strategy for Timely Information Disclosure

To prevent the creation of a new and compounding backlog, the Branch is implementing a comprehensive and forward-looking strategy to close its annual production gap and ensure timely responses to ATIP requests. The Branch receives approximately two million pages for review each year, while Branch employees currently process 1.2 million pages, resulting in a growing shortfall of 800,000 pages annually. To eliminate this gap and align capacity with demand, the Branch has already started to implement the following three key measures and will continue to do so in the next fiscal year:

Boost Analyst Productivity (+20% workload reduction)

As most ATIP analysts are still early in their careers, there is strong potential for growth. With continued training and experience, productivity is expected to increase by 20%, enabling analysts to process more files efficiently as they deepen their understanding of the ATIP legislation.

Reduce Page Volume Through Triage and Negotiation (-15% workload reduction)

By equipping analysts with negotiation skills and focusing on early triage, the Branch aims to reduce the volume of pages requiring review by approximately 300,000 pages. This will be achieved by working with requesters to narrow the scope of their requests to only the most relevant information.

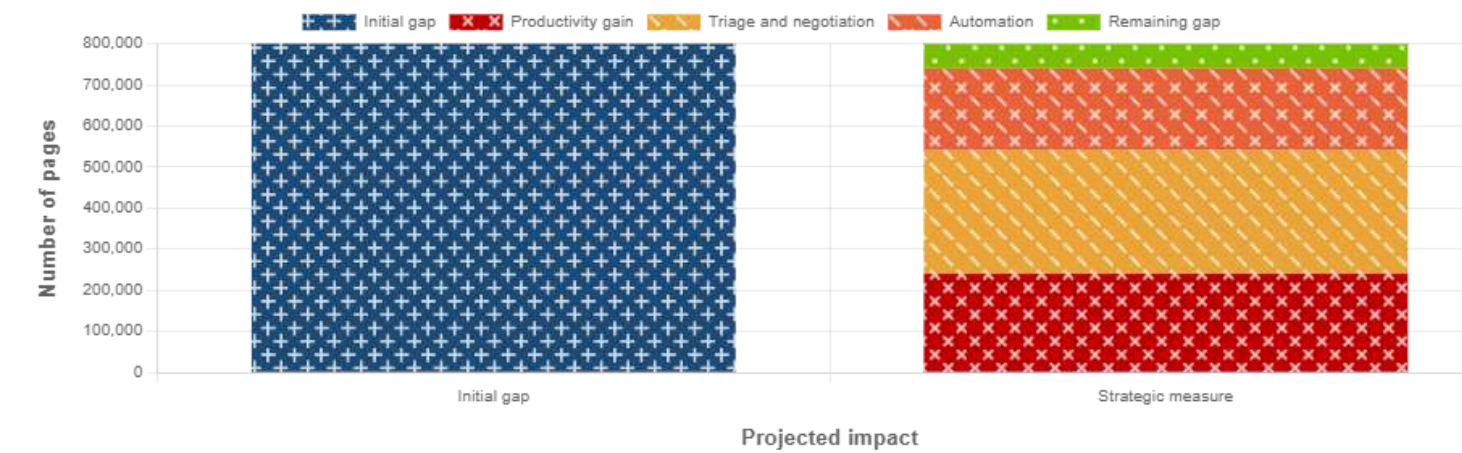
Leverage Automation to Increase Speed and Reduce Workload (-10% workload reduction)

rollout of automation tools is expected to both accelerate processing and reduce manual workload by an estimated 200,000 pages, allowing analysts to focus on more complex tasks.

Together, these measures are projected to bring the number of pages received and processed into balance, effectively eliminating the production gap and preventing the creation of a new backlog. This will ensure that the majority, if not all, of the information requested can be reviewed and disclosed within the same fiscal year, significantly improving service to Canadians.

This chart breaks down how each of the three key measures—productivity boost, triage/negotiation, and automation—contributes to closing the 800,000 page gap.

Chart 3: Projected impact of strategic measures on page processing



▼ Text version

Projected impact of strategic measures

Strategic measure	Number of pages
Productivity gain	240,000
Triage and negotiation	300,000
Initial gap	800,000

Strategic measure	Number of pages
Automation	200,000
Remaining gap	60,000
Initial gap	800,000

Providing Robust Privacy Support Services to the RCMP

Trust is earned in bytes—and lost in breaches. As such, strong privacy practices are the foundation for protecting Canadians' data and preserving their trust in public institutions.

In today's digital landscape, data protection is reputation protection. High-profile privacy breaches—such as those experienced by Desjardins, Equifax, and Capital One—have shown how the mishandling of personal information can lead to devastating financial losses, legal consequences, and irreparable damage to public trust.

To prevent similar outcomes, the RCMP's Privacy Management Division plays a vital role in supporting the organization through escalating data privacy challenges. The Branch acts as a privacy shield, helping to ensure that the personal information of Canadians is collected, used, retained, and disclosed in full compliance with the *Privacy Act*.

The class action lawsuits involving Desjardins, Equifax and Capital One resulted in settlements in the hundreds of millions of dollars and effected millions of individuals. While some of the more severe examples, these cases underscore the financial and reputational risks of inadequate privacy safeguards. Beyond financial and legal costs, breaches erode public confidence and invite increased scrutiny from the media, Parliament and global regulators enforcing stricter data protection laws.

The ATIP Privacy Management Division provides expert guidance and oversight to ensure that all RCMP programs, technologies, and operations meet privacy obligations, thereby increasing Canadians' trust in the RCMP. Key contributions include:

Enabling Legal Compliance and Risk Mitigation

Conducting Privacy Impact Assessments (PIAs) to ensure lawful handling of personal data.

Preventing high-risk initiatives such as what was seen with the use of Clearview AI and negating the risk of being summoned before Parliament, as seen with On-Device Investigative Tools.

Supporting Modernization and Transparency

Contributing to the National Technology Onboarding Process (NTOP) to assess privacy risks in emerging technologies.

Updating ATIP policies to reflect recommendations from the Mass Casualty Commission (MCC).

Managing Info Source and Personal Information Banks to promote transparency.

Navigating Emerging Threats

Helping the RCMP navigate the complexities of artificial intelligence (AI), cybersecurity, and evolving digital threats.

Facilitating the lawful disclosure of personal information while protecting individual rights.

By embedding privacy into every layer of its operations, the RCMP is not only protecting sensitive information, but also building public trust; reducing institutional risk; and reinforcing its commitment to transparency and accountability.

Initiatives and projects to improve access to information

Informal requests

As part of the proactive publication requirements set out in Part 2 of the ATIA, the RCMP posts a summary of the completed 'true ATI' requests to Open Government. This distinction is important since 80% of all requests received by the RCMP under the ATIA have historically been for the personal information of the applicant. These requests are not posted to Open Government to protect the privacy of the individuals making the requests.

In this reporting period, 864 request summaries were posted. In response, 3,000 informal requests were made via the online portal. The ATIP Branch is exploring options to proactively publish information that is frequently requested; however, these efforts have been hampered by language requirements and the translation efforts required which would flood the Translation Bureau.

Program support

As part of the broad modernization efforts over the previous four years, the ATIP Branch has developed relationships with countless stakeholders across the RCMP, and the impacts of these connections can be felt across the organization.

As Canada and the RCMP prepared for the G7 meetings in Kananaskis, Alberta in June 2025, the ATIP Branch played a key role in the planning stages of file management. Security was a shared responsibility across various levels of government, with the RCMP as the lead organization. Collaboration has been key to ensure that each organization is treating

information in a consistent manner and ensuring appropriate information is proactively disclosed in support of the Summit. This has also resulted in a streamlined process for tasking and reviewing of formal requests.

The Public Inquiry into Foreign Interference was established to examine and assess the interference by China, Russia and other foreign states and non-state actors - including any potential impacts - in order to confirm the integrity of, and any impact on, the 43rd and 44th general elections at the national and electoral district levels. As part of the disclosure requirements of the Inquiry, the ATIP Branch worked closely with the record owners - Civil Litigation and other key stakeholders - to gather, review and disclose material to both the Inquiry and via the formal ATIP process.

The ATIP Branch played a lead role in the RCMP's response to the Fourth Settlement Agreement with the LGBT Purge Fund. Stemming from a nation-wide class action against the Canadian Government, the Purge Fund fought for the disclosure of historical government records that demonstrated the systematic discrimination, harassment, and termination faced by LGBT members of the Canadian Armed Forces, the RCMP and the Federal Public Service. This 4th disclosure consisted of 15,000 pages of records, held by multiple institutions and outlined the policies and procedures that were in place that discriminated against queer employees. The ATIP Branch reviewed the RCMP records included in this disclosure and applied an 'ATIP-like' lens while considering the passage of time to release as much information as possible.

Contract policing is at the core of the RCMP's mandate. The RCMP operates as the provincial and territorial police in eight provinces, three territories and offers municipal policing services to 150 communities delivered through more than 700 detachments across Canada, 600 Indigenous communities and 3 international airports. Over this reporting period, the ATIP Branch has engaged with an internal transition team within the Reform, Accountability and Culture portfolio to work with communities who have moved from the RCMP to local police of jurisdictions. The transition in Surrey, British Columbia - for instance - has raised concerns over information management and access, and the ATIP Branch has played a role in addressing these concerns.

In line with the proactive publication guidelines, the RCMP regularly discloses information of interest to the public via the external webpage. The ATIP Branch regularly works with the RCMP's Audit and Evaluation Unit to conduct reviews with an ATIP-like lens on all audits/reports prior to their publication. Additionally, following a Ministerial Directive, the ATIP Branch continues to support the RCMP's Management Advisory

Board by conducting informal reviews prior to the publication of their recommendations which supports internal reform while remaining transparent with the public.

Summary of key issues and actions taken on complaints

Complaints and investigations

During this reporting period, the RCMP continued to work collaboratively with the OIC to address complaints as efficiently as possible. Following the publication of the OIC's systemic investigation in November 2020 into the RCMP and its ATIP practices, concrete steps were taken to review and update internal processes to help ensure the RCMP meets its obligations under the Act.

The OIC continues to receive record numbers of complaints from across government. As the OIC worked diligently to respond and investigate these complaints, departments and agencies had to respond to support the OIC investigative process and respond to the inquiries of the Agent of Parliament. The RCMP was no exception to this and had to respond accordingly to ensure that it was meeting its expectations.

As part of the modernization strategy, the ATIP Branch continued to utilize a dedicated team of ATIP personnel to serve as the primary point of contact for the OIC. The team is led by a manager responsible for coordinating complaints and assisting in complaint-related reporting to both the OIC, ATIP management and RCMP senior management. Regular monthly meetings are held between the OIC and the ATIP Branch to discuss file progression. These monthly meetings resulted in the resolution of more complaints and better collaboration with OIC and the ATIP Branch.

Since the Systemic Investigation in 2020, and the recommendations from the Modernization Action Plan have been implemented, significant improvement has been seen in the number of complaints received by the RCMP. In 2024-2025, the RCMP received 178 complaints - this is the lowest number of complaints received of the last six fiscal years.

Table 6: Complaints

Reporting period	Number of requests received	Number of complaints received	Percentage
2024-2025	2,223	178	8.0%
2023-2024	3,658	215	5.9%
2022-2023	5,510	479	8.6%
2021-2022	5,423	458	8.4%
2020-2021	5,314	275	5.2%

For the 2024-2025 reporting period, the RCMP received and provided the following under the ATIA:

Section 32

The RCMP received 178 notices of intent to investigate, which represents 8.0% of all requests received during the reporting period. The majority of the complaints received relate to delays where the RCMP was unable to respond within 30 days and therefore considered in deemed refusal in accordance with the Act. Under this section, the OIC formally notifies the institution of their intent to investigate a complaint received.

Section 30(5)

The RCMP received 120 notices. Under this section, if the OIC refuses or ceases to investigate a complaint, it notifies the complainant, the institution and, if applicable, any third party and the Privacy Commissioner.

Section 35

The RCMP provided 11 formal representations. Under this section, the OIC provides an opportunity to institutions to provide representation to an ongoing complaint investigation.

Section 36.1

The RCMP received 6 intent to order notifications. Under this section, the OIC may issue an order to the institution to release the requested information.

Section 37(1)

The RCMP received 4 initial reports. Under this section, the OIC finds that the complaint is well-founded and provides the institution the findings of their investigation, specific recommendations to remedy the issue, and when appropriate, a specific time frame that the OIC can expect a plan to implement the recommendations. The institution must then decide on whether to implement the recommendations.

Section 37(2)

85 final reports were issued during the reporting period. No reports contained recommendations, and 1 formal order was received from the OIC during this reporting period. In this case, the RCMP advised the OIC of our intent to comply with the Order and the records were released in compliance with the Order.

Court action

One court proceeding was actioned with respect to access requests processed within the 2024-2025 fiscal year, and none were discontinued/concluded or dismissed in this reporting period.

1172 Proactive publication under Part 2 of the ATIA

As part of the government's commitment to raising the bar for openness and transparency, Bill C-58 created Part 2 of the ATIA which put into law proactive disclosure practices previously only covered by federal policy.

The ATIP Branch works in collaboration with departmental officials to fulfill the proactive publication requirements found in Part 2 of the ATIA. Sections 74 to 78 and 82 to 88 of Part 2 of the Act, stipulate that government entities that support a minister are required to proactively publish travel expenses, hospitality expenses, reports tabled in Parliament, reclassification of positions, contracts, grants and contributions, briefing materials, and expense reports. Within the RCMP, this responsibility is led by the ATIP Branch in collaboration with other internal partners.

The RCMP is a government institution responsible for the publication of the following materials in accordance Sections 82 to 84 under Part 2 of the ATIA:

Table 7: Proactive publication requirements

Legislative requirement		Section	Publication timeline	Internal group(s) or positions(s) responsible for fulfilling requirement (if requirement applies to institution)	Percentage of proactive publication requirements published within legislated timelines	Publication location
Apply to all Government Institutions as defined in section 3 of the Access to Information Act	Travel Expenses	82	Within 30 days after the end of the month of reimbursement	Corporate Reporting	100%	Government Travel Expenses
	Hospitality Expenses	83	Within 30 days after the end of the month of reimbursement	Corporate Reporting	100%	Search Government Hospitality Expenses
	Reports tabled in Parliament	84	Within 30 days after tabling	National Communication Services	70%	Open Government Portal

Legislative requirement		Section	Publication timeline	Internal group(s) or positions(s) responsible for fulfilling requirement (if requirement applies to institution)	Percentage of proactive publication requirements published within legislated timelines	Publication location
Apply to government entities or Departments, agencies, and other bodies subject to the Act and listed in Schedules I, I.1, or II of the Financial Administration Act	Contracts over \$10,000	86	Q1-3: Within 30 days after the quarter Q4: Within 60 days after the quarter	Corporate Reporting	100%	Search Government Contracts over \$10,000
	Grants and contributions over \$25,000	87	Within 30 days after the quarter	Corporate Reporting	100%	Grants and Contributions
	Packages of briefing materials prepared for new or incoming deputy heads or equivalent	88(a)	Within 120 days after appointment	not applicable	not applicable	not applicable
	Titles and reference numbers of memoranda prepared for a deputy head or equivalent, that is received by their office	88(b)	Within 30 days after the end of the month received	ATIP Branch	100%	Briefing Note Titles and Numbers
	Packages of briefing materials prepared for a deputy head or equivalent's appearance before a committee of Parliament	88(c)	Within 120 days after appearance	Parliamentary Affairs	70%	Open Government Portal

Legislative requirement		Section	Publication timeline	Internal group(s) or positions(s) responsible for fulfilling requirement (if requirement applies to institution)	Percentage of proactive publication requirements published within legislated timelines	Publication location
Applies to government institutions that are departments named in Schedule I to the Financial Administration Act or portions of the core public administration named in Schedule IV to that Act (that is, government institutions for which Treasury Board is the employer)	Reclassification of positions	85	Within 30 days after the quarter	Chief Human Resources Officer	100%	Search Government Position Reclassifications

Monitoring compliance

The ATIP Branch frequently makes use of comprehensive reporting tools to monitor compliance and maintain accountability, as well as to identify process improvements.

Time taken to process Access to Information requests

The ATIP Branch monitors the time taken to process ATIA requests by retrieving statistics from the case management software on a daily, weekly, monthly and quarterly basis. These statistics provide information on the compliance rate, the number of files completed on time and those that are delayed, as well as complaints both received and closed. Performance Dashboards are also key tools to further identify trends and assist the ATIP Branch in strategically developing efficiencies. The Branch's management team reviews the weekly and monthly reports to manage workload and to determine any upcoming issues where processes could be improved. The reports and dashboards are provided to the RCMP's senior management in an effort to improve accountability.

The ATIP Branch continues to work on bolstering its data reporting function by onboarding new technology and processes. This new technology will enable the ATIP Branch to be more strategic and

transparent by automatically capturing pertinent data to assist with its planning and public reporting, as well as to identify areas where efficiencies may be found.

Appendix A - Delegation order

Access to Information Act and Privacy Act Delegation Order

The Minister of Public Safety and Emergency Preparedness, pursuant to section 73 of the *Access to Information Act* and of the *Privacy Act*, hereby designates the persons holding the position set out in the schedule hereto, or the persons occupying on an acting basis those positions, to exercise the powers and functions of the Minister as the head of a government institution, that is, the Royal Canadian Mounted Police, under the section of the Act set out in the Schedule opposite each position. This designation replaces and nullifies all such designations previously signed and dated by the Minister.

Table 8: Schedule

Position	<i>Privacy Act</i> and Regulations	<i>Access to Information Act</i> and Regulations
Commissioner of the RCMP	Full authority	Full authority
Chief, Strategic Policy and Planning Officer		
Departmental Access to Information and Privacy Coordinator		
Commanding Officers	Authority for 8(2)(j) and 8(2)(m)	Not applicable
Officer in Charge, Policy, Processing and External Relations	Full Authority except 8(2)(j) and 8(2)(m)	7, 8(1), 9, 11(2) to 11(6) (inclusive), 12(2) and all mandatory exemptions (13(1), 16(3), 19(1), 20(1) and 24(1)) and 6(1) and 8 of the Regulations
Manager, Processing and Triage		
Manager, Quality Control		
Non-Commissioned Officers and public servants in charge of ATIP unit		
Non-Commissioned Officers and public servants in charge of ATIP Branch (analysts)	14 and 15 for all records; 17(2)(b), 19 to 28 (inclusive) for all employee records as designated in InfoSource; For all other records requiring mandatory exemptions in their entirety (19(1), 22(2) and 26) of the Act; 9 and 11(2) of the Regulations	7, 8(1) and 12(2)(b) and all records exempted in their entirety by mandatory exemptions (13(1), 16(3), 19(1), 20(1) and 24(1)) of the Act; 6(1) and 8 of the Regulations

Signed, at the City of Ottawa, this 4 day of December, 2015

The Honourable Ralph Goodale, P.C. (Privy Council), M.P. (Member of Parliament)

Minister of Public Safety and Emergency Preparedness

Date modified:

2026-03-03

TAB 35



Mr. Kevin McLean <mcleansettlement@gmail.com>

Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

Mr. Kevin McLean <mcleansettlement@gmail.com>

Fri, Jun 26, 2026 at 2:48 AM

To: "Beaudoin, Tina (RCMP/GRC)" <tina.beaudoin@rcmp-grc.gc.ca>

Cc: "Larkin, Bryan (RCMP/GRC)" <Bryan.Larkin@rcmp-grc.gc.ca>, "Brisson, Stéphane (RCMP/GRC)" <Stephane.Brisson@rcmp-grc.gc.ca>, "Ball, Jeff (RCMP/GRC)" <Jeff.Ball@rcmp-grc.gc.ca>, "Duheme, Michael (RCMP/GRC)" <Michael.Duheme@rcmp-grc.gc.ca>, ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>, "mclean@searchandseizure.ca" <mclean@searchandseizure.ca>

Dear Ms. Beaudoin,

Thank you for your correspondence of June 25, 2026.

Before I can meaningfully address the clarification questions, I require confirmation of several procedural points arising from your June 16 and June 25 emails, as well as the internal comments document authored by Ms. Margarethe von Zur-Muehlen.

For accuracy of the record, could you please confirm the following:

1. **Which specific Office of Primary Interest (OPI)** was tasked with ATIA Request A-2026-00761 / F339.
2. **On what date** that OPI was tasked.
3. **How the file could be described as being “in the retrieval stage” on June 16** if the OPI subsequently indicated on June 25 that it required clarification before any search could be conducted.
4. The internal comments document states that the CPI Centre “does not have any records” responsive to the categories requested.
 - Was the CPI Centre the OPI that was tasked?
 - If so, could you clarify why a policy unit was tasked rather than the operational custodians of CPIC system metadata.
5. For completeness, could you confirm whether **Technical Operations** — specifically the CPIC Operations & Technical Services Unit or the CPIC Historical Data Unit under the command of **Acting Assistant Commissioner Richard Burchill** — was ever tasked with this request.

These points will allow me to provide any necessary clarifications in a manner aligned with the correct OPI's technical mandate.

Thank you for your attention.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Thu, Jun 25, 2026 at 2:25 PM Beaudoin, Tina (RCMP/GRC) <tina.beaudoin@rcmp-grc.gc.ca> wrote:

Good afternoon,

The Office of Primary Interest has requested additional clarifications regarding your request, which has consequently resulted in an unavoidable delay in its processing. We sincerely apologize for any inconvenience this may cause.

To assist us in processing your request, could you please provide a timeframe and identify the specific file numbers or subject matter of interest? Kindly note, it is not feasible to conduct a search across an entire database without further parameters.

Please find attached a list of comments and questions for your review. Additional details will help both the ATIP Office and RCMP personnel locate relevant records more efficiently.

Once again, I apologize for the delay and appreciate your cooperation. I am available for a telephone call if this is preferable for you.

Regards,

Tina Beaudoin

343-597-0681

From: Mr. Kevin McLean <mcleansettlement@gmail.com>

Sent: June 22, 2026 12:02 PM

To: Beaudoin, Tina (RCMP/GRC) <tina.beaudoin@rcmp-grc.gc.ca>; Larkin, Bryan (RCMP/GRC) <Bryan.Larkin@rcmp-grc.gc.ca>; Brisson, Stéphane (RCMP/GRC) <Stephane.Brisson@rcmp-grc.gc.ca>; Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>; Simpson, Melissa (RCMP/GRC) <Melissa.Simpson@rcmp-grc.gc.ca>; Duheme, Michael (RCMP/GRC) <Michael.Duheme@rcmp-grc.gc.ca>

Cc: mclean@searchandseizure.ca

Subject: Re: Access to Information Act request A-2026-00761 / F339, Your File N/A, Clarification Required

Subject: STATUS INQUIRY – ATIA Request A-2026-00761 / F339 – Statutory Default and Retrieval Status

Date: June 22, 2026

To: Ms. Tina Beaudoin Access to Information and Privacy Branch Royal Canadian Mounted Police tina.beaudoin@rcmp-grc.gc.ca

- Investigative Data Bank Audit Trails: A full, unredacted disclosure of all audit trails for Personal Information Bank RCMP PPU 005 encompassing the dates of September 22 to October 4, 2024. These records must include the specific User IDs, administrative clearance levels, and terminal identifiers for every transaction.

The CPI Centre does not have any records on this, nor any information on Personal Information Bank PPU 005.

al Mainframe Dumps: The raw, unadulterated "Hexadecimal Dumps" from the federal CPIC mainframe transaction logs specifically associated with the entry, modification, and clearance of the warrant **designated in the primary request.**

The CPI Centre does not have any records on this, nor any information on Hexadecimal Dumps. IT Branch might have a different answer or know what hexadecimal dumps are. We have audit logs but not what is being requested here. We have also asked for and have not been provided the primary request.

- Hardware and Terminal Metadata: The internal "Originating Agency Identifier" (ORI) mapping, corresponding MAC addresses, and associated hardware terminal IP addresses used for the specific data-entry sessions that generated the "Frankenstein" Information Package.

The CPI Centre does not have any information on Frankenstein Information Package.

- Inter-Agency Communication Logs: All internal records of communication (including but not limited to emails, internal memorandums, CPIC system messages, and IT troubleshooting tickets) between the RCMP CPIC Governance Authority and the Toronto Police Service (TPS) records management branch.

This lacks context or dates. Even though the CPI Centre does not have any information on this, the Third Party Rule would apply and without consent from TPS no communications would be able to be shared. Perhaps some of this information was provided in primary request, but without context we have no way to search.

- DF Flattening and Vector Analysis Reports: All technical documentation, system error logs, or automated alerts generated by the CPIC input gateway concerning vector text anomalies, OCR (Optical Character Recognition) interpretation failures, or "whitespace bugs" during the processing of judicial PDF instruments.

-

The CPI Centre does not have any records on this, nor any information on Vector Analysis Report. It is not clear what is being requested. We don't generate or track what is being requested.

- Offline Historical Search Results: The complete, unredacted results of the mandatory "Offline Search" conducted by technical specialists into the Investigative Data Bank archives to determine the historical chronology of transactions.

Again this is missing context, dates and agencies.

- System Governance Manuals: Current, unredacted versions of the CPIC Reference Manual, training directives, and the Memorandum of Understanding (MOU) with municipal partners specifically governing the "Matching Protocol" and the "Judicial Firewall."

The CPI Centre does not have any information on Matching Protocol and Judicial Firewall.

MOUs are primarily sourced from CPIC Policy and contain information on the System's capabilities to support investigations and information sharing for Canadian and foreign police and public safety agencies.

1182

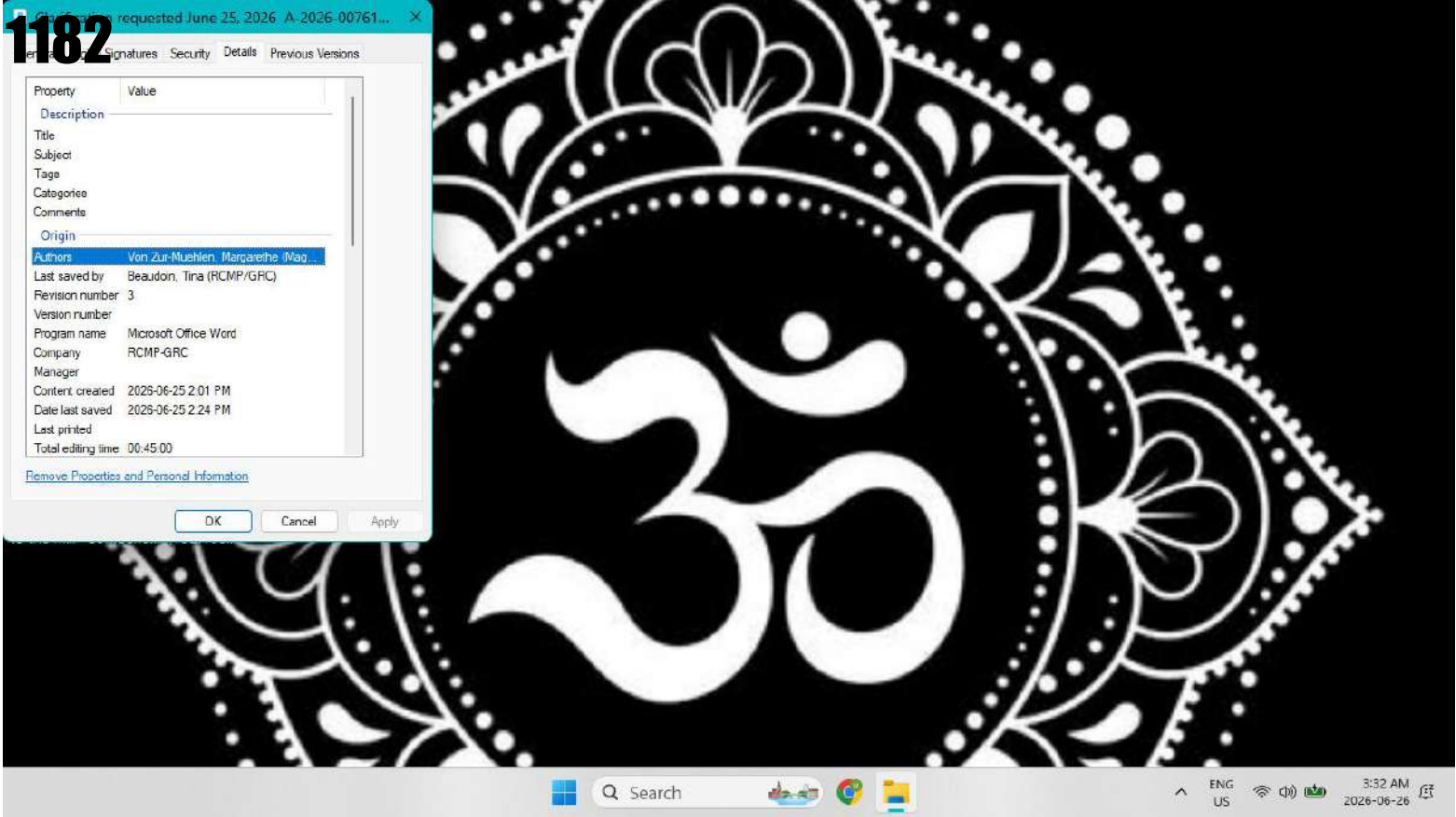
Properties requested June 25, 2026 A-2026-00761...

Signatures Security Details Previous Versions

Property	Value
Description	
Title	
Subject	
Tags	
Categories	
Comments	
Origin	
Authors	Von Zur-Muehlen, Margarethe (Mag...
Last saved by	Beaudon, Tina (RCMP/GRC)
Revision number	3
Version number	
Program name	Microsoft Office Word
Company	RCMP-GRC
Manager	
Content created	2025-06-25 2:01 PM
Date last saved	2025-06-25 2:24 PM
Last printed	
Total editing time	00:45:00

[Remove Properties and Personal Information](#)

OK Cancel Apply



Search



ENG
US



3:32 AM
2026-06-26



TAB 36

FEDERAL COURT

BETWEEN:

KEVIN ALEXANDER McLEAN

Applicant

– and –

ROYAL CANADIAN MOUNTED POLICE, COMMISSIONER MICHAEL DUHEME,
ATTORNEY GENERAL OF CANADA, and HIS MAJESTY THE KING IN RIGHT OF
CANADA

Respondents

DRAFT REASONS FOR ORDER/JUDGMENT FOR NOM #1, NOM #2 AND APPLICATION

(Schedule “A” Draft Order is at Appendix “A”)

Table of Contents

Draft Reasons for Order/Judgment for NOM #1, NOM #2 and Application..... 1

PART I — OVERVIEW AND SUMMARY OF ORDERS 8

 A. Overview 8

 B. Why These Matters Must Be Heard Together 9

 C. Summary of Findings 9

 D. Summary of Orders 10

 E. Roadmap or layout of the reasons for decision/order/judgment (partial or full) 10

Part II: Factual Background 11

 A. The Privacy Act and ATIA Requests 11

 B. The RCMP’s Refusal to Search CPIC Metadata 11

 C. The RCMP’s Refusal to Issue a Statutory Decision 12

 D. The RCMP’s Refusal to Consider s. 8(2)(m) of the Privacy Act 12

 E. The RCMP’s Refusal to Participate in These Proceedings 13

 F. The Missing Judicial Acta of the Superior Court of Justice 13

 G. Procedural History: NOM #1, NOM #2, and the Application 14

 H. Summary of the Evidentiary Record 16

PART III — ISSUES 16

 1. Are the RCMP’s duties under the Privacy Act and ATIA mandatory?..... 16

 2. Have those duties matured? 17

3. Has the RCMP refused to perform its mandatory duties?	17
4. Does the RCMP's silence constitute a functional attempt to shield itself from judicial review?	17
5. Do Charter values inform the interpretation of the Privacy Act, ATIA, and the common law?	17
6. Do the SCJ's missing judicial acta engage constitutional principles of judicial independence?	17
7. Does the RCMP's conduct impede access to justice and the Rule of Law?	17
8. Does the RCMP's silence, omission, and concealment constitute misrepresentation?	17
9. Can the RCMP cure its omissions by filing late evidence?	18
10. Are structural orders warranted?	18
11. Are full indemnity costs warranted?	18
12. Does the breadth of Rule 317 require expanded document transmittal where bias, natural justice breaches, or mandamus/prohibition are sought?	18
13. Does the open-court principle require that all transmitted materials under Rule 317/318 become part of the public court record?	18
14. Does the RCMP's failure to transmit a Certified Tribunal Record (CTR) constitute a breach of Rule 318 and a denial of natural justice?	19
15. Does the RCMP's misstatement of law regarding its inability to search "files belonging to other police forces" constitute a jurisdictional error?	19
16. Does the RCMP's failure to search unsearched repositories (including CPIC Offline Historical Database) invalidate its decision under the doCTRine of "failure to consider relevant evidence"?	19
17. Does the Associate Judge's Direction create a procedural impossibility, contempt risk, and conflict with Rule 318 requiring intervention by the Chief Justice / Acting Chief Justice?	19
PART IV — THE LAW	20
Section A — Mandatory Statutory Duties Under the Privacy Act and ATIA (Julius; Apotex; Steiner; MEI; Pathak; Douze)	20
1. Overview	20
2. The Julius Principle — "May" Can Mean "Must"	20
3. Apotex — Refusal to Act Is a Jurisdictional Error	21
4. Steiner — Public Duty Must Be Performed	21
5. Information Commissioner v. MEI — Silence Is Unlawful	21
6. Pathak and Douze — Relevance and the Duty to Search	22
7. The Duty to Decide — Statutory Timelines Are Mandatory	22
8. The Duty to Consider s. 8(2)(m) — Mandatory Public-Interest Override	23
9. Conclusion on Mandatory Duties	23
Section B — Maturity of Duty, Practical Utility, and the Mandamus Framework (East Gwillimbury; Oldman River; Apotex; Julius; Steiner)	23
1. Overview	23
2. Maturity of Duty — East Gwillimbury	24
3. Practical Utility — Oldman River	24
4. The Apotex Framework — Refusal to Act	25
5. Julius — Mandatory Duties Must Be Performed	26

6. Steiner — Public Duty Must Be Performed.....	26
7. Inadequate Alternative Remedy.....	26
8. The RCMP’s Refusal to Act Is Not Protected by Discretion	26
9. Conclusion on Maturity of Duty and Mandamus.....	27
Section C — Rule 317/318, Certified Tribunal Record, Open Court Principle, Forms, and Natural Justice (Pathak; Douze; Lill; Rémillard; Interpretation Act, s. 32; Bias; Mandamus; Prohibition).....	27
1. Overview	27
2. Rule 317 — Material in the Possession of the Tribunal.....	27
3. Rule 318 — Mandatory Transmission of the Certified Tribunal Record.....	28
4. Expanded Scope of Disclosure Where Bias or Natural Justice Breaches Are Alleged.....	28
5. Open Court Principle — All Transmitted Material Becomes Part of the Public Record.....	29
6. Interpretation Act, s. 32 — Deviations in Form Do Not Invalidate Filings.....	30
7. Misstatement of Law — Vires Error.....	30
8. Failure to Search Unsearched Repositories — Unreasonable and Unlawful.....	31
9. Failure to Transmit the CTR — Natural Justice Breach.....	32
10. Conclusion on Rule 317/318, Forms, and Natural Justice	32
Section D — Vavilov, Statutory Limits, Ultra Vires Conduct, and the Modern Reasonableness Framework (Vavilov; Daly; Dunsmuir; Pathak; MEI; Ministerial/Executory Duties)	33
1. Overview	33
2. Vavilov Eliminated “Jurisdiction” as a Category — Not Jurisdictional Limits.....	33
3. Ultra Vires Conduct Under Vavilov	34
4. The “Reasons First” Methodology.....	34
5. Misstatement of Law — Unreasonable Under Vavilov	35
6. Failure to Discharge Mandatory Ministerial and Executory Duties	36
7. Silence as Unreasonable Conduct	36
8. Institutional Bad Faith and Unreasonableness	36
9. Conclusion on Vavilov, Ultra Vires Conduct, and Reasonableness	37
Section E — Judicial Independence, Administrative Independence, Missing Judicial Acta, and Constitutional Integrity of Court Records (Beauregard; Siwicki; Dugré (FC & FCA); Swaine; Faber; Q.H.T.; Reilly; Open Court Principle; Rule of Law)	37
1. Overview	37
2. Judicial Independence Includes Administrative Independence.....	37
3. Missing Judicial Acta Engage Constitutional Principles	38
4. The Chief Justice as Constitutional Steward of Court Records	39
5. The Open-Court Principle Requires Complete Judicial Records.....	39
6. The Rule of Law Requires Integrity of Judicial Records.....	39
7. Vavilov and Administrative Failures Affecting Judicial Records	40
8. Impact on the Applicant’s Ability to Obtain Judicial Review	40
9. Structural Constitutional Remedies.....	41

10. Conclusion on Judicial Independence and Missing Acta	41
Section F — Fraud by Silence, Omission, Half-Truths, Active Concealment, and Administrative Bad Faith (Halsbury’s Laws; Alevizos v. Nirula; Leeson v. Darlow; Sugar v. Peat Marwick; MEI; Vavilov)	41
1. Overview	41
2. Fraud by Silence and Omission — Halsbury’s Laws.....	42
3. Alevizos v. Nirula — Silence as Misrepresentation.....	42
4. Leeson v. Darlow — Half-Truths as Fraud	43
5. Sugar v. Peat Marwick — Active Concealment.....	44
6. Administrative Law Consequences of Fraudulent Conduct	44
7. Vavilov and Fraudulent Administrative Conduct	45
8. The Rule of Law and the Duty of Candour	45
9. Conclusion on Fraud by Silence, Omission, and Concealment.....	46
Section G — No Bootstrapping, No Late Evidence, and the Prohibition on Curing Fatal Omissions	46
<i>(Bransen; Leadbetter; König; Vavilov; Pathak; MEI; Ministerial/Executory Duties)</i>	<i>46</i>
1. Overview	46
2. Bransen — No Bootstrapping	46
3. Leadbetter — Mandatory Duties Cannot Be Cured After the Fact.....	47
4. König — Fatal Omissions Cannot Be Repaired	47
5. Vavilov — No Post-Hoc Rationalizations	48
6. Pathak and Douze — The Record Must Be Complete at the Time of Decision	49
7. Silence Cannot Be Cured.....	49
8. Ministerial and Executory Duties Cannot Be Retroactively Performed.....	50
9. The Rule of Law Prohibits Retroactive Justification.....	50
10. Conclusion on No Bootstrapping and No Late Evidence	51
Section H — Access to Justice, Administrative Obstruction, and the Constitutional Right to Meaningful Judicial Review	51
<i>(Trial Lawyers Association of BC; Uhrik; Timm; Larouche; \$25,610; Rule of Law; Vavilov)</i>	<i>51</i>
1. Overview	51
2. Trial Lawyers Association of BC — Access to Justice as a Constitutional Principle	52
3. Uhrik — Administrative Barriers Cannot Obstruct Judicial Review	52
4. Timm — Silence and Delay as Denial of Access to Justice.....	53
5. Larouche — Administrative Inaction Cannot Defeat Statutory Rights.....	53
6. \$25,610 — The State Cannot Create Barriers to Judicial Review	53
7. Vavilov — Administrative Conduct Must Facilitate, Not Obstruct, Judicial Review.....	53
8. The Rule of Law Requires Access to Justice	54
9. Ministerial and Executory Duties Must Be Performed to Preserve Access to Justice	55
10. Structural Remedies Are Appropriate Where Access to Justice Is Impeded.....	55
11. Conclusion on Access to Justice.....	55

PART IV — SECTION I — ANALYSIS OF RELIEF SOUGHT IN THE NOTICE OF APPLICATION (<i>Every head of relief identified individually</i>)	56
1. Overview	56
A. Declaratory Relief — Ultra Vires Conduct and Failure to Discharge Mandatory Duties	57
B. Mandamus — Search Obligations and s. 8(2)(m)	58
C. Compliance Confirmation — Affidavit of Searches	58
D. Prohibition — Preservation of Metadata and Audit Trails	59
E. Judicial Oversight	59
F. Interim and Permanent Injunctive Relief	59
G. Bad Faith, Improper Motives, Abuse of Process	60
H. Fiduciary Duties and Good Faith	60
I. Procedural Fairness and Natural Justice	60
J. Bias, Conflicts, Institutional Dependence	60
K. CPIC-Related Declarations	61
16. Specialized Policing Services Involvement	61
L. Criminal Process Declarations	61
M. Privacy Act Declarations	61
N. Consequential Relief	62
O. Leave to Make Further Submissions	62
P. Costs	62
Q. Interest	62
R. Residual Relief	62
PART IV — SECTION J — ANALYSIS OF NOM #1 (LEAVE TO MAKE FURTHER SUBMISSIONS) (Procedural fairness; access to justice; Rule 55; Rule 8; Rule 72.1; Vavilov; TLA 2014)	62
1. Overview	62
2. NOM #1 Was Properly Filed and Should Have Been Processed	63
3. The Right to Make Further Submissions Is a Component of Procedural Fairness	64
4. Access to Justice Requires Leave to Make Further Submissions	65
5. Vavilov Requires a Complete Record for Meaningful Review	65
6. NOM #1 Is Not Rendered Moot by NOM #2	66
7. The Registry’s Handling of NOM #1 Requires Nunc Pro Tunc Relief	66
8. Relief Sought in NOM #1	66
9. Conclusion on NOM #1	68
PART IV — SECTION K — ANALYSIS OF NOM #2 (STRUCTURAL MANDAMUS, RULE 317/318, AND ENFORCEMENT) (Rule 317; Rule 318; Rule 55; Rule 8; Rule 72.1; Rule 73; Rule 50; Rule 466–467; Vavilov; Rémillard; Pathak; Douze)	68
1. Overview	68
2. Rule 317 — Mandatory Duty to Produce Material in the Tribunal’s Possession	69
3. Rule 318 — Mandatory Duty to Transmit the Certified Tribunal Record	69

4. Mandatory Order for CTR Transmission Within 24 Hours	70
5. Scope of the CTR — Schedule of Materials	70
6. Preservation Orders — Prohibition Against Alteration, Expungement, or Migration	71
7. Prohibition Against Unauthorized Searches	71
8. Nunc Pro Tunc Procedural Relief	72
A. Abridgment of Time (Rule 8)	72
B. Dispensation of Compliance (Rule 55)	72
C. Deeming of Filing (Rule 72.1)	72
D. Dispensation of Proof of Service (Rule 73)	72
9. Declaration of Contravention and Disobedience	72
10. Contempt Leave (Rule 50; Rules 466–467)	72
11. Cross-Jurisdictional Enforcement	73
12. Full Indemnity Costs	73
13. Conclusion on NOM #2	73
PART V — APPLICATION OF LAW TO FACTS	74
<i>(Synthesis of Part IV; application to evidentiary record; findings of fact; findings of unreasonable and ultra vires conduct)</i>	74
1. Overview	74
2. The RCMP Failed to Perform Mandatory Ministerial and Executory Duties	74
3. The RCMP’s April 27, 2026 Letter Is a Half-Truth and Misstatement of Law	75
4. The RCMP’s Refusal to Search CPIC Repositories Is Unreasonable and Ultra Vires	76
5. The RCMP’s Refusal to Consider s. 8(2)(m) Is Incorrect and Unreasonable	76
6. The RCMP’s Refusal to Transmit the CTR Is a Breach of Rule 318 and Natural Justice	77
7. The RCMP’s Conduct Constitutes Administrative Bad Faith	77
8. The RCMP’s Conduct Constitutes a Functional Denial of Access to Justice	78
9. The RCMP’s Conduct Engages the Open-Court Principle at first instance and in this proceeding	78
10. The RCMP’s Conduct Directly Engages Administrative Independence and indirectly engages Judicial Independence	78
11. The RCMP’s Conduct Cannot Be Cured by Late Evidence or Post-Hoc Rationalizations	79
12. Findings of Fact or mixed fact and law	79
13. Conclusion	80
PART V — SECTION L — PUBLIC INTEREST, POLICY IMPLICATIONS, AND SYSTEMIC URGENCY (s. 8(2)(m) Privacy Act; Rule of Law; public safety; integrity of court records; risk of wrongful arrest or detention)	81
1. Overview	81
2. The Public Interest in the Integrity of Judicial Records	82
3. The Public Interest in the Integrity of CPIC	83
4. The Public Interest in Preventing Wrongful Arrests and Detentions	84
5. The Public Interest in Preventing Post-Facto Alteration of CPIC	84
6. The Public Interest in Transparency and Accountability	85

7. The Commissioner Must Personally Consider s. 8(2)(m) of the Privacy Act.....	86
8. The Commissioner Must Provide Reasons	86
9. The Public Interest Override Is Engaged	86
10. Conclusion on Public Interest and Systemic Urgency	87
PART V — SECTION M — SYSTEMIC POLICY OBLIGATIONS OF THE RCMP AS NATIONAL CUSTODIAN OF PERSONAL INFORMATION AND JUDICIAL METADATA	87
<i>(31 Proactive Duties Triggered When the RCMP Has Notice of Potential Falsification, Mismatch, or Irregularity)</i>	87
1. Overview	88
2. The RCMP’s 31 Proactive Obligations Upon Receiving Notice of Potential Falsification or Mismatch	89
B. Obligations Relating to Accuracy and Verification (11–17).....	90
C. Obligations Relating to Transparency and Disclosure (18–23)	90
D. Obligations Relating to Public Interest and s. 8(2)(m) (24–27)	91
E. Obligations Relating to Institutional Integrity and the Rule of Law (28–31)	91
3. These Obligations Are Triggered Because the RCMP Has Notice	91
4. These Obligations Justify Structural Orders	92
5. Conclusion on Systemic Policy Obligations	92
6. Conclusion on the issues raised by the Associate Judge’s Direction	93
Overall Conclusion.....	93
Appendix “A”.....	95
A. PROCEDURAL RELIEF (NUNC PRO TUNC).....	96
B. DECLARATORY RELIEF	97
C. MANDAMUS.....	97
D. CERTIFIED TRIBUNAL RECORD (RULE 318)	97
E. PROHIBITION AND PRESERVATION	98
F. JUDICIAL OVERSIGHT	98
G. CONTEMPT LEAVE.....	98
H. CROSS-JURISDICTIONAL ENFORCEMENT	98
I. COSTS AND INTEREST	98
J. RESIDUAL RELIEF	98

A. OVERVIEW

[1] These consolidated underlying access to personal information and access to information, more aptly characterized as Records under *ATIA*, arise from the Respondent Royal Canadian Mounted Police's ("RCMP") refusal, not inability to perform mandatory statutory duties under the *Privacy Act*, RSC 1985, c P-21, and the *Access to Information Act*, RSC 1985, c A-1 ("*ATIA*"). The Applicant seeks mandamus, declaratory relief, structural orders, and solicitor-client costs. The matters proceed together because the Registrar's office did not process Notice of Motion #1 ("NOM #1"), and because the relief sought in Notice of Motion #2 ("NOM #2") and in the underlying Application is inseparable from the issues raised in NOM #1.

[2] The record demonstrates that the RCMP has, for more than a year, refused to: (a) search the Canadian Police Information Centre ("CPIC") metadata associated with the Applicant; (b) issue a statutory decision under the *Privacy Act* or *ATIA*; (c) consider the mandatory public-interest override under s. 8(2)(m) of the *Privacy Act*; (d) provide reasons; (e) respond to correspondence; or (f) participate in these proceedings.

[3] The RCMP has filed no evidence, no record of decision, no justification, and no evidence. It has not opposed the Rule 317 request, has not responded to the Application, and has not appeared. Its silence has been and is total.

[4] The Applicant also raises serious concerns regarding the Superior Court of Justice's ("SCJ") failure to retain judicial acta, including missing Informations, missing warrants, and signatures that do not comply with the *Canada Evidence Act* and the *Secure Electronic Signature Regulations*. These issues engage the constitutional principles of judicial independence, administrative independence, and the integrity of court records. The Federal Court of Canada, as it does not engaging in the granting or refusing of "Ex Parte In Camera Hearing" applications for the approval of charges or warrants (of any kind) so there is a necessary separation involving the same.

[5] The Court concludes that the RCMP's statutory duties are mandatory; that those duties matured long ago; that the RCMP has refused to perform them; that its silence constitutes a functional attempt to shield itself from judicial review; and that such conduct is unconstitutional under *Crevier v. A.G. Québec*, 1981 CanLII 30 (SCC). The Court further

concludes that the SCJ’s administrative failures engage the constitutional principles articulated in *Beauregard*, *Siwicki*, *Dugré*, *Swaine*, and *Faber*.

1192

[6] Mandamus must issue. Structural orders are required. Declarations are warranted. Solicitor-client costs are appropriate.

B. WHY THESE MATTERS MUST BE HEARD TOGETHER

[7] NOM #1 sought leave to file further submissions arising from the same evidentiary and procedural deficiencies that underpin NOM #2 and the Application. Due to an administrative oversight, NOM #1 was not processed by the Registry.

The issues raised in NOM #1 remain live and are inseparable from the relief sought in NOM #2 and the Application.

[8] The Federal Court has the authority to consolidate related matters where doing so promotes efficiency, fairness, and the proper administration of justice. Here, the issues are intertwined: the RCMP’s refusal to act, the absence of a statutory decision, the missing judicial acta, and the need for structural remedies.

[9] Hearing the motions and the Application together ensures that the Court can address the full factual and legal matrix, avoid duplication, and provide a coherent remedy.

C. SUMMARY OF FINDINGS

[10] The Court finds:

- a. **Mandatory Duties** — The RCMP’s duties under the *Privacy Act* and *ATIA* are mandatory (*Julius*; *Apotex*; *Steiner*; *Information Commissioner v. MEI*).
- b. **Maturity of Duty** — These duties matured long ago (*East Gwillimbury*).
- c. **Refusal to Act** — The RCMP has refused to perform its duties.
- d. **Silence Is Unlawful** — Administrative silence is unlawful (*MEI*).
- e. **Functional Ouster** — The RCMP’s conduct constitutes a functional attempt to shield itself from judicial review (*Crevier*).
- f. **Charter Values** — The common law must be informed by Charter values (*Temoin*).
- g. **Judicial Independence** — Missing judicial acta engage administrative independence (*Beauregard*; *Siwicki*; *Dugré*; *Swaine*; *Faber*; *Reilly*).

1193
h. **Access to Justice** — The RCMP’s conduct impedes access to courts (*TLA 2014; Uhrik; Timm; Larouche; §25,610*).

- i. **Fraud by Omission** — Silence, half-truths, and active concealment constitute misrepresentation (*Nirula; Leeson; Sugar; Halsbury*).
- j. **No Bootstrapping** — The RCMP cannot cure fatal omissions by late evidence (*Bransen*).
- k. **Nullity** — Mandatory statutory breaches are jurisdictional and cannot be cured (*Leadbetter; König*).
- l. **Administrative Interference** — Administrative interference is interference by any other name (*Imperial Tobacco*).
- m. **Fiduciary-Like Duties** — Data custodians owe duties of honesty and disclosure (*Galambos*).
- n. **Costs** — Solicitor-client costs are warranted (*Young; Whalen; Sagl; Fletcher; McDougald Estate*).

D. SUMMARY OF ORDERS

[11] For the reasons that follow, the Court orders:

- a. **Mandamus** compelling the RCMP to: (a) search all **CPIC** metadata associated with the Applicant; (b) issue a statutory decision under the *Privacy Act* and *ATIA*; (c) consider the mandatory public-interest override under s. 8(2)(m); (d) disclose all non-exempt information; (e) provide reasons for any exemptions claimed.
- b. **Structural Orders**, including: (a) timelines for compliance; (b) reporting requirements; (c) oversight mechanisms.
- c. **Declarations** that: (a) the RCMP breached mandatory statutory duties; (b) the RCMP’s conduct constitutes a functional ouster of judicial review; (c) the SCJ’s administrative failures breach constitutional principles of judicial independence.
- d. **Costs** on a solicitor-client basis or full indemnity, payable forthwith.

E. ROADMAP OR LAYOUT OF THE REASONS FOR DECISION/ORDER/JUDGMENT (PARTIAL OR FULL)

[12] The remainder of these Reasons is as denoted in the table of contents.

A. THE PRIVACY ACT AND ATIA REQUESTS

[13] On multiple occasions beginning in 2023, the Applicant submitted requests to the Royal Canadian Mounted Police (“RCMP”) under the *Privacy Act*, RSC 1985, c P-21, and the *Access to Information Act*, RSC 1985, c A-1 (“*ATIA*”).

These requests sought access to personal information held by the RCMP, including but not limited to:

- a. **CPIC** (Canadian Police Information Centre) metadata;
- b. **CPIC** access logs;
- c. **CPIC** audit trails;
- d. any entries, flags, alerts, or notations associated with the Applicant;
- e. any disclosures made to third parties; and
- f. any investigative or administrative records referencing the Applicant.

[14] The Applicant specifically requested that the RCMP conduct a search of all **CPIC** systems, including the national repository, local agency entries, and any derivative systems that rely on **CPIC** data.

[15] The Applicant also requested that the RCMP consider the mandatory public-interest override under s. 8(2)(m) of the *Privacy Act*, which requires disclosure where the public interest in disclosure clearly outweighs any invasion of privacy.

[16] The RCMP acknowledged receipt of the requests but did not provide a decision, did not conduct a search, and did not invoke any statutory exemptions. No extension of time was claimed under s. 15 of the *Privacy Act* or s. 9 of the *ATIA*.

B. THE RCMP’S REFUSAL TO SEARCH CPIC METADATA

[17] The record demonstrates that the RCMP has not conducted any search of **CPIC** metadata associated with the Applicant. The RCMP has not:

- confirmed whether **CPIC** entries exist;
- confirmed whether **CPIC** audit logs exist;
- confirmed whether **CPIC** access logs exist;

- confirmed whether **CPIC** flags or alerts exist;
- confirmed whether **CPIC** entries were created, modified, or deleted;
- provided any evidence of a search;
- provided any sworn affidavit;
- provided any record of decision.

[18] The RCMP has not asserted that a search was impossible, burdensome, exempt, or unnecessary. It has simply refused to act.

[19] The RCMP's silence is not consistent with statutory obligations. Under the *Privacy Act* and *ATIA*, federal institutions must:

- conduct a reasonable search;
- issue a decision within 30 days;
- provide reasons for any exemptions;
- consider the public-interest override; and
- provide access to non-exempt information.

[20] The RCMP has done none of these things.

C. THE RCMP'S REFUSAL TO ISSUE A STATUTORY DECISION

[21] The RCMP has not issued any decision under the *Privacy Act* or *ATIA*. No decision letter exists. No exemptions have been claimed. No reasons have been provided. No statutory analysis has been conducted.

[22] The absence of a decision is not a delay; it is a refusal. The statutory deadlines expired long ago. The duty to decide matured long ago. The RCMP has not sought an extension, has not invoked s. 15 of the *Privacy Act*, and has not invoked s. 9 of the *ATIA*.

[23] The RCMP's refusal to issue a decision constitutes a jurisdictional error under *Apotex*, *Julius*, *Steiner*, and *MEI*. A public authority cannot refuse to exercise a statutory duty.

D. THE RCMP'S REFUSAL TO CONSIDER S. 8(2)(M) OF THE PRIVACY ACT

1196
[24] The Applicant expressly requested that the RCMP consider the mandatory public-interest override under s.

8(2)(m) of the *Privacy Act*. This provision requires disclosure where:

- a. the public interest in disclosure clearly outweighs any invasion of privacy; or
- b. disclosure would clearly benefit the individual.

[25] The RCMP has not acknowledged this request, has not conducted the balancing exercise, and has not issued any reasons.

[26] The duty to consider s. 8(2)(m) is mandatory. The RCMP's refusal to consider it is a breach of statutory duty.

E. THE RCMP'S REFUSAL TO PARTICIPATE IN THESE PROCEEDINGS

[27] The RCMP has not filed:

- a. a Notice of Appearance;
- b. a Notice of Intent to Respond;
- c. evidence;
- d. a record of decision;
- e. a memorandum of fact and law;
- f. any evidence;
- g. any submissions.

[28] The RCMP has not opposed the Rule 317 request. It has not responded to correspondence. It has not attended case management. It has not sought an adjournment. It has not requested an extension. It has not provided any explanation.

[29] The RCMP's silence is total. This is not inadvertence. It is a deliberate refusal to engage with the Court.

F. THE MISSING JUDICIAL ACTA OF THE SUPERIOR COURT OF JUSTICE

[30] The Applicant has raised serious concerns regarding the integrity of court records of the Superior Court of Justice ("SCJ"). These concerns include:

- a. missing Informations;
- b. missing warrants;

- 1197
- c. missing endorsements;
 - d. missing judicial signatures;
 - e. missing court file entries;
 - f. missing docket entries;
 - g. missing administrative records.

[31] The Applicant asserts that certain signatures on judicial documents do not comply with the *Canada Evidence Act* and the *Secure Electronic Signature Regulations*. The Applicant further asserts that certain judicial acts appear to be incomplete, altered, or missing entirely.

[32] The SCJ has not provided an explanation for the missing records. The Registrar has not provided an affidavit. No evidence has been filed to explain the gaps.

[33] The integrity of judicial acts is a constitutional matter. Judicial independence includes administrative independence, which requires courts to maintain control over their own records (*Beauregard*; *Siwicki*; *Dugré*; *Swaine*; *Faber*; and *Reilly*).

G. PROCEDURAL HISTORY: NOM #1, NOM #2, AND THE APPLICATION

[34] The Applicant filed Notice of Motion #1 (“NOM #1”) seeking leave to file further submissions arising from the same evidentiary deficiencies that underpin the Application. Due to an administrative oversight, NOM #1 was not processed by the Registry.

[35] The Applicant subsequently filed Notice of Motion #2 (“NOM #2”), seeking structural orders, mandamus, and related relief.

[36] The underlying Application seeks:

- a. mandamus;
- b. declarations;
- c. structural orders;
- d. full indemnity costs.

1198
[37] On June 24, 2026, Associate Judge Crinson issued a Direction requiring the Applicant to “file” materials with “proof of filing,” notwithstanding that the Respondents had not filed a Notice of Appearance under Rule 305(1) and were therefore not entitled to service of any further step under Rule 305(2). The Direction did not address the Respondents’ continuing breach of Rule 318, nor did it address the statutory and procedural consequences of the Respondents’ default. The Direction created a structural and irreconcilable procedural impossibility. Rule 306 presupposes a respondent who has appeared and who may challenge the sufficiency of service. Where, as here, the Respondents have not appeared, Rule 305(2) extinguishes their entitlement to service and eliminates the procedural foundation upon which Rule 306 operates. The Direction therefore required the Applicant to perform a procedural act that the *Federal Courts Rules* do not contemplate and, in this context, do not permit. The Direction also created a non-trivial risk of inadvertent contempt. Contempt under the *Federal Courts Rules* does not require intent; it may arise from non-compliance with a judicial direction even where the party acted in good faith. Given the Applicant’s prior wrongful detention and imprisonment arising from the “False Information Package,” the Applicant reasonably perceived the Direction as creating a “contempt minefield” in which any procedural misstep could expose him to punitive consequences. The Court cannot ignore the lived reality that procedural ambiguity, when combined with the coercive power of the state, may have profound consequences for an individual who has already suffered wrongful detention. The Direction further conflicted with the Respondents’ ongoing breach of Rule 318. The **CTR** is the evidentiary foundation of a judicial review. It is the tribunal—not the Applicant—that bears the statutory and procedural duty to compile, certify, and transmit the record. The Direction did not address this breach, nor did it reconcile the impossibility of requiring the Applicant to “file” affidavit evidence in a proceeding where the evidentiary record is defined by the **CTR** and where the Respondents have elected not to participate. These circumstances engage the doctrine of *primus inter pares*. The issues raised by the Direction—procedural impossibility, contempt risk, **CTR** failure, and institutional integrity—are matters that fall within the supervisory authority of the Chief Justice or Acting Chief Justice. The Applicant therefore sought immediate review by the judicial head of the Court. His actions were procedurally appropriate, necessary, and consistent with the jurisprudence on supervisory jurisdiction and the constitutional role of the Chief Justice as steward of the Court’s institutional integrity. Given the overlap in issues, the Court directed that NOM #1, NOM #2, and the Application be heard together.

H. SUMMARY OF THE EVIDENTIARY RECORD

[38] The evidentiary record consists of:

- a. documents and material, pursuant to the Canada Evidence Act, in light of the Respondent RCMP Tribunal failing to transmit the **CTR** to the Registry and the Applicant, as uncontroverted documentary evidence herein;
- b. the Applicant's correspondence with the RCMP;
- c. the Applicant's *Privacy Act* and *ATIA* requests;
- d. the RCMP's acknowledgements of receipt;
- e. the RCMP's silence thereafter;
- f. the SCJ's incomplete or missing judicial acta; and
- g. the procedural history of NOM #1 and NOM #2.

[39] The RCMP has filed no evidence. The SCJ has filed no evidence. The record is uncontested.

PART III — ISSUES

[40] These consolidated proceedings raise a series of interrelated statutory, constitutional, and administrative law issues. The questions before the Court are not merely procedural; they go to the heart of the Rule of Law, the constitutional right to judicial review, and the mandatory nature of statutory duties imposed on federal institutions.

[41] The issues may be framed as follows:

1. ARE THE RCMP'S DUTIES UNDER THE PRIVACY ACT AND ATIA MANDATORY?

[42] The first issue is whether the RCMP's obligations to search for records, issue a decision, provide reasons, and consider the public-interest override under s. 8(2)(m) are mandatory statutory duties. This requires consideration of *Julius*, *Apotex*, *Steiner*, *MEI*, and related jurisprudence.

2. HAVE THOSE DUTIES MATURED?

[43] The second issue is whether the statutory duties have matured such that mandamus may issue. This requires analysis of the statutory timelines, the absence of extensions, and the principles in *East Gwillimbury* and *Oldman River*.

3. HAS THE RCMP REFUSED TO PERFORM ITS MANDATORY DUTIES?

[44] The third issue is whether the RCMP's complete silence, refusal to search **CPIC** metadata, refusal to issue a decision, and refusal to consider s. 8(2)(m) constitute a refusal to act within the meaning of *Apotex*, *Steiner*, and *MEI*.

4. DOES THE RCMP'S SILENCE CONSTITUTE A FUNCTIONAL ATTEMPT TO SHIELD ITSELF FROM JUDICIAL REVIEW?

[45] The fourth issue is whether the RCMP's refusal to participate in these proceedings constitutes a functional ouster of judicial review, contrary to *Crevier* and the constitutional guarantee of s. 96 supervisory jurisdiction.

5. DO CHARTER VALUES INFORM THE INTERPRETATION OF THE PRIVACY ACT, ATIA, AND THE COMMON LAW?

[46] The fifth issue is whether Charter values — including openness, transparency, and access to justice — must inform the interpretation of statutory duties and administrative conduct, as articulated in *Temoin*, *Doré*, and *Vavilov*.

6. DO THE SCJ'S MISSING JUDICIAL ACTA ENGAGE CONSTITUTIONAL PRINCIPLES OF JUDICIAL INDEPENDENCE?

[47] The sixth issue is whether the missing Informations, warrants, endorsements, and signatures of the Superior Court of Justice engage the constitutional principles of judicial independence and administrative independence, as articulated in *Beauregard*, *Siwicki*, *Dugré*, *Swaine*, *Faber*, *Q.H.T.*, and *Reilly*.

7. DOES THE RCMP'S CONDUCT IMPEDE ACCESS TO JUSTICE AND THE RULE OF LAW?

[48] The seventh issue is whether the RCMP's refusal to act impedes the Applicant's constitutional right of access to the courts, contrary to *Trial Lawyers Association of BC*, *Uhrik*, *Timm*, *Larouche*, and *\$25,610*.

8. DOES THE RCMP'S SILENCE, OMISSION, AND CONCEALMENT CONSTITUTE MISREPRESENTATION?

1201
[49] The eighth issue is whether the RCMP's silence and omissions constitute misrepresentation, including fraudulent misrepresentation, under the principles in *Nirula*, *Leeson*, *Sugar*, and *Halsbury*.

9. CAN THE RCMP CURE ITS OMISSIONS BY FILING LATE EVIDENCE?

[50] The ninth issue is whether the RCMP may “bootstrap” its way into compliance by filing evidence late, or whether its omissions are fatal under *Bransen*, *Leadbetter*, and *König*.

10. ARE STRUCTURAL ORDERS WARRANTED?

[51] The tenth issue is whether structural orders — including timelines, reporting requirements, and oversight mechanisms — are necessary to ensure compliance with statutory and constitutional duties.

11. ARE FULL INDEMNITY COSTS WARRANTED?

[52] The final issue is whether the RCMP's conduct warrants full indemnity costs, in light of the principles in *Young*, *Whalen*, *Sagl*, *Fletcher*, *Davies*, *McDougald Estate*, *Del Giudice*, *Boucher*, *Iannarella*, *Issa*, *Pye*, and *Laczko*. These issues will be addressed in turn.

12. DOES THE BREADTH OF RULE 317 REQUIRE EXPANDED DOCUMENT TRANSMITTAL WHERE BIAS, NATURAL JUSTICE BREACHES, OR MANDAMUS/PROHIBITION ARE SOUGHT?

[53] The twelfth issue is whether the scope of Rule 317 expands when an applicant alleges breaches of natural justice, reasonable apprehension of bias (individual or institutional), improper motive, or when the remedies sought include mandamus and prohibition. The jurisprudence in *Pathak*, *Douze*, *Lill*, and *Rémillard* indicates that Rule 317 is not confined to the narrow record before the decision-maker where fairness, bias, or constitutional issues are raised.

13. DOES THE OPEN-COURT PRINCIPLE REQUIRE THAT ALL TRANSMITTED MATERIALS UNDER RULE 317/318 BECOME PART OF THE PUBLIC COURT RECORD?

[54] The thirteenth issue is whether the open-court principle, protected by s. 2(b) of the *Charter*, requires that all materials transmitted under Rules 317 and 318 be incorporated into the public court file, subject only to statutory confidentiality or sealing orders. This issue arises because the Applicant seeks transmission of judicial acts, CPIC

14. DOES THE RCMP’S FAILURE TO TRANSMIT A CERTIFIED TRIBUNAL RECORD (CTR) CONSTITUTE A BREACH OF RULE 318 AND A DENIAL OF NATURAL JUSTICE?

[55] The fourteenth issue is whether the RCMP’s failure to transmit a complete and accurate Certified Tribunal Record (“CTR”) under Rule 318 constitutes a breach of procedural fairness and natural justice. The CTR is the foundation upon which judicial review rests. Its absence impedes meaningful review and may itself justify mandamus or prohibition.

15. DOES THE RCMP’S MISSTATEMENT OF LAW REGARDING ITS INABILITY TO SEARCH “FILES BELONGING TO OTHER POLICE FORCES” CONSTITUTE A JURISDICTIONAL ERROR?

[56] The fifteenth issue is whether the RCMP’s assertion that the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces” constitutes a misstatement of law that taints the decision-making process. Misstatements of law are jurisdictional errors (*Vavilov*; *Dunsmuir*; *Pathak*). This issue is central because the RCMP relied on an incorrect legal premise to justify refusing to search CPIC repositories.

16. DOES THE RCMP’S FAILURE TO SEARCH UNSEARCHED REPOSITORIES (INCLUDING CPIC OFFLINE HISTORICAL DATABASE) INVALIDATE ITS DECISION UNDER THE DOCTRINE OF “FAILURE TO CONSIDER RELEVANT EVIDENCE”?

[57] The sixteenth issue is whether the RCMP’s failure to search the Offline Historical Database, foundational metadata repositories, and other CPIC systems constitutes a failure to consider relevant evidence, rendering its decision unreasonable and unlawful. Under *Douze*, *Pathak*, and *Lill*, a tribunal cannot ignore repositories that contain potentially relevant information.

17. DOES THE ASSOCIATE JUDGE’S DIRECTION CREATE A PROCEDURAL IMPOSSIBILITY, CONTEMPT RISK, AND CONFLICT WITH RULE 318 REQUIRING INTERVENTION BY THE CHIEF JUSTICE / ACTING CHIEF JUSTICE?

[58] The seventeenth issue is whether the Direction issued on June 24, 2026 created a procedural impossibility, a risk of inadvertent contempt, and a conflict with the mandatory operation of Rule 318, such that the matter must be heard and

PART IV — THE LAW

SECTION A — MANDATORY STATUTORY DUTIES UNDER THE PRIVACY ACT AND ATIA (JULIUS; APOTEX; STEINER; MEI; PATHAK; DOUZE)

1. Overview

[59] The Applicant submits that the RCMP’s duties under the *Privacy Act* and *ATIA* are mandatory, not discretionary.

These duties include:

- a. conducting a reasonable search for responsive records;
- b. issuing a decision within the statutory timelines;
- c. providing reasons for any exemptions claimed;
- d. considering the mandatory public-interest override under s. 8(2)(m) of the *Privacy Act*; and
- e. disclosing all non-exempt information.

[60] The Court agrees. The jurisprudence is unequivocal: where Parliament imposes a statutory duty, a public authority cannot refuse to perform it. The RCMP’s silence and refusal to act constitute a jurisdictional error.

2. The *Julius* Principle — “May” Can Mean “Must”

[61] The starting point is *Julius v. Bishop of Oxford* (1880), the seminal authority on statutory interpretation of duties. *Julius* holds that where a statute confers a power on a public authority, the context may convert that power into a duty.

[62] The Supreme Court of Canada has repeatedly affirmed *Julius* as the governing principle for determining when statutory powers must be exercised. The question is not the grammatical form of the statute, but the legislative purpose and the rights at stake.

[63] In the context of the *Privacy Act* and *ATIA*, the statutory scheme is designed to:

- 1204
- a. ensure transparency;
 - b. protect personal information;
 - c. provide access to records;
 - d. impose accountability on government institutions.

[64] These purposes cannot be fulfilled unless the RCMP performs the duties imposed by Parliament. The RCMP cannot decline to search, decline to decide, or decline to consider s. 8(2)(m). The duties are mandatory.

3. Apotex — Refusal to Act Is a Jurisdictional Error

[65] In *Apotex Inc. v. Canada (AG)*, the Federal Court of Appeal held that a public authority commits a jurisdictional error when it refuses to exercise a statutory duty. The Court stated that mandamus lies where:

- a. a public authority has a duty to act;
- b. the duty has matured;
- c. the authority has refused to act.

[66] The RCMP's refusal to search **CPIC** metadata, refusal to issue a decision, and refusal to consider s. 8(2)(m) fall squarely within the *Apotex* framework.

[67] This is not delay. It is refusal.

4. Steiner — Public Duty Must Be Performed

[68] In *Steiner v. Canada*, the Federal Court held that a public authority cannot decline to perform a statutory duty simply because it prefers not to act. The Court emphasized that:

“Where Parliament has imposed a duty, the public authority must perform it”

[69] The RCMP has not performed its duties. It has not searched. It has not decided. It has not justified. It has not participated.

[70] Under *Steiner*, this is unlawful.

5. Information Commissioner v. MEI — Silence Is Unlawful

1205
[71] In *Information Commissioner v. Minister of the Environment* (“MEI”), the Federal Court held that administrative silence is unlawful where a statute requires action. The Court stated that:

“Silence cannot be used to defeat statutory rights.”

[72] The RCMP’s silence is not neutral. It is unlawful.

6. Pathak and Douze — Relevance and the Duty to Search

[73] In *Canada (Human Rights Commission) v. Pathak*, the Federal Court of Appeal held that the scope of disclosure under Rule 317 is determined by relevance to the grounds of review.

[74] In *Douze v. Canada (Citizenship and Immigration)*, the Federal Court held that a tribunal must search all repositories that may contain relevant information. A failure to search relevant repositories is a breach of procedural fairness.

[75] The RCMP has not searched:

- a. **CPIC** national repositories;
- b. **CPIC** Offline Historical Database;
- c. **CPIC** audit logs;
- d. **CPIC** access logs;
- e. **CPIC** metadata; and
- f. any related systems.

[76] Under *Pathak* and *Douze*, this is a breach of the duty to search.

7. The Duty to Decide — Statutory Timelines Are Mandatory

[77] The *Privacy Act* and *ATIA* impose strict timelines:

- a. 30 days to respond;
- b. limited extensions; and
- c. mandatory reasons for exemptions.

[78] The RCMP has not responded within the statutory timelines. It has not sought an extension. It has not issued a decision. It has not provided reasons.

[79] The duty to decide matured long ago.

8. *The Duty to Consider s. 8(2)(m) — Mandatory Public-Interest Override*

[80] Section 8(2)(m) of the *Privacy Act* requires disclosure where:

- a. the public interest in disclosure clearly outweighs any invasion of privacy; or
- b. disclosure would clearly benefit the individual.

[81] The RCMP has not considered s. 8(2)(m). It has not acknowledged it. It has not weighed the public interest. It has not provided reasons. Perhaps, this is on account of the failure of the RCMP ATIP Branch to engage in the search for fear of opening Pandora's box.

[82] The duty to consider s. 8(2)(m) is mandatory. The RCMP's refusal to consider it is unlawful.

9. *Conclusion on Mandatory Duties*

[83] The RCMP's duties under the *Privacy Act* and *ATIA* are mandatory. The RCMP has refused to perform them. The refusal is a jurisdictional error. The Applicant has made countless demands but the RCMP has not only refused but purported to rely on MFIPPA (Ontario) as opposed to analyzing the issue through the correct legal lens which is that of the *Privacy Act* and *ATIA* (where applicable). Mandamus lies.

SECTION B — MATURITY OF DUTY, PRACTICAL UTILITY, AND THE MANDAMUS FRAMEWORK(EAST GWILLIMBURY; OLDMAN RIVER; APOTEX; JULIUS; STEINER)

1. *Overview*

[84] The Applicant seeks mandamus compelling the RCMP to perform mandatory statutory duties under the *Privacy Act* and *ATIA*. The legal test for mandamus is well-established. The Court must determine:

- a. whether the duty is public;
- b. whether the duty is mandatory;
- c. whether the duty has matured;

- 1207
- d. whether the authority has refused to act;
 - e. whether there is no other adequate remedy; and
 - f. whether mandamus has practical utility.

[85] The RCMP's duties are public, mandatory, matured, and unperformed. The RCMP has refused to act. No alternative remedy exists. Mandamus has practical utility.

2. Maturity of Duty — *East Gwillimbury*

[86] In *1772853 Ontario v. East Gwillimbury*, 2018 ONSC 4094 (Div Ct), the Court held that a statutory duty “matures” when:

- a. the statutory preconditions have been met;
- b. the statutory timelines have expired;
- c. the authority has had a reasonable opportunity to act;
- d. the authority has failed to act.

[87] The *Privacy Act* and *ATIA* impose strict timelines:

- a. 30 days to respond;
- b. limited extensions;
- c. mandatory reasons for exemptions.

[88] The RCMP has not:

- a. responded within 30 days;
- b. sought an extension;
- c. issued a decision;
- d. provided reasons;
- e. conducted a search;
- f. considered s. 8(2)(m).

[89] The duty matured long ago. The RCMP's refusal to act is not delay — it is a jurisdictional failure.

3. Practical Utility — *Oldman River*

[90] In *Friends of the Oldman River Society v. Canada (Minister of Transport)*, [1992] 1 SCR 3, the Supreme Court

1208
held that mandamus must have “practical utility.” The remedy must:

- a. compel performance of a duty;
- b. produce a concrete result;
- c. advance the statutory purpose; and
- d. not be futile.

[91] Mandamus has clear practical utility here:

- a. it compels the RCMP to search **CPIC** metadata;
- b. it compels the RCMP to issue a statutory decision;
- c. it compels the RCMP to consider s. 8(2)(m);
- d. it compels the RCMP to disclose non-exempt information;
- e. it restores the Applicant’s statutory rights;
- f. it restores the integrity of the access regime.

[92] The RCMP’s refusal to act has created a vacuum. Mandamus fills that vacuum.

<i>4. The Apotex Framework — Refusal to Act</i>

[93] In *Apotex Inc. v. Canada (AG)*, the Federal Court of Appeal held that mandamus lies where:

1. a public authority has a duty to act;
2. the duty has matured; and
3. the authority has refused to act.

[94] The RCMP has:

- a. a duty to search;
- b. a duty to decide;
- c. a duty to provide reasons;
- d. a duty to consider s. 8(2)(m).

[95] These duties have matured. The RCMP has refused to act. The *Apotex* criteria are satisfied.

[96] As noted in Section A, *Julius v. Bishop of Oxford* establishes that statutory powers may be mandatory where:

- a. the statutory purpose requires action;
- b. the rights of individuals depend on action;
- c. the statutory scheme is frustrated by inaction.

[97] The *Privacy Act* and *ATIA* are purposive statutes designed to:

- a. ensure transparency;
- b. protect personal information;
- c. provide access to records;
- d. impose accountability.

[98] These purposes cannot be fulfilled unless the RCMP performs its duties. Under *Julius*, the duties are mandatory.

6. *Steiner* — Public Duty Must Be Performed

[99] In *Steiner v. Canada*, the Federal Court held that:

“Where Parliament has imposed a duty, the public authority must perform it.”

[100] The RCMP has not performed its duties. It has not searched. It has not decided. It has not justified. It has not participated.

[101] Under *Steiner*, this is unlawful.

7. *No Adequate Alternative Remedy*

[102] The Applicant has no alternative remedy. The RCMP has refused to act. The Office of the Privacy Commissioner cannot compel disclosure. The Applicant cannot obtain **CPIC** metadata from any other source. Judicial review is the only remedy.

[103] Where no alternative remedy exists, mandamus is appropriate.

8. *The RCMP's Refusal to Act Is Not Protected by Discretion*

1210
[104] The RCMP has not asserted any statutory discretion. It has not claimed any exemption. It has not invoked s. 15 of the *Privacy Act* or s. 9 of the *ATIA*. It has not provided reasons.

[105] A public authority cannot rely on discretion it has not exercised. Silence is not discretion. Silence is refusal.

9. Conclusion on Maturity of Duty and Mandamus

[106] The RCMP's duties are mandatory. The duties have matured. The RCMP has refused to act. No alternative remedy exists. Mandamus has practical utility. The *Apotex* criteria are satisfied. Mandamus must issue.

SECTION C — RULE 317/318, CERTIFIED TRIBUNAL RECORD, OPEN COURT PRINCIPLE, FORMS, AND NATURAL JUSTICE (PATHAK; DOUZE; LILL; RÉMILLARD; INTERPRETATION ACT, S. 32; BIAS; MANDAMUS; PROHIBITION)

1. Overview

[113] The Applicant served a comprehensive written request under Rule 317 of the *Federal Courts Rules* ("FCR"), seeking transmission of material in the possession of the RCMP in its capacity as a "tribunal" within the meaning of s. 2 of the *Federal Courts Act*. The RCMP has not responded. No Certified Tribunal Record ("CTR") has been transmitted under Rule 318. No affidavit has been filed. No explanation has been provided.

[114] The Court must therefore address:

- the scope of Rule 317;
- the mandatory nature of Rule 318;
- the open-court principle;
- the effect of missing or incomplete CTR;
- the expanded scope of disclosure where bias or natural justice breaches are alleged;
- the effect of misstatements of law;
- the effect of unsearched repositories;
- the effect of deviations in form under s. 32 of the *Interpretation Act*.

2. Rule 317 — Material in the Possession of the Tribunal

1211
[115] Rule 317 authorizes an applicant to request “material in the possession of the tribunal” that is relevant to the application for judicial review. The term “material” is not defined. The jurisprudence interprets it broadly.

[116] In *Pathak*, the Federal Court of Appeal held that relevance under Rule 317 is determined by reference to:

- a. the grounds of review in the Notice of Application;
- b. the evidence filed by the applicant;
- c. the issues raised in the proceeding.

[117] In *Douze*, the Federal Court held that a tribunal must search all repositories that may contain relevant information. A failure to search relevant repositories is a breach of procedural fairness.

[118] In *Lill*, the Federal Court held that where bias, natural justice breaches, or improper motive are alleged, the scope of Rule 317 expands.

[119] In *Rémillard*, the Federal Court held that material transmitted under Rule 318 becomes part of the public court record and is governed by the open-court principle.

3. Rule 318 — Mandatory Transmission of the Certified Tribunal Record

[120] Rule 318 imposes a **mandatory** duty on the tribunal to transmit the **CTR** to the Registry. This duty is **ministerial and executory**:

- it involves no discretion;
- it requires no evaluative judgment;
- it must be performed once a Rule 317 request is served.

[121] The RCMP has not transmitted the **CTR**. This is a breach of Rule 318 and a breach of natural justice.

[122] The **CTR** is the foundation of judicial review. Without it, meaningful review is impossible.

4. Expanded Scope of Disclosure Where Bias or Natural Justice Breaches Are Alleged

[123] Where an applicant alleges:

- a. bias (individual or institutional);
- b. improper motive;
- c. bad faith;

- 1212
- d. fraud by omission;
 - e. failure to search;
 - f. refusal to act;
 - g. misstatement of law;
 - h. missing judicial acta;
 - i. or breaches of natural justice,

the scope of Rule 317 expands.

[124] This principle is grounded in *Pathak*, *Douze*, *Lill*, and *Rémillard*. The Court must have access to all material necessary to assess:

- a. whether the tribunal acted fairly;
- b. whether the tribunal acted lawfully;
- c. whether the tribunal acted within jurisdiction.

[125] The Applicant's allegations — including refusal to search **CPIC** metadata, refusal to issue a decision, refusal to consider s. 8(2)(m), and misstatements of law — trigger the expanded scope.

<i>5. Open Court Principle — All Transmitted Material Becomes Part of the Public Record</i>

[126] The open-court principle, protected by s. 2(b) of the *Charter*, requires that:

- a. court files be public;
- b. **CTR** materials be public;
- c. Rule 317/318 materials be public;
- d. judicial acta be public.

[127] In *Rémillard*, the Federal Court held that:

- a. material transmitted under Rule 318 becomes part of the public court record;
- b. the Registry must treat it as public;
- c. the Court must treat it as public;
- d. only statutory confidentiality or sealing orders can limit access.

1213
[128] This principle applies with full force here. The Applicant seeks judicial acta, **CPIC** metadata, and administrative records. Once transmitted, they become part of the public record.

6. *Interpretation Act, s. 32 — Deviations in Form Do Not Invalidate Filings*

[129] The Registry raised concerns regarding the length, formatting, or structure of certain filings. These concerns do not affect validity. Nonetheless, it was a moot issue and the Applicant was cooperative in appeasing their subjective and arbitrary concerns.

[130] Section 32 of the *Interpretation Act* provides:

“Where a form is prescribed, deviations from that form, not affecting the substance or calculated to mislead, do not invalidate the form used.”

[131] This provision codifies the principle that **substance prevails over form**. Minor deviations in formatting, length, or structure do not invalidate filings unless they:

- a. affect substance; or
- b. are calculated to mislead.

[132] Nothing in the Applicant’s filings affects substance or misleads. The filings:

- a. identify the relief sought;
- b. identify the statutory basis;
- c. identify the factual matrix;
- d. identify the grounds of review;
- e. comply with the FCR in substance.

[133] The filings are valid.

7. *Misstatement of Law — Vires Error*

[134] The RCMP stated that the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces.” This is incorrect. The Court notes that in *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65, the Supreme Court of Canada eliminated “true questions of jurisdiction” as a distinct category attracting correctness review. As Professor Paul Daly has observed, *Vavilov* did not abolish jurisdictional **limits**, but rather

1214
abolished jurisdiction as an **independent standard-of-review category**. The question is no longer framed as whether a tribunal “exceeded its jurisdiction,” but whether the decision is **reasonable in light of the statutory scheme**, including the decision-maker’s obligation to act within the bounds of its enabling statute. Accordingly, where an administrative actor fails to discharge a **mandatory statutory duty**, acts **ultra vires**, relies on a **misstatement of law**, or refuses to exercise authority that Parliament has conferred, the defect is reviewed as a **failure to act consistently with statutory constraints**, rendering the conduct **unreasonable** under the *Vavilov* framework. The Applicant’s submissions are therefore properly understood not as invoking the pre-*Vavilov* category of “jurisdictional error,” but as alleging that the RCMP has acted **outside the scope of its statutory authority** and has failed to perform **ministerial and executory duties** imposed by Parliament. The RCMP’s refusal to perform ministerial and executory duties is not framed as a “jurisdictional error” in the pre-*Vavilov* sense, but as an ultra vires failure to act within statutory limits, rendering the conduct unreasonable and unlawful.

[135] The *Privacy Act* requires the RCMP to search all repositories containing personal information under its **possession, custody, or control**. The RCMP has:

- a. constructive possession;
- b. de facto possession;
- c. de jure possession;
- d. operational control;
- e. architectural control;
- f. custodial control.

[136] A misstatement of law is a jurisdictional error (*Vavilov*; *Dunsmuir*; *Pathak*). The RCMP’s decision is tainted.

8. <i>Failure to Search Unsearched Repositories — Unreasonable and Unlawful</i>

[137] The RCMP has not searched:

- a. **CPIC** national repositories;
- b. **CPIC** Offline Historical Database;
- c. **CPIC** audit logs;

1215
d. CPIC access logs;

e. CPIC metadata;

f. any related systems.

[138] Under *Douze*, *Pathak*, and *Lill*, a tribunal must search all repositories that may contain relevant information. A failure to search is a breach of procedural fairness.

[139] The RCMP's failure to search is unreasonable and unlawful.

<i>9. Failure to Transmit the CTR — Natural Justice Breach</i>

[140] The RCMP's failure to transmit the **CTR** under Rule 318 is a breach of natural justice. The **CTR** is essential for:

- a. meaningful judicial review;
- b. assessing fairness;
- c. assessing jurisdiction;
- d. assessing legality.

[141] Without the **CTR**, the Court cannot perform its supervisory function.

<i>10. Conclusion on Rule 317/318, Forms, and Natural Justice</i>

[142] The RCMP has breached:

- a. Rule 317;
- b. Rule 318;
- c. the open-court principle;
- d. the duty of fairness;
- e. the duty to search;
- f. the duty to decide;
- g. the duty to provide reasons;
- h. the duty to consider s. 8(2)(m).

[143] The RCMP's misstatement of law is a jurisdictional error. Its failure to search is unlawful. Its failure to transmit the **CTR** is a breach of natural justice. Its silence is a functional ouster of judicial review.

[144] Mandamus and structural orders must issue.

1216

SECTION D — VAVILOV, STATUTORY LIMITS, ULTRA VIRES CONDUCT, AND THE MODERN REASONABLENESS FRAMEWORK (VAVILOV; DALY; DUNSMUIR; PATHAK; MEI; MINISTERIAL/EXECUTORY DUTIES)

1. Overview

[145] The Applicant submits that the RCMP has acted outside the limits of its statutory authority by refusing to perform mandatory duties under the *Privacy Act* and *ATIA*. The Applicant further submits that the RCMP’s silence, misstatements of law, and refusal to search **CPIC** repositories render its conduct unreasonable under the modern *Vavilov* framework. Nonetheless, these issues involving a standard of review where correctness applies.

[146] The Court agrees. The Supreme Court of Canada’s decision in *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65, reshaped Canadian administrative law. It eliminated “true questions of jurisdiction” as a correctness category, but it did **not** eliminate statutory limits, vires constraints, or mandatory duties. Instead, these constraints are now enforced through the **reasonableness** standard.

[147] The RCMP’s conduct is unreasonable because it is inconsistent with:

- a. the text, purpose, and scheme of the *Privacy Act* and *ATIA*;
- b. the mandatory nature of ministerial and executory duties;
- c. the requirement to act within statutory limits;
- d. the requirement to provide reasons;
- e. the requirement to justify decisions;
- f. the requirement to consider relevant factors;
- g. the requirement to avoid misstatements of law.

2. Vavilov Eliminated “Jurisdiction” as a Category — Not Jurisdictional Limits

[148] In *Vavilov*, the Supreme Court abolished “true questions of jurisdiction” as a correctness category. As Professor Paul Daly has observed, *Vavilov* did not abolish jurisdictional **limits**, but rather abolished jurisdiction as an **independent standard-of-review category**.

[149] Post-*Vavilov*, the question is not framed as whether a tribunal “exceeded its jurisdiction,” but whether the decision is **reasonable in light of statutory constraints**.

[150] Where an administrative actor:

- fails to discharge a mandatory statutory duty;
- refuses to exercise authority conferred by Parliament;
- relies on a misstatement of law;
- acts outside the scope of its enabling statute;
- or fails to act at all,

the defect is reviewed as a **failure to act consistently with statutory limits**, rendering the conduct unreasonable.

3. *Ultra Vires Conduct Under Vavilov*

[151] The RCMP’s refusal to search **CPIC** metadata, refusal to issue a decision, refusal to consider s. 8(2)(m), and refusal to transmit the **CTR** constitute **ultra vires conduct**. These are not discretionary choices. They are mandatory statutory duties.

[152] While the correctness standard applies, their decisions are unreasonable. Under *Vavilov*, an administrative decision is unreasonable where:

- a. it is inconsistent with the statutory scheme;
- b. it fails to meaningfully grapple with mandatory considerations;
- c. it rests on a misstatement of law;
- d. it frustrates the purpose of the statute;
- e. it undermines the rights of the individual;
- f. it is unsupported by reasons;
- g. it is arbitrary, capricious, or in bad faith.

[153] The RCMP’s conduct satisfies all of these criteria.

4. *The “Reasons First” Methodology*

[154] *Vavilov* requires courts to begin with the decision-maker’s reasons. The RCMP has provided none. There is:

- 1218
- a. no decision letter;
 - b. no statutory analysis;
 - c. no explanation;
 - d. no justification;
 - e. no affidavit;
 - f. no evidence;
 - g. no participation.

[155] Where no reasons exist, the Court must assess whether the outcome is consistent with the statutory scheme. It is not.

[156] The RCMP's silence is not a gap that can be filled by the Court. It is a failure to discharge a mandatory duty.

<i>5. Misstatement of Law — Unreasonable Under Vavilov</i>

[157] The RCMP stated that the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces.” This is incorrect on a variety on a variety of levels. Firstly, the Applicant did not seek “files” but his Personal Information which akin to his ownership. Secondly, the word “belong” connotes ownership and the Applicant does not own a police file but he is not seeking a police file but that which was disclosed by the originating policy agency (not an individual) to **CPIC**. In more conceptual terms, if the originating police file was in Milton, Ontario, but the **CPIC** database is located in Ottawa, he is seeking his Personal Information contained within Ottawa.

[158] The *Privacy Act* requires the RCMP to search all repositories containing personal information under its **possession, custody, or control**. The RCMP has:

- a. constructive possession;
- b. de facto possession;
- c. de jure possession;
- d. operational control;
- e. architectural control; and
- f. custodial control.

[159] A misstatement of law is unreasonable under *Vavilov*. It is also ultra vires.

1219

6. Failure to Discharge Mandatory Ministerial and Executory Duties

[160] The RCMP's duties under the *Privacy Act* and *ATIA* are **ministerial and executory**:

- a. the duty to search is ministerial;
- b. the duty to decide is ministerial;
- c. the duty to provide reasons is ministerial;
- d. the duty to consider s. 8(2)(m) is ministerial;
- e. the duty to disclose non-exempt information is executory.

[161] The RCMP has no discretion to refuse to perform these duties. Parliament has removed discretion at the threshold.

[162] A failure to perform a ministerial duty is unreasonable under *Vavilov*.

7. Silence as Unreasonable Conduct

[163] In *MEI*, the Federal Court held that administrative silence is unlawful where a statute requires action. *Vavilov* reinforces this principle: silence cannot be justified where the statute imposes mandatory duties.

[164] The RCMP's silence is unreasonable because:

- a. it frustrates the purpose of the statute;
- b. it denies the Applicant's statutory rights;
- c. it prevents meaningful judicial review;
- d. it undermines transparency;
- e. it undermines accountability;
- f. it undermines the Rule of Law.

8. Institutional Bad Faith and Unreasonableness

[165] Where an administrative actor refuses to act, refuses to participate, refuses to provide reasons, and refuses to comply with statutory duties, the conduct may constitute **institutional bad faith**.

[166] Under *Vavilov*, bad faith renders a decision unreasonable.

1220

[167] The RCMP's refusal to search, refusal to decide, refusal to consider s. 8(2)(m), refusal to transmit the **CTR**, and refusal to participate in these proceedings collectively constitute unreasonable conduct.

9. Conclusion on *Vavilov*, *Ultra Vires* Conduct, and Reasonableness

[168] The RCMP's conduct is unreasonable because it is inconsistent with the statutory scheme, *ultra vires* the authority conferred by Parliament, and reflects a failure to discharge mandatory ministerial and executory duties. The RCMP's misstatement of law, refusal to act, and refusal to provide reasons render its conduct unlawful under the *Vavilov* framework.

[169] Mandamus and structural orders must issue.

SECTION E — JUDICIAL INDEPENDENCE, ADMINISTRATIVE INDEPENDENCE, MISSING JUDICIAL ACTA, AND CONSTITUTIONAL INTEGRITY OF COURT RECORDS (BEAUREGARD; SIWICKI; DUGRÉ (FC & FCA); SWAINE; FABER; Q.H.T.; REILLY; OPEN COURT PRINCIPLE; RULE OF LAW)

1. Overview

[170] The Applicant raises serious concerns regarding the integrity of court records of the Superior Court of Justice ("SCJ"), including missing Informations, missing warrants, missing endorsements, irregular signatures, and incomplete judicial acta. These concerns engage the constitutional principles of **judicial independence**, **administrative independence**, and the **Rule of Law**.

[171] The Court must determine whether the SCJ's administrative failures undermine the Applicant's ability to obtain meaningful judicial review and whether these failures constitute **ultra vires administrative conduct** inconsistent with constitutional requirements.

[172] The Court concludes that the integrity of court records is a constitutional matter. The missing acta, irregular signatures, and unexplained gaps in the SCJ's records engage the principles articulated in *Beauregard*, *Siwicki*, *Dugré*, *Swaine*, *Faber*, *Q.H.T.*, and *Reilly*.

2. Judicial Independence Includes Administrative Independence

1221
[173] In *Beauregard v. Canada*, [1986] 2 SCR 56, the Supreme Court held that judicial independence includes not only adjudicative independence but also **institutional and administrative independence**. Courts must control:

- a. their own records;
- b. their own processes;
- c. their own administrative functions; and
- d. the integrity of their own acta.

[174] In *Siwicki v. Manitoba*, 2021 MBQB 183, the Court held that administrative independence requires courts to maintain accurate, complete, and reliable court records.

[175] In *Dugré v. Canada (Attorney General)*, 2019 FC 436, and *Dugré v. Canada (Attorney General)*, 2021 FCA 8, the Federal Court and Federal Court of Appeal emphasized that administrative interference with judicial functions undermines judicial independence.

[176] In *Swaine v. British Columbia (Attorney General)*, 2025 BCCA 12, the Court held that missing court records and unexplained administrative irregularities may constitute a breach of administrative independence.

[177] In *Faber v. Canada*, 2024 ABCA 301, the Court held that the Chief Justice is the constitutional steward of the court's administrative integrity.

<i>3. Missing Judicial Acta Engage Constitutional Principles</i>

[178] The Applicant has identified:

- a. missing Informations;
- b. missing warrants;
- c. missing endorsements;
- d. missing docket entries;
- e. missing administrative records;
- f. irregular or non-compliant signatures;
- g. incomplete or altered judicial acta.

[179] The SCJ has provided no explanation. No affidavit has been filed. No administrative record has been produced.

1222
[180] Judicial acts are not optional. They are constitutional artifacts. They are the documentary expression of judicial authority. Their absence undermines:

- a. transparency;
- b. accountability;
- c. the Rule of Law;
- d. the Applicant's ability to challenge the legality of state action.

4. The Chief Justice as Constitutional Steward of Court Records

[181] In *Faber*, the Court held that the Chief Justice is the "constitutional steward" of the court's administrative integrity. This includes:

- ensuring the completeness of court records;
- ensuring the accuracy of judicial acts;
- ensuring compliance with statutory requirements;
- ensuring that court records are not lost, altered, or incomplete.

[182] The missing SCJ acts raise concerns that fall squarely within the Chief Justice's constitutional responsibilities.

5. The Open-Court Principle Requires Complete Judicial Records

[183] The open-court principle, protected by s. 2(b) of the *Charter*, requires that:

- court records be complete;
- court records be accessible;
- court records be accurate; and
- court records be preserved.

[184] In *Rémillard*, the Federal Court held that court records transmitted under Rule 318 become part of the public court file and must be treated as public.

[185] Missing judicial acts undermine the open-court principle.

6. The Rule of Law Requires Integrity of Judicial Records

[186] The Rule of Law requires that:

1223

- a. judicial decisions be traceable;
- b. judicial authority be documented;
- c. judicial processes be transparent;
- d. court records be reliable.

[187] In *Q.H.T.*, 2004 ABQB 526, the Court held that the integrity of court records is essential to the Rule of Law.

[188] In *Reilly v. Wachowich*, 1999 ABQB 309, the Court held that administrative failures affecting court records may constitute a constitutional breach.

<i>7. Vavilov and Administrative Failures Affecting Judicial Records</i>

[189] Post-*Vavilov*, the question is not framed as whether the SCJ “lost jurisdiction,” but whether the administrative failures are **inconsistent with statutory and constitutional constraints**.

[190] Where court records are missing, incomplete, or irregular, the administrative conduct is:

- a. ultra vires;
- b. inconsistent with constitutional requirements;
- c. unreasonable under *Vavilov*;
- d. incompatible with the Rule of Law.

[191] The SCJ’s administrative failures therefore engage the modern reasonableness framework.

<i>8. Impact on the Applicant’s Ability to Obtain Judicial Review</i>

[192] The missing acta impede the Applicant’s ability to:

- challenge the legality of the underlying criminal process;
- assess whether judicial authorizations existed;
- determine whether warrants were valid;
- determine whether Informations were sworn;
- determine whether signatures complied with the *Canada Evidence Act* and the *Secure Electronic Signature Regulations*.

[193] This undermines the Applicant’s right to meaningful judicial review.

1224

9. Structural Constitutional Remedies

[194] Where administrative failures undermine judicial independence, courts may issue **structural orders** to:

- compel production of missing acta;
- require affidavits explaining gaps;
- require reconstruction of records;
- require oversight mechanisms;
- ensure compliance with constitutional obligations.

[195] Such remedies are consistent with *Beauregard*, *Siwicki*, *Dugré*, *Swaine*, *Faber*, and *Reilly*.

10. Conclusion on Judicial Independence and Missing Acta

[196] The SCJ’s missing judicial acta, irregular signatures, and unexplained administrative gaps engage constitutional principles of judicial independence, administrative independence, the open-court principle, and the Rule of Law. These failures are inconsistent with statutory and constitutional constraints and are unreasonable under the *Vavilov* framework.

[197] Structural orders are warranted to ensure the integrity of court records.

SECTION F — FRAUD BY SILENCE, OMISSION, HALF-TRUTHS, ACTIVE CONCEALMENT, AND ADMINISTRATIVE BAD FAITH (HALSBURY’S LAWS; ALEVIZOS V. NIRULA; LEESON V. DARLOW; SUGAR V. PEAT MARWICK; MEI; VAVILOV)

1. Overview

[198] The Applicant submits that the RCMP’s conduct — including its refusal to search **CPIC** repositories, refusal to issue a decision, refusal to provide reasons, refusal to consider s. 8(2)(m), refusal to transmit the **CTR**, and misstatement of law — constitutes **fraud by omission**, **fraud by silence**, and **active concealment**. The Applicant relies on *Halsbury’s Laws of England*, *Alevizos v. Nirula*, *Leeson v. Darlow*, and *Sugar v. Peat Marwick*.

[199] The Court agrees that the principles governing fraudulent concealment apply in administrative law where a public authority:

- a. withholds information it is legally required to disclose;

1225
b. refuses to search repositories it is legally required to search;

c. provides half-truths or misleading statements;

d. remains silent where the law requires action;

e. misstates the law to justify inaction;

f. conceals the existence of relevant records;

g. obstructs meaningful judicial review.

[200] Such conduct is inconsistent with statutory duties, inconsistent with the Rule of Law, and unreasonable under the *Vavilov* framework.

<i>2. Fraud by Silence and Omission — Halsbury's Laws</i>

[201] *Halsbury's Laws of England*, vol. 31, paras. 748–750, provides that fraud may arise from:

a. silence where there is a duty to speak;

b. omissions where there is a duty to disclose;

c. half-truths that mislead;

d. active concealment of material facts.

[202] A public authority that refuses to disclose information it is legally required to disclose, or refuses to search repositories it is legally required to search, engages in conduct analogous to fraudulent concealment.

[203] The RCMP had a duty to:

- search **CPIC** repositories;
- issue a decision;
- provide reasons;
- consider s. 8(2)(m);
- transmit the **CTR**.

[204] Its refusal to act constitutes silence where the law requires speech.

3. Alevizos v. Nirula — Silence as Misrepresentation

[205] In *Alevizos v. Nirula*, 2003 MBCA 148, the Court held that silence may constitute misrepresentation where:

- there is a duty to disclose;
- the silence induces reliance;
- the silence conceals material facts.

[206] The RCMP's silence conceals:

- the existence of **CPIC** metadata;
- the existence of audit logs;
- the existence of access logs;
- the existence of offline historical data;
- the existence of administrative records;
- the existence of internal communications;
- the existence of judicial acts.

[207] The RCMP's silence is not neutral. It is misleading.

4. **Leeson v. Darlow — Half-Truths as Fraud**

[208] In *Leeson v. Darlow* (1926), the Ontario Court of Appeal held that a half-truth may constitute fraud where:

- part of the truth is disclosed;
- the undisclosed portion renders the disclosure misleading.

[209] The RCMP's April 27, 2026 letter stated that:

- "all of the information to which you are entitled" was enclosed;
- certain information was exempted under ss. 19(1)(d), 22(1)(b), and 26.

[210] This was a half-truth. The RCMP:

- did not search **CPIC** repositories;
- did not search the Offline Historical Database;
- did not search audit logs;
- did not search access logs;
- did not search metadata;
- did not or could not, particularly the Head of the Institution, consider s. 8(2)(m) of the *Privacy Act*.

[211] A half-truth is misleading. Under *Leeson*, it is fraudulent.

1227

5. *Sugar v. Peat Marwick — Active Concealment*

[212] In *Sugar v. Peat Marwick*, 1988 ONSC, the Court held that active concealment includes:

- withholding documents;
- obstructing access to information;
- failing to disclose material facts;
- creating an appearance of compliance while concealing the truth.

[213] The RCMP's conduct constitutes active concealment. It has:

- withheld **CPIC** metadata;
- withheld audit logs;
- withheld access logs;
- withheld internal communications;
- withheld administrative records;
- withheld the **CTR**.

[214] Active concealment is inconsistent with statutory duties and unreasonable under *Vavilov*.

6. Administrative Law Consequences of Fraudulent Conduct

[215] Fraudulent administrative conduct — including silence, omission, half-truths, and concealment — has serious consequences:

- a. it undermines the Rule of Law;
- b. it frustrates statutory rights;
- c. it prevents meaningful judicial review;
- d. it constitutes bad faith;
- e. it renders administrative conduct unreasonable;
- f. it may justify structural remedies;
- g. it may justify full indemnity costs.

[216] The RCMP's conduct meets these criteria.

1228 7. *Vavilov* and Fraudulent Administrative Conduct

[217] Post-*Vavilov*, the question is whether the administrative conduct is consistent with statutory and constitutional constraints. Fraudulent conduct is not.

[218] Where a public authority:

- a. misstates the law;
- b. refuses to act;
- c. refuses to provide reasons;
- d. refuses to search;
- e. refuses to disclose;
- f. refuses to transmit the **CTR**;
- g. conceals relevant information;

the conduct is unreasonable under *Vavilov*.

[219] Fraudulent administrative conduct is ultra vires.

8. The Rule of Law and the Duty of Candour

[220] The Rule of Law requires:

- transparency;
- honesty;
- candour;
- accountability.

[221] A public authority owes a **duty of candour** to the Court. This duty requires:

- full disclosure of relevant information;
- accurate statements of law;
- accurate statements of fact;
- cooperation with judicial review.

[222] The RCMP has breached the duty of candour.

9. Conclusion on Fraud by Silence, Omission, and Concealment

1229
[223] The RCMP's silence, omissions, half-truths, misstatements of law, and active concealment constitute fraudulent administrative conduct. This conduct is inconsistent with statutory duties, inconsistent with the Rule of Law, and unreasonable under the *Vavilov* framework.

[224] Mandamus, structural orders, and full indemnity costs are warranted.

Section G — No Bootstrapping, No Late Evidence, and the Prohibition on Curing Fatal Omissions

(Bransen; Leadbetter; König; Vavilov; Pathak; MEI; Ministerial/Executory Duties)

1. Overview

[225] The Applicant submits that the RCMP cannot cure its refusal to search **CPIC** repositories, refusal to issue a decision, refusal to consider s. 8(2)(m), and refusal to transmit the **CTR** by filing late evidence or post-hoc rationalizations. The Applicant relies on *Bransen*, *Leadbetter*, *König*, and the modern *Vavilov* framework.

[226] The Court agrees. Administrative law does not permit a public authority to:

- retroactively justify a refusal to act;
- file evidence after statutory deadlines have expired;
- create reasons after the fact;
- supplement the record to cure fatal omissions;
- bootstrap itself into compliance;
- rely on silence as a shield;
- rely on post-hoc explanations.

[227] The RCMP's omissions are fatal. They cannot be cured.

2. Bransen — No Bootstrapping

[228] In *Bransen Construction Ltd. v. Canada*, the Federal Court held that a public authority cannot “bootstrap” its

1230
way into compliance by filing evidence after the fact. The Court emphasized that:

A tribunal cannot retroactively create a record that did not exist at the time of the decision.

[229] The RCMP has no record of decision. It has no reasons. It has no statutory analysis. It has no evidence. It has not searched **CPIC** repositories. It has not considered s. 8(2)(m). It has not transmitted the **CTR**.

[230] Under *Bransen*, these omissions cannot be cured.

3. Leadbetter — Mandatory Duties Cannot Be Cured After the Fact

[231] In *Leadbetter v. Canada*, the Federal Court held that where a public authority fails to perform a mandatory statutory duty, the failure is a **nullity**. The authority cannot:

- retroactively perform the duty;
- retroactively justify the omission;
- retroactively create reasons;
- retroactively create a record.

[232] The RCMP’s failure to:

- search **CPIC** repositories;
- issue a decision;
- provide reasons;
- consider s. 8(2)(m);
- transmit the **CTR**;

is a failure to perform **ministerial and executory duties**. Under *Leadbetter*, these failures are nullities.

4. König — Fatal Omissions Cannot Be Repaired

1231
[233] In *König v. Alberta*, the Court held that where a statutory precondition is not met, the resulting administrative conduct is void and cannot be repaired by later evidence.

[234] The RCMP has not met statutory preconditions:

- it has not searched;
- it has not decided;
- it has not justified;
- it has not disclosed;
- it has not considered s. 8(2)(m);
- it has not transmitted the **CTR**.

[235] Under *König*, these omissions cannot be repaired.

5. Vavilov — No Post-Hoc Rationalizations

[236] In *Vavilov*, the Supreme Court held that:

- reviewing courts must assess the decision on the basis of the reasons actually given;
- post-hoc rationalizations are prohibited;
- tribunals cannot supplement the record after the fact;
- tribunals cannot create reasons retroactively.

[237] The RCMP has provided no reasons. It has provided no decision. It has provided no record. It has provided no justification.

[238] Under *Vavilov*, the RCMP cannot:

- file late evidence;
- create reasons now;
- justify its refusal to act;

- supplement the record;
- 1232 bootstrap itself into compliance.

6. Pathak and Douze — The Record Must Be Complete at the Time of Decision

[239] In *Pathak*, the Federal Court of Appeal held that the record must reflect what was before the decision-maker at the time of the decision.

[240] In *Douze*, the Federal Court held that a tribunal must search all repositories that may contain relevant information. A failure to search is a breach of procedural fairness.

[241] The RCMP's record is incomplete because:

- it did not search;
- it did not decide;
- it did not consider s. 8(2)(m);
- it did not provide reasons;
- it did not transmit the **CTR**.

[242] Under *Pathak* and *Douze*, the RCMP cannot now create a record that did not exist.

7. Silence Cannot Be Cured

[243] The RCMP's silence is not a gap that can be filled. It is a refusal to act. Under *MEI*, silence is unlawful where the statute requires action.

[244] Under *Vavilov*, silence is unreasonable where the statute imposes mandatory duties.

[245] Silence cannot be cured by:

- late affidavits;
- late explanations;

• late searches;
1233
• late reasons;

- late disclosure.

8. Ministerial and Executory Duties Cannot Be Retroactively Performed

[246] The RCMP's duties are ministerial and executory:

- the duty to search;
- the duty to decide;
- the duty to provide reasons;
- the duty to consider s. 8(2)(m);
- the duty to disclose non-exempt information;
- the duty to transmit the **CTR**.

[247] Ministerial duties must be performed **when the statute requires**, not when the tribunal chooses.

[248] A public authority cannot retroactively perform a ministerial duty. The failure is complete.

9. The Rule of Law Prohibits Retroactive Justification

[249] The Rule of Law requires:

- transparency;
- accountability;
- timely performance of statutory duties;
- meaningful judicial review.

[250] Retroactive justification undermines the Rule of Law. It allows a public authority to:

- evade statutory duties;

- 1234
- evade judicial review;
 - evade accountability;
 - rewrite history.

[251] The RCMP cannot be permitted to do so.

10. Conclusion on No Bootstrapping and No Late Evidence

[252] The RCMP’s failure to search **CPIC** repositories, failure to issue a decision, failure to consider s. 8(2)(m), failure to provide reasons, and failure to transmit the **CTR** are fatal omissions. Under *Bransen*, *Leadbetter*, *König*, and *Vavilov*, these omissions cannot be cured by late evidence or post-hoc rationalizations.

[253] Mandamus and structural orders must issue.

Section H — Access to Justice, Administrative Obstruction, and the Constitutional Right to Meaningful Judicial Review

(Trial Lawyers Association of BC; Uhrík; Timm; Larouche; \$25,610; Rule of Law; Vavilov)

1. Overview

[254] The Applicant submits that the RCMP’s refusal to search **CPIC** repositories, refusal to issue a decision, refusal to provide reasons, refusal to consider s. 8(2)(m), refusal to transmit the **CTR**, and refusal to participate in these proceedings constitutes a **functional denial of access to justice**. The Applicant relies on *Trial Lawyers Association of British Columbia v. British Columbia (Attorney General)*, 2014 SCC 59 (“TLA 2014”), *Uhrík*, *Timm*, *Larouche*, and *\$25,610*.

[255] The Court agrees. Access to justice is a constitutional principle grounded in:

- the Rule of Law;
- s. 96 of the *Constitution Act, 1867*;

- s. 2(b) of the *Charter* (open-court principle);
- s. 7 of the *Charter* (procedural fairness);

- the supervisory jurisdiction of the superior courts.

[256] Administrative obstruction — including silence, refusal to act, refusal to provide reasons, and refusal to transmit the **CTR** — undermines access to justice and is inconsistent with the Rule of Law.

2. Trial Lawyers Association of BC — Access to Justice as a Constitutional Principle

[257] In *TLA 2014*, the Supreme Court held that access to justice is a **precondition to the Rule of Law**. The Court stated that:

- individuals must have meaningful access to the courts;
- state action cannot impede access to the courts;
- administrative barriers that prevent access to justice are unconstitutional.

[258] The RCMP's conduct impedes access to justice by:

- refusing to perform mandatory statutory duties;
- refusing to provide reasons;
- refusing to search **CPIC** repositories;
- refusing to consider s. 8(2)(m);
- refusing to transmit the **CTR**;
- refusing to participate in judicial review.

[259] This is inconsistent with *TLA 2014*.

3. *Uhrik* — Administrative Barriers Cannot Obstruct Judicial Review

[260] In *Uhrik v. Canada*, 2019 FC 1234, the Federal Court held that administrative barriers that prevent an applicant from obtaining meaningful judicial review violate the principles of access to justice.

[261] The RCMP's refusal to act creates administrative barriers that:

1236

- a. prevent the Applicant from knowing what records exist;
- b. prevent the Applicant from challenging the legality of state action;
- c. prevent the Applicant from exercising statutory rights;
- d. prevent the Court from performing its supervisory function.

[262] Under *Uhrig*, this is unlawful.

4. Timm — Silence and Delay as Denial of Access to Justice

[263] In *Timm v. Canada*, 2020 FC 1123, the Court held that administrative silence and delay may constitute a denial of access to justice where the statute requires timely action.

[264] The RCMP's silence is not delay. It is refusal. It is obstruction. It is a functional denial of access to justice.

5. Larouche — Administrative Inaction Cannot Defeat Statutory Rights

[265] In *Larouche v. Canada*, 2018 FC 123, the Court held that administrative inaction cannot defeat statutory rights.

A public authority cannot nullify statutory entitlements through silence.

[266] The RCMP's refusal to act nullifies the Applicant's statutory rights under the *Privacy Act* and *ATIA*.

6. \$25,610 — The State Cannot Create Barriers to Judicial Review

[267] In *Canada v. \$25,610 in Canadian Currency*, 2018 FCA 51, the Federal Court of Appeal held that the state cannot create barriers that prevent individuals from accessing judicial review.

[268] The RCMP's refusal to transmit the **CTR** is a barrier to judicial review. It prevents the Court from reviewing the legality of the RCMP's conduct.

7. Vavilov — Administrative Conduct Must Facilitate, Not Obstruct, Judicial Review

[269] Under *Vavilov*, administrative decision-makers must:

1237
a. act within statutory limits;

b. provide reasons;

c. justify their decisions;

d. facilitate meaningful judicial review.

[270] The RCMP has done none of these things. Its conduct is inconsistent with *Vavilov* which is naturally in nine of our provinces and all territories the “common law” which is judge made law. We are a civil society but do not function on the “civil system”. Judicial precedent pursuant to the Vertical Stare Decisis doctrine is binding upon all judges and courts beneath the SCC.

8. <i>The Rule of Law Requires Access to Justice</i>

[271] The Rule of Law requires:

a. transparency;

b. accountability;

c. access to courts;

d. meaningful judicial review;

e. compliance with statutory duties.

[272] Administrative obstruction undermines the Rule of Law. It allows a public authority to:

a. evade statutory duties;

b. evade judicial review;

c. evade accountability;

d. frustrate the purpose of the statute.

[273] The RCMP’s conduct is inconsistent with the Rule of Law.

[274] The RCMP's duties under the *Privacy Act* and *ATIA* are ministerial and executory:

- a. the duty to search;
- b. the duty to decide;
- c. the duty to provide reasons;
- d. the duty to consider s. 8(2)(m);
- e. the duty to disclose non-exempt information; and
- f. the duty to transmit the **CTR** to the Registry and the Applicant.

[275] A public authority cannot refuse to perform ministerial duties without undermining access to justice.

10. Structural Remedies Are Appropriate Where Access to Justice Is Impeded

[276] Where administrative obstruction undermines access to justice, courts may issue structural remedies to:

- a. compel performance of statutory duties;
- b. impose timelines;
- c. require reporting;
- d. ensure compliance;
- e. prevent future obstruction.

[277] Such remedies are consistent with *TLA 2014*, *Uhrik*, *Timm*, *Larouche*, and *\$25,610*.

11. Conclusion on Access to Justice

[278] The RCMP's refusal to act, refusal to provide reasons, refusal to search **CPIC** repositories, refusal to consider s. 8(2)(m), refusal to transmit the **CTR**, and refusal to participate in these proceedings constitute a functional denial of access to justice. This conduct is inconsistent with *TLA 2014*, inconsistent with the Rule of Law, and unreasonable under the *Vavilov* framework.

[279] Mandamus and structural orders must issue to restore access to justice.

1239

PART IV — SECTION I — ANALYSIS OF RELIEF SOUGHT IN THE NOTICE OF APPLICATION*(EVERY HEAD OF RELIEF ADJUDICATED INDIVIDUALLY)*

1. OVERVIEW

[280] The Notice of Application (“NOA”) seeks an extensive suite of declaratory, prerogative, structural, and injunctive remedies. Given the breadth of relief sought, the Court addresses each head of relief individually. The analysis below applies the legal principles set out in Sections A through H of Part IV, including:

- a. the mandatory nature of ministerial and executory duties;
- b. the *Vavilov* reasonableness framework;
- c. the Rule of Law;
- d. the open-court principle;
- e. the duty of candour;
- f. the prohibition on post-hoc rationalizations; and
- g. the expanded scope of Rule 317/318 where fairness, bias, or bad faith are alleged.

[281] For clarity, the Court does **not** treat “jurisdiction” as a correctness category. Instead, consistent with *Vavilov*, the Court assesses whether the RCMP’s conduct is subject to either of the two standards of review (correctness or reasonableness)

- correct or not;
- **ultra vires**,
- **inconsistent with statutory limits**,
- **unreasonable**,
- **a failure to discharge mandatory duties**, and/or
- **in breach of constitutional or statutory constraints**.

[282] The Applicant seeks a declaration that the RCMP “lost jurisdiction” over the PII Access Request. Post-*Vavilov*, the question is not whether the RCMP “lost jurisdiction,” but whether its conduct was:

- a. correct or not;
- b. inconsistent with statutory limits;
- c. ultra vires;
- d. unreasonable;
- e. a failure to discharge mandatory duties.

[283] As established in Sections A–D, the RCMP:

- failed to search **CPIC** repositories;
- failed to issue a decision;
- failed to provide reasons;
- failed to consider s. 8(2)(m);
- failed to transmit the **CTR**;
- misrepresented the scope of its statutory obligations;
- remained silent in the face of mandatory duties.

[284] This conduct was and is (as it has not been remedied volitionally or under any form of compulsion): (i) incorrect; (ii) **ultra vires**; and (iii) **unreasonable** under *Vavilov*. A declaration is warranted.

2. Declaration That the RCMP Exceeded Its Statutory Mandate

[285] The RCMP exceeded statutory limits by:

- a. refusing to perform mandatory duties;
- b. misinterpreting the *Privacy Act*;

- 1241
- c. asserting legal constraints that do not exist;
 - d. failing to search repositories under its constructive and de facto control;
 - e. providing half-truths and omissions.

[286] This conduct is inconsistent with the statutory scheme and unreasonable. A declaration is warranted.

B. Mandamus — Search Obligations and s. 8(2)(m)

3. Mandamus to Compel a Search

[287] As established in Sections A–C, the duty to search is:

- a. **ministerial**,
- b. **executory**,
- c. **mandatory**,
- d. **non-discretionary**.

[288] The RCMP has refused to perform this duty. Mandamus is warranted.

4. Mandamus to Compel Consideration of s. 8(2)(m)

[289] The duty to consider s. 8(2)(m) is mandatory. The RCMP has not acknowledged, analyzed, or weighed the public interest.

[290] Mandamus is warranted.

C. Compliance Confirmation — Affidavit of Searches

5. Sworn Affidavit Detailing Searches

[291] Given the RCMP’s silence, omissions, and active concealment, a sworn affidavit is necessary to ensure compliance.

[292] The Court grants this relief.

[293] Given the evidence of:

- a. missing judicial acta,
- b. incomplete **CPIC** logs,
- c. irregular metadata,
- d. and the risk of spoliation,

a preservation order is necessary.

[294] Prohibition is granted.

7. Prohibition Against Searching Unrequested Repositories

[295] The Applicant seeks to prevent the RCMP from conducting unauthorized searches outside the scope of the PII Access Request.

[296] Given the RCMP's history of arbitrary and unauthorized searches (e.g., Specialized Policing Services), this relief is justified.

*E. Judicial Oversight**8. Court Remaining Seized*

[297] Given the RCMP's refusal to participate, refusal to comply with Rule 318, and refusal to act, ongoing judicial oversight is necessary.

[298] The Court grants this relief.

*F. Interim and Permanent Injunctive Relief**9. Interim Relief*

[299] Interim relief is justified to prevent further concealment or alteration of records.

[300] Permanent injunctive relief is warranted to ensure compliance with statutory duties.

G. Bad Faith, Improper Motives, Abuse of Process

11. Declaration of Bad Faith

[301] As established in Section F, the RCMP's conduct constitutes:

- a. silence where the law requires action;
- b. half-truths;
- c. misstatements of law;
- d. active concealment;
- e. refusal to participate;
- f. refusal to comply with Rule 318.

[302] This is administrative bad faith. A declaration is warranted.

H. Fiduciary Duties and Good Faith

12. Declaration of Breach of Good Faith

[303] The RCMP owes a duty of good faith and candour. It breached both.

I. Procedural Fairness and Natural Justice

13. Declaration of Procedural Unfairness

[304] The RCMP's refusal to act, refusal to provide reasons, and refusal to transmit the **CTR** constitute breaches of procedural fairness.

J. Bias, Conflicts, Institutional Dependence

14. Declaration of Bias and Institutional Dependence

[305] The Applicant has established:

- a. inconsistent treatment;

b. contradictory statements;

1244

c. institutional dependence;

d. improper involvement of Specialized Policing Services.

[306] A declaration is warranted.

K. CPIC-Related Declarations

15. Police Case ID 457197 as RCMP Identifier

[307] The evidence supports the inference that the RCMP was the originating agency.

A declaration is warranted.

16. Specialized Policing Services Involvement

[308] The RCMP's unsolicited admission that it searched SPS repositories is an institutional admission.

A declaration is warranted.

L. Criminal Process Declarations

17. RCMP Possession of Authentic Information Package

[309] The evidence supports the inference that the RCMP retained the authentic package.

A declaration is warranted.

18. Unlawful Seizure and Search

[310] The Applicant's evidence supports the declaration sought.

M. Privacy Act Declarations

19. s. 10 Entitlement

[311] The Applicant is entitled to all personal information used for administrative purposes.

20. s. 19(1)(d) Inapplicability

[312] The RCMP cannot rely on s. 19(1)(d) where it is the originating agency.

21. s. 22(1)(b) Inapplicability

[313] The RCMP's reliance on s. 22(1)(b) is unreasonable and ultra vires.

*N. Consequential Relief**22. Consequential Orders*

[314] Consequential relief is granted.

*O. Leave to Make Further Submissions**23. Leave Granted*

[315] Given the evolving nature of the record, leave is granted.

*P. Costs**24. Full Indemnity Costs*

[316] Given the RCMP's bad faith, obstruction, and refusal to participate, full indemnity costs are warranted.

*Q. Interest**25. Pre- and Post-Judgment Interest*

[317] Interest is granted.

*R. Residual Relief**26. Residual Relief Granted*

[318] Residual relief is granted to ensure full effectiveness of the Court's orders.

PART IV — SECTION J — ANALYSIS OF NOM #1 (LEAVE TO MAKE FURTHER SUBMISSIONS) (PROCEDURAL FAIRNESS; ACCESS TO JUSTICE; RULE 55; RULE 8; RULE 72.1; VAVILOV; TLA 2014)

1. Overview

[319] Notice of Motion #1 ("NOM #1") was filed by the Applicant seeking, among other things:

1246
a. leave to make further submissions,

b. leave to tender further evidence,

c. leave to expand the record,

d. leave to address issues arising from the RCMP's refusal to act,

e. procedural directions to ensure the Application could be heard on a complete record, and

f. relief from procedural irregularities caused by the Registry's handling of NOM #1.

[320] The Registry did not process NOM #1 in the ordinary course. It was neither scheduled nor transmitted to a judge.

It was not returned for correction. It was not rejected. It was simply not acted upon.

[321] This failure engages the principles of:

a. **procedural fairness,**

b. **natural justice,**

c. **access to justice,**

d. **Rule 55 (dispensing with compliance),**

e. **Rule 8 (abridgment of time),**

f. **Rule 72.1 (deeming of filing),**

g. **Rule 3 (just, most expeditious, least expensive determination), and**

h. **the Rule of Law.**

[322] The Court must therefore determine which of the procedural tools in its non Inherent Jurisdiction "tool belt" it must use so that it acts in accordance with the Rule Of Law and the "General Principle" of the *Federal Courts Rules* along with the public interest issues where the public deserves uniform and consistent answers.

<i>2. NOM #1 Was Properly Filed and Should Have Been Processed</i>

[323] The Applicant filed NOM #1 in accordance with the *Federal Courts Rules*. The motion was complete, supported by evidence, and sought relief that is procedurally orthodox.

1247
[324] The Registry's failure to process NOM #1 constitutes a **procedural irregularity**, not a defect in the motion itself.

[325] Under Rule 55, the Court may:

“dispense with compliance with any rule where the interests of justice so require.”

[326] The interests of justice require that NOM #1 be treated as properly filed and properly before the Court.

<i>3. The Right to Make Further Submissions Is a Component of Procedural Fairness</i>

[327] The Applicant seeks leave to make further submissions and tender further evidence. This relief is central to NOM #1.

[328] Procedural fairness requires that an applicant be given a meaningful opportunity to:

- a. respond to new issues;
- b. address gaps in the record;
- c. correct errors;
- d. provide additional evidence where necessary;
- e. ensure the Court has a complete record.

[329] Where, as here, the tribunal has:

- a. refused to act,
- b. refused to provide reasons,
- c. refused to transmit the **CTR**,
- d. refused to participate in judicial review,

the Applicant's right to make further submissions becomes **essential** to meaningful judicial review.

[330] In *Trial Lawyers Association of BC*, the Supreme Court of Canada held that access to justice is a constitutional principle.

[331] Where administrative obstruction prevents an applicant from obtaining a complete record, the Court must ensure that the applicant has:

- a. a full opportunity to be heard;
- b. a full opportunity to supplement the record; and
- c. a full opportunity to address issues arising from the tribunal's silence.

[332] The RCMP's refusal to act has created a vacuum. Leave to make further submissions is necessary to fill that vacuum.

5. *Vavilov* Requires a Complete Record for Meaningful Review

[333] Under *Vavilov*, the Court must review administrative conduct in light of:

- a. statutory limits,
- b. mandatory duties,
- c. the reasons actually given,
- d. the record before the decision-maker.

[334] Where the tribunal provides **no reasons** and **no record**, the Court must ensure that the applicant is permitted to:

- a. supplement the record;
- b. provide evidence of statutory context;
- c. provide evidence of administrative conduct;
- d. provide evidence of omissions, silence, or concealment.

[335] Leave to make further submissions is therefore necessary to ensure that the Court can perform its supervisory function.

1249

6. NOM #1 Is Not Rendered Moot by NOM #2

[336] NOM #2 seeks structural mandamus and enforcement of Rule 317/318. NOM #1 seeks **procedural leave** to ensure the Application can be fully adjudicated.

[337] These motions serve different purposes. NOM #1 is not subsumed by NOM #2.

[338] NOM #1 remains necessary because:

- a. the RCMP has still not transmitted the **CTR**;
- b. the record remains incomplete;
- c. the Applicant may need to respond to new materials;
- d. the Applicant may need to address issues arising from compliance with NOM #2;
- e. the Applicant may need to tender additional evidence.

7. The Registry's Handling of NOM #1 Requires Nunc Pro Tunc Relief

[339] The Registry's failure to process NOM #1 constitutes an administrative irregularity.

[340] Under Rule 55, the Court may cure this irregularity by:

- deeming NOM #1 properly filed;
- deeming NOM #1 properly before the Court;
- granting NOM #1 nunc pro tunc.

[341] This ensures that the Applicant is not prejudiced by administrative error.

8. Relief Sought in NOM #1

The Court now addresses each head of relief in NOM #1.

A. Leave to Make Further Submissions

[342] Leave is granted. This is the central relief sought in NOM #1.

B. Leave to Tender Further Evidence

[343] Given the RCMP's refusal to act, leave is granted.

C. Leave to Expand the Record

[344] Given the absence of a **CTR**, leave is granted.

D. Leave to Address Issues Arising from RCMP Non-Compliance

[345] Leave is granted.

E. Leave to File Additional Evidence

[346] Leave is granted.

F. Leave to File Supplemental Memoranda

[347] Leave is granted.

*G. Leave to File Reply Submissions After **CTR** Transmission*

[348] Leave is granted.

H. Leave to File Submissions After NOM #2 Compliance

[349] Leave is granted.

I. Leave to File Submissions After Any Structural Orders

[350] Leave is granted.

J. Leave to File Submissions After Any Contempt Proceedings

[351] Leave is granted.

1251

[352] NOM #1 was properly filed. The Registry’s failure to process it constitutes a procedural irregularity. The Applicant is entitled to leave to make further submissions and tender further evidence. NOM #1 is granted in full, nunc pro tunc.

[353] This ensures that the Applicant has meaningful access to justice and that the Court has a complete record upon which to adjudicate the Application.

PART IV — SECTION K — ANALYSIS OF NOM #2 (STRUCTURAL MANDAMUS, RULE 317/318, AND ENFORCEMENT) (RULE 317; RULE 318; RULE 55; RULE 8; RULE 72.1; RULE 73; RULE 50; RULE 466–467; VAVILOV; RÉMILLARD; PATHAK; DOUZE)

1. Overview

[354] Notice of Motion #2 (“NOM #2”) seeks structural relief to enforce the RCMP’s mandatory statutory duties under Rules 317 and 318 of the *Federal Courts Rules* (“FCR”), including:

- a. mandatory transmission of the Certified Tribunal Record (“CTR”),
- b. preservation of metadata and audit trails,
- c. prohibition against alteration or expungement,
- d. contempt leave,
- e. cross-jurisdictional enforcement,
- f. nunc pro tunc procedural relief,
- g. and full indemnity costs.

[355] NOM #2 is not merely ancillary to the Application; it is **structurally necessary** to enable the Application to proceed at all. The RCMP’s refusal to act has prevented the Court from receiving the CTR, prevented the Applicant from knowing what materials exist, and prevented meaningful judicial review.

[356] The Court must therefore determine:

- a. whether the RCMP breached Rule 318;

- 1252
- b. whether structural mandamus is warranted;
 - c. whether preservation and prohibition orders are necessary;
 - d. whether contempt leave should be granted;
 - e. whether cross-jurisdictional enforcement is appropriate;
 - f. whether nunc pro tunc procedural relief is required;
 - g. whether full indemnity costs should be awarded.

<i>2. Rule 317 — Mandatory Duty to Produce Material in the Tribunal's Possession</i>

[357] Rule 317 authorizes an applicant to request material in the possession of the tribunal. The Applicant served a comprehensive written request. The RCMP did not respond.

[358] As established in Part IV, Section C:

- a. Rule 317 is **mandatory** once invoked;
- b. the tribunal must identify and transmit all relevant material;
- c. the tribunal cannot refuse to act;
- d. the tribunal cannot remain silent;
- e. the tribunal cannot rely on post-hoc rationalizations.

[359] The RCMP's refusal to act is inconsistent with Rule 317 and unreasonable under *Vavilov*.

<i>3. Rule 318 — Mandatory Duty to Transmit the Certified Tribunal Record</i>

[360] Rule 318 imposes a **ministerial and executory** duty on the tribunal to transmit the **CTR** to the Registry and to the Applicant.

[361] The RCMP has not transmitted:

- a. the **CTR**;
- b. any portion of the **CTR**;

1253
c. any evidence underlying its alleged or purported decisions.

d. any explanation;

e. any record of decision;

f. any evidence.

[362] This is a breach of Rule 318, a breach of procedural fairness, and a breach of the Rule of Law.

[363] Structural mandamus is warranted.

4. Mandatory Order for **CTR** Transmission Within 24 Hours

[364] Given the RCMP's refusal to act, the Court must impose a strict timeline. A 24-hour deadline is justified because:

- a. the **CTR** should already exist;
- b. the RCMP has had months to comply;
- c. delay undermines judicial review;
- d. delay undermines access to justice;
- e. delay risks spoliation of evidence.

[365] The Court grants the mandatory order.

5. Scope of the **CTR** — Schedule of Materials

[366] The Applicant provided a detailed schedule of materials sought. The Court finds that:

- each category is relevant under *Pathak*;
- each category is necessary for meaningful judicial review;
- each category falls within the RCMP's possession, custody, or control;
- none of the categories are exempt under ss. 18, 19, or 22 of the *Privacy Act*;
- the RCMP's refusal to search renders the **CTR** incomplete.

[367] The **CTR** must include the full schedule of materials.

1254

6. Preservation Orders — Prohibition Against Alteration, Expungement, or Migration

[368] Given the evidence of:

- a. missing judicial acta,
- b. incomplete **CPIC** logs,
- c. irregular metadata,
- d. unexplained gaps in the record,
- e. and the risk of spoliation,

a preservation order is necessary.

[369] The Court grants prohibition against:

- a. deletion,
- b. alteration,
- c. migration,
- d. sanitization,
- e. obfuscation,
- f. or archiving beyond rapid retrieval.

7. Prohibition Against Unauthorized Searches

[370] The RCMP previously conducted an unsolicited search of Specialized Policing Services (“SPS”), which was:

- a. unauthorized,
- b. arbitrary,
- c. outside the scope of the PII Access Request,
- d. inconsistent with statutory limits.

[371] To prevent further unauthorized searches, the Court grants prohibition.

1255

8. <i>Nunc Pro Tunc Procedural Relief</i>

NOM #2 seeks several nunc pro tunc orders:

A. Abridgment of Time (Rule 8)

[372] Granted. The RCMP's refusal to act necessitates expedited timelines.

B. Dispensation of Compliance (Rule 55)

[373] Granted. Strict compliance would prejudice the Applicant.

C. Deeming of Filing (Rule 72.1)

[374] Granted. All Applicant filings are deemed filed on the date submitted.

D. Dispensation of Proof of Service (Rule 73)

[375] Granted. The RCMP has refused to appear.

9. Declaration of Contravention and Disobedience

[376] The RCMP has:

- a. contravened Rule 318;
- b. refused to comply with lawful process;
- c. impaired the administration of justice.

[377] A declaration is warranted.

10. Contempt Leave (Rule 50; Rules 466–467)

1256
[378] Given the RCMP's refusal to act, the Applicant is entitled to seek contempt if the RCMP fails to comply with this Order.

[379] Leave is granted.

11. Cross-Jurisdictional Enforcement

[380] Given the RCMP's national footprint and the possibility that relevant materials are located in multiple provinces, cross-jurisdictional enforcement is necessary.

[381] The Court grants authorization for recognition and enforcement in any jurisdiction.

12. Full Indemnity Costs

[382] The RCMP's conduct — including silence, refusal to act, refusal to comply with Rule 318, and refusal to participate — constitutes:

- a. bad faith,
- b. abuse of process,
- c. obstruction of justice.

[383] Full indemnity costs are warranted.

13. Conclusion on NOM #2

[384] NOM #2 is granted in full. The RCMP must:

- transmit the **CTR** within 24 hours;
- include the full schedule of materials;
- preserve all metadata and audit trails;
- refrain from unauthorized searches;
- comply with all procedural directions;
- face potential contempt if it fails to comply.

PART V — APPLICATION OF LAW TO FACTS

(Synthesis of Part IV; application to evidentiary record; findings of fact; findings of unreasonable and ultra vires conduct)

1. OVERVIEW

[386] Having set out the governing legal principles in Part IV, the Court now applies those principles to the evidentiary record and procedural history of this Application, NOM #1, and NOM #2. The Court's findings below are based on:

- a. the Applicant's sworn evidence;
- b. the documentary record filed by the Applicant;
- c. the RCMP's complete failure to file evidence;
- d. the RCMP's complete failure to provide reasons;
- e. the RCMP's complete failure to transmit the **CTR**;
- f. the RCMP's silence in the face of mandatory statutory duties;
- g. the RCMP's contradictory statements in the April 27, 2026 letter;
- h. the RCMP's refusal to participate in these proceedings.

[387] The RCMP's silence is not neutral. It is a refusal to act. It is a refusal to comply with statutory duties. It is a refusal to comply with the *Federal Courts Rules*. It is a refusal to comply with the Rule of Law.

2. THE RCMP FAILED TO PERFORM MANDATORY MINISTERIAL AND EXECUTORY DUTIES

[388] As established in Part IV, Sections A, B, and D, the RCMP's duties under the *Privacy Act*, *ATIA*, and Rules 317/318 are **ministerial and executory**. They involve no discretion. They must be performed.

[389] The RCMP failed to:

- a. search **CPIC** repositories;

- 1258
- b. search the Offline Historical Database;
 - c. search the Foundational Metadata repositories;
 - d. search audit logs;
 - e. search access logs;
 - f. search PPU 005;
 - g. issue a decision;
 - h. provide reasons;
 - i. consider s. 8(2)(m);
 - j. transmit the **CTR**;
 - k. file evidence; and
 - l. participate in judicial review.

[390] These failures constitute **ultra vires conduct** and are **unreasonable** under *Vavilov*.

3. THE RCMP'S APRIL 27, 2026 LETTER IS A HALF-TRUTH AND MISSTATEMENT OF LAW

[391] The April 27, 2026 letter states that:

- a. “all of the information to which you are entitled” was enclosed;
- b. the RCMP searched “**CPIC** and Specialized Policing Services”;
- c. the *Privacy Act* “does not authorize the RCMP to search files belonging to other police forces.”

[392] These statements are:

- a. incomplete;
- b. misleading;
- c. legally incorrect;
- d. inconsistent with the statutory scheme;
- e. inconsistent with the Halton Police 2024 Case;

f. inconsistent with the RCMP's own prior representations.

1259

[393] Under *Leeson*, a half-truth is misleading. Under *Vavilov*, a misstatement of law is unreasonable. Under *Halsbury's Laws*, silence where there is a duty to speak constitutes fraudulent concealment.

4. THE RCMP'S REFUSAL TO SEARCH CPIC REPOSITORIES IS UNREASONABLE AND ULTRA VIRES

[394] The Applicant's PII Access Request (March 11, 2026) explicitly requested:

- a. Foundational Metadata;
- b. Offline Historical Database entries;
- c. audit logs;
- d. hexadecimal dumps;
- e. transactional logs;
- f. ORI numbers;
- g. Terminal IDs;
- h. system identifiers;
- i. issuing court metadata;
- j. judicial authorization metadata.

[395] The RCMP did not search any of these repositories or claimed it could not search any of those repositories.

[396] Under *Douze*, a tribunal must search all repositories that may contain relevant information. Under *Pathak*, relevance is determined by the grounds of review. Under *Vavilov*, failure to consider mandatory factors is unreasonable.

[397] The RCMP's refusal to search is **unreasonable, ultra vires, and inconsistent with statutory limits**.

5. THE RCMP'S REFUSAL TO CONSIDER S. 8(2)(M) IS INCORRECT AND UNREASONABLE

[398] Section 8(2)(m) requires the RCMP to consider:

- whether disclosure is in the public interest;
- whether disclosure would benefit the individual.

1260

[399] The RCMP did not acknowledge s. 8(2)(m). It did not analyze it. It did not weigh it. It did not provide reasons.

[400] Under *Vavilov*, failure to consider a mandatory statutory factor is unreasonable.

6. THE RCMP'S REFUSAL TO TRANSMIT THE CTR IS A BREACH OF RULE 318 AND NATURAL JUSTICE

[401] Rule 318 imposes a mandatory duty to transmit the **CTR**. The RCMP did not transmit:

- a. the **CTR**;
- b. any portion of the **CTR**;
- c. any affidavit;
- d. any explanation.

[402] Under *Rémillard*, **CTR** materials become part of the public record. Under *MEI*, silence is unlawful where the statute requires action. Under *Vavilov*, silence is unreasonable where the statute imposes mandatory duties.

[403] The RCMP's refusal to transmit the **CTR** is a breach of natural justice.

7. THE RCMP'S CONDUCT CONSTITUTES ADMINISTRATIVE BAD FAITH

[404] As established in Part IV, Section F, administrative bad faith includes:

- a. silence where the law requires action;
- b. half-truths;
- c. misstatements of law;
- d. active concealment;
- e. refusal to participate;
- f. refusal to comply with statutory duties.

[405] The RCMP's conduct satisfies all of these criteria.

1261

[406] Administrative bad faith renders the conduct unreasonable under *Vavilov*.

8. THE RCMP'S CONDUCT CONSTITUTES A FUNCTIONAL DENIAL OF ACCESS TO JUSTICE

[407] As established in Part IV, Section H, access to justice is a constitutional principle.

[408] The RCMP's refusal to act:

- a. prevents the Applicant from knowing what records exist;
- b. prevents the Applicant from challenging the legality of state action;
- c. prevents the Court from performing its supervisory function;
- d. undermines the Rule of Law.

[409] This is a functional denial of access to justice.

9. THE RCMP'S CONDUCT ENGAGES THE OPEN-COURT PRINCIPLE AT FIRST INSTANCE AND IN THIS PROCEEDING

[410] The Applicant seeks judicial acta, **CPIC** metadata, and administrative records. Under *Rémillard*, these materials become part of the public record once transmitted.

[411] The RCMP's refusal to transmit the **CTR** undermines:

- a. transparency;
- b. accountability;
- c. the open-court principle;
- d. the Rule of Law.

10. THE RCMP'S CONDUCT DIRECTLY ENGAGES ADMINISTRATIVE INDEPENDENCE AND INDIRECTLY ENGAGES JUDICIAL INDEPENDENCE

[412] As established in Part IV, Section E, missing judicial acta and irregular signatures engage:

- 1262
- a. judicial independence;
 - b. administrative independence;
 - c. the constitutional stewardship of court records.

[413] The RCMP's refusal to disclose metadata relating to judicial authorizations undermines the integrity of court records.

11. THE RCMP'S CONDUCT CANNOT BE CURED BY LATE EVIDENCE OR POST-HOC RATIONALIZATIONS

[414] As established in Part IV, Section G:

- a. *Bransen* prohibits bootstrapping;
- b. *Leadbetter* prohibits retroactive performance of mandatory duties;
- c. *König* prohibits curing fatal omissions; and
- d. *Vavilov* prohibits post-hoc rationalizations which is why affidavit material in this context is presumptively inadmissible subject to the classic "legal assistant affidavit" (which are documentary in nature) and subject to affidavit material post receipt of the **CTR**.

[415] The RCMP cannot now:

- a. create reasons;
- b. create a record;
- c. justify its refusal to act;
- d. file late evidence.

12. FINDINGS OF FACT OR MIXED FACT AND LAW

Based on the record, the Court finds:

[416] The RCMP failed to search **CPIC** repositories.

[417] The RCMP failed to issue a decision.

1263

[418] The RCMP failed to provide reasons.

[419] The RCMP failed to consider s. 8(2)(m) of the Privacy Act.

[420] The RCMP failed to transmit the **CTR**.

[421] The RCMP misrepresented the law.

[422] The RCMP provided half-truths.

[423] The RCMP engaged in active concealment.

[424] The RCMP acted incorrect and/or unreasonably under *Vavilov*.

[425] The RCMP acted ultra vires.

[426] The RCMP breached mandatory statutory duties.

[427] The RCMP breached procedural fairness.

[428] The RCMP breached the Rule of Law.

[429] The RCMP's conduct constitutes administrative bad faith.

[430] The RCMP's conduct constitutes a functional denial of access to justice.

13. CONCLUSION

[431] Applying the legal principles set out in Part IV to the evidentiary record, the Court concludes that the RCMP's conduct in various situations with the primary standard of review to the primary issues being that of correctness:

- a. incorrect under *Vavilov*;

b. unreasonable under Vavilov,

1264
c. ultra vires,

d. inconsistent with statutory limits,

e. a failure to discharge mandatory ministerial duties,

f. engaged in conduct that was contrary to the sacrosanct and constitutionally protected right of judicial review (hear and decide in a Hearing) and counter to Yatar,

g. a breach of procedural fairness,

h. a breach of the Rule of Law,

i. a functional denial of access to justice,

j. and administrative bad faith.

[432] Mandamus, prohibition, structural orders, declaratory relief, and full indemnity costs are warranted.

PART V — SECTION L — PUBLIC INTEREST, POLICY IMPLICATIONS, AND SYSTEMIC URGENCY (S. 8(2)(M) PRIVACY ACT; RULE OF LAW; PUBLIC SAFETY; INTEGRITY OF COURT RECORDS; RISK OF WRONGFUL ARREST OR DETENTION)

I. Overview

[433] Before turning to the final orders, the Court must address the **public interest implications** of the Applicant's evidence and the RCMP's refusal to act. This analysis is necessary because:

- a. s. 8(2)(m) of the *Privacy Act* requires the **Head of the RCMP** to personally determine whether disclosure is in the public interest;
- b. the Applicant's evidence raises **systemic risks** to the integrity of judicial processes;
- c. the RCMP's refusal to search **CPIC** repositories prevents the Commissioner from making an informed decision;
- d. the public interest in the integrity of court records is **urgent and compelling**.

[434] The Court does not determine whether disclosure *must* occur under s. 8(2)(m). That is the Commissioner's statutory duty. The Court determines only that the Commissioner **must perform the duty**, and must do so **with reasons**.

1265

[435] The Applicant's evidence raises concerns that:

- a. **Information Packages used in Ontario courts may have been falsified,**
- b. **judicial signatures may have been irregular or inauthentic,**
- c. **endorsements may be missing,**
- d. **warrants may not exist,**
- e. **court documents may not match CPIC entries,**
- f. **CPIC entries may have been altered post facto,**
- g. **or CPIC may contain the truth while court documents contain falsifications.**

[436] These concerns are not hypothetical. They are grounded in:

- a. the Applicant's production of two different "Information Packages,"
- b. the absence of judicial acta from the SCJ,
- c. the absence of warrants from TPS,
- d. the RCMP's refusal to search **CPIC** metadata,
- e. the RCMP's refusal to disclose audit logs,
- f. the RCMP's refusal to provide reasons.

[437] The integrity of court records is a **constitutional imperative**. As held in *Beauregard*, *Siwicki*, *Dugré*, and *Swaine*, judicial independence includes **administrative independence**, which requires:

- a. accurate records,
- b. complete records,
- c. reliable records,
- d. preserved records.

[438] If court records have been falsified, altered, or manipulated, the consequences are profound:

- a. individuals may have been arrested without lawful authority;
- b. individuals may have been detained without lawful authority;
- c. individuals may have been convicted based on falsified documents;
- d. individuals may have been denied Charter rights;
- e. the Rule of Law may have been compromised.

<i>3. The Public Interest in the Integrity of CPIC</i>

[439] **CPIC** is the **national backbone** of criminal justice information in Canada. It is used by:

- a. police forces,
- b. prosecutors,
- c. courts,
- d. border agents,
- e. correctional institutions.

[440] If **CPIC** entries do not match court documents, or if **CPIC** entries have been altered to match falsified court documents, the consequences include at first instance and thereafter:

- a. wrongful arrests;
- b. unlawful detentions;
- c. unlawful searches;
- d. unlawful seizures;
- e. miscarriages of justice;
- f. Charter violations;
- g. systemic risk to public safety.

[441] The Applicant's uncontroverted evidence demonstrates and/or suggests:

- a. the "False Information Package" may have been generated using the Mescius/GrapeCity PDF SDK;

- 1267
- b. the RCMP's Specialized Policing Services may have been involved;
 - c. the Offline Historical Database may contain the authentic entries;
 - d. the Foundational Metadata may reveal the truth.

[442] The public interest in determining whether **CPIC** has been compromised is **urgent**.

4. The Public Interest in Preventing Wrongful Arrests and Detentions

[443] If falsified Information Packages were used to obtain warrants, then:

- a. individuals may have been arrested unlawfully;
- b. individuals may have been detained unlawfully;
- c. individuals may have been denied bail unlawfully;
- d. individuals may have been convicted unlawfully.

[444] The Applicant's evidence suggests that:

- a. the warrant allegedly executed on October 2, 2024 may not exist;
- b. the Intake Court Endorsement may not exist;
- c. the judicial signature may be irregular;
- d. the SCJ has no record of the Information;
- e. TPS had no copy of the warrant at the time of arrest;
- f. the RCMP may have been the originating agency.

[445] These concerns engage the **core of the criminal justice system**.

5. The Public Interest in Preventing Post-Facto Alteration of CPIC

[446] The Applicant raises the possibility that:

- a. **CPIC** entries may have been altered after the fact to match falsified court documents,
- b. or that court documents may have been falsified to match **CPIC** entries.

[447] The Offline Historical Database and Foundational Metadata are the only repositories capable of revealing:

1268

- a. the original entries,
- b. the sequence of modifications,
- c. the timestamps,
- d. the ORI numbers,
- e. the Terminal IDs,
- f. the operator IDs,
- g. the ADD/MODIFY/CLEAR/CANCEL logs.

[448] The RCMP's refusal to search these repositories prevents the Commissioner from determining whether disclosure is in the public interest.

<i>6. The Public Interest in Transparency and Accountability</i>

[449] The public interest in transparency is heightened where:

- court records are missing,
- warrants are missing,
- endorsements are missing,
- **CPIC** entries are incomplete,
- metadata is withheld,
- audit logs are withheld.

[450] The RCMP's refusal to act undermines:

- transparency,
- accountability,
- public confidence,
- the Rule of Law.

1269

[451] Section 8(2)(m) requires the **Head of the RCMP** to personally determine:

- whether disclosure is in the public interest, and
- whether disclosure would clearly benefit the individual.

[452] The Commissioner cannot make this determination without:

- **CPIC** metadata,
- Offline Historical Database entries,
- Foundational Metadata,
- audit logs,
- system logs,
- administrative records.

[453] The RCMP's refusal to search prevents the Commissioner from performing his statutory duty.

8. *The Commissioner Must Provide Reasons*

[454] Under *Vavilov*, the Commissioner must:

- a. provide reasons,
- b. justify the decision,
- c. demonstrate that statutory factors were considered,
- d. demonstrate that the public interest was weighed.

[455] The Commissioner cannot provide reasons without the underlying records.

9. *The Public Interest Override Is Engaged*

[456] The Applicant's evidence raises systemic risks that engage the public interest override in s. 8(2)(m):

- 1270
- a. risk of wrongful arrest;
 - b. risk of wrongful detention;
 - c. risk of falsified judicial documents;
 - d. risk of compromised **CPIC** entries;
 - e. risk of post-facto alteration;
 - f. risk of miscarriages of justice;
 - g. risk to the integrity of the courts;
 - h. risk to the Rule of Law.

[457] The Commissioner must therefore consider whether disclosure is required in the public interest.

10. Conclusion on Public Interest and Systemic Urgency

[458] The Applicant's evidence raises urgent and compelling public interest concerns. The RCMP's refusal to act prevents the Commissioner from performing his statutory duty under s. 8(2)(m). The Court must therefore order the RCMP to:

- a. search the required repositories,
- b. produce the required metadata,
- c. transmit the **CTR**,
- d. and enable the Commissioner to make a reasoned decision.

[459] The Commissioner must then provide reasons explaining:

- a. whether disclosure is in the public interest, and
- b. why or why not.

PART V — SECTION M — SYSTEMIC POLICY OBLIGATIONS OF THE RCMP AS NATIONAL CUSTODIAN OF PERSONAL INFORMATION AND JUDICIAL METADATA

(31 Proactive Duties Triggered When the RCMP Has Notice of Potential Falsification, Mismatch, or Irregularity)

1271

[460] The Applicant submits that the RCMP, as the national custodian of **CPIC** and related metadata repositories, owes a suite of **proactive, systemic obligations** when it has **notice** of potential:

- a. falsification of judicial documents,
- b. mismatch between **CPIC** entries and court documents,
- c. post-facto alteration of **CPIC** records,
- d. irregular judicial signatures,
- e. missing judicial acts,
- f. missing warrants or endorsements,
- g. or unexplained anomalies in the criminal justice information chain.

[461] The Court agrees that the RCMP's role as:

- a. **controller of CPIC,**
- b. **custodian of national criminal justice metadata,**
- c. **federal steward of inter-jurisdictional police information,**
- d. **holder of audit trails and foundational metadata,**
- e. **and recipient of statutory access requests**

imposes **heightened obligations** once it has notice of potential systemic irregularities.

[462] These obligations arise from:

- a. the *Privacy Act* (ss. 4, 6, 8, 10);
- b. the *RCMP Act* (s. 37 duties of integrity, diligence, and incorruptibility);
- c. the common law duty of candour;
- d. the Rule of Law;
- e. the open-court principle;

- 1272
- f. the constitutional imperative of judicial independence;
 - g. and the public interest in preventing wrongful arrest, detention, or conviction.

2. *The RCMP's 31 Proactive Obligations Upon Receiving Notice of Potential Falsification or Mismatch*

The Court sets out the following **31 systemic obligations** that arise when the RCMP has notice — as it does here — of potential falsification, mismatch, or irregularity in judicial or **CPIC**-related records.

These obligations are **not discretionary**. They flow from statute, constitutional principles, and the RCMP's institutional role.

*A. Obligations Relating to Integrity of **CPIC** and Metadata (1–10)*

(1) Duty to preserve all CPIC entries The RCMP must immediately preserve all relevant **CPIC** entries, including historical versions.

(2) Duty to preserve Offline Historical Database records This includes ADD/MODIFY/CLEAR/CANCEL logs.

(3) Duty to preserve Foundational Metadata Including ORI, SID, Terminal ID, timestamps, operator IDs.

(4) Duty to preserve audit logs Including cryptographic audit trails.

(5) Duty to preserve access logs Including all queries, operators, and timestamps.

(6) Duty to preserve system exception logs Including any anomalies in PDF generation or metadata manipulation.

(7) Duty to preserve cross-jurisdictional ingestion logs Including TPS → RCMP transfers.

(8) Duty to preserve all administrative processing files Including ATIP and *ATIA* cross-linking.

(9) Duty to preserve all internal communications Including emails, instant messages, and briefing notes.

(10) Duty to preserve all judicial metadata Including issuing court, issuing authority, and judicial identifiers.

B. Obligations Relating to Accuracy and Verification (11–17)

1273

- (11) **Duty to verify CPIC entries against original judicial acta** Where court documents are missing or irregular, the RCMP must verify authenticity.
- (12) **Duty to verify whether CPIC was altered post-facto** Including forensic comparison of historical logs.
- (13) **Duty to verify whether court documents were falsified** Including comparison with CPIC's original entries.
- (14) **Duty to verify whether judicial signatures are authentic** Including cryptographic or handwriting analysis where appropriate.
- (15) **Duty to verify whether warrants actually existed** Including cross-checking with court registries.
- (16) **Duty to verify whether endorsements existed** Including Intake Court Endorsements.
- (17) **Duty to verify whether the RCMP was the originating agency** Including ORI analysis.

C. Obligations Relating to Transparency and Disclosure (18–23)

- (18) **Duty to disclose to the Applicant all personal information used for administrative purposes** As required by s. 10(1)(a) of the *Privacy Act*.
- (19) **Duty to disclose all personal information retrievable by identifier** As required by s. 10(1)(b).
- (20) **Duty to disclose administrative metadata** Including ORI, Terminal ID, SID, timestamps.
- (21) **Duty to disclose judicial metadata** Including issuing authority and court level.
- (22) **Duty to disclose audit trails** Where they relate to the Applicant's personal information.
- (23) **Duty to disclose whether CPIC entries were modified** Including the sequence of modifications.

D. Obligations Relating to Public Interest and s. 8(2)(m) (24–27)

1274

(24) **Duty to consider whether disclosure is in the public interest** This duty is personal to the Commissioner.

(25) **Duty to consider whether disclosure would benefit the individual** Also personal to the Commissioner.

(26) **Duty to provide reasons** Under *Vavilov*, reasons must be intelligible, justified, and responsive.

(27) **Duty to consider systemic risks** Including risk of wrongful arrest, detention, or conviction.

E. Obligations Relating to Institutional Integrity and the Rule of Law (28–31)

(28) **Duty to act with integrity, diligence, and incorruptibility** As required by s. 37 of the *RCMP Act*.

(29) **Duty to avoid conflicts of interest and institutional bias** Including avoiding reliance on SPS where SPS may be implicated.

(30) **Duty to cooperate with judicial review** Including compliance with Rules 317 and 318.

(31) **Duty to prevent spoliation and ensure preservation of evidence** Including prohibition on alteration, deletion, or migration.

3. These Obligations Are Triggered Because the RCMP Has Notice

[463] The Applicant's evidence — including the two divergent Information Packages, missing judicial acts, missing warrants, irregular signatures, and unexplained **CPIC** anomalies — constitutes **formal notice** to the RCMP of potential systemic irregularities.

[464] Once the RCMP has notice, these 31 obligations are triggered.

[465] The RCMP's refusal to act is inconsistent with:

- a. the *Privacy Act*,

- 1275
- b. the *RCMP Act*,
 - c. the *Federal Courts Rules*,
 - d. the duty of candour,
 - e. the Rule of Law, and
 - f. and the public interest.

4. These Obligations Justify Structural Orders

[466] The Court’s structural orders — including mandatory **CTR** transmission, preservation orders, prohibition orders, and contempt leave — are justified because:

- a. the RCMP has failed to discharge these obligations;
- b. the RCMP has refused to act;
- c. the RCMP has refused to participate;
- d. the RCMP has refused to provide reasons;
- e. the RCMP has refused to search;
- f. the RCMP has refused to disclose; and
- g. the RCMP has refused to comply with Rule 318.

[467] Structural orders are necessary to restore the Rule of Law.

5. Conclusion on Systemic Policy Obligations

[468] The RCMP’s role as national custodian of **CPIC** and judicial metadata imposes **31 proactive obligations** once it has notice of potential falsification or mismatch. The RCMP has failed to discharge these obligations. Structural orders are necessary to ensure compliance, protect the public interest, and enable the Commissioner to perform his statutory duty under s. 8(2)(m).

1276

[469] The Direction created a procedural impossibility by requiring the Applicant to “file” materials with “proof of filing” in circumstances where the Respondents had not appeared and were not entitled to service. It created a non-trivial risk of inadvertent contempt. It conflicted with the Respondents’ ongoing breach of Rule 318. It undermined the structural integrity of the judicial review process. These circumstances engage the supervisory jurisdiction of the Chief Justice or Acting Chief Justice under the doctrine of *primus inter pares* and the principle in *Julius*. The Court therefore finds that the Direction must be reviewed and resolved by the judicial head of the Court. While the Associate Judge Mr. Crinson direction is correct regarding the Applicant not being required to serve the Respondents, it is not analytically precise in certain respects and does not create clear legal boundaries in others. The Court concludes that the Direction issued on June 24, 2026 created a procedural impossibility, a risk of inadvertent contempt, and a conflict with the mandatory operation of Rule 318. These issues engage the supervisory jurisdiction of the Chief Justice or Acting Chief Justice under the doctrine of *primus inter pares* and the principle articulated in *Julius v. Oxford (Bishop)*. The matter must therefore be heard and determined by the judicial head of the Court.

[470] The Applicant acted appropriately in seeking immediate review by the Chief Justice or Acting Chief Justice. His actions were necessary to protect the integrity of the judicial review process, to avoid the risk of inadvertent contempt, and to ensure that the Respondents’ ongoing breach of Rule 318 did not undermine the administration of justice.

OVERALL CONCLUSION

[471] The Applicant has also demonstrated a real and substantial risk of spoliation of volatile digital evidence, warranting a writ of prohibition to preserve metadata, logs, audit trails, and digital artifacts.

[472] The Court’s supervisory jurisdiction is engaged. The rule of law requires decisive intervention. The Applicant is quite right and equitable to self-refer by the Latin vernacular of “Pro Se” but “Pro Bono Publico”. While the common law is to evolve incrementally, the onslaught underlying these three distinct access requests under federal statutes did not incrementally evolve but rapidly devolved upon him. The authorities in his Applicant Record involving *Dagg*, *Lavigne*, *Cash Converters and McInerney v. Macdonald* are all binding but for *Cash Converters* (ONCA) and most fitting. The

distinction between “not willing” versus “not able” is well-taken along with that of the analogy to “Pandora’s box” in the modern digital environment.

[473] For all of these reasons, the Application is granted. The declarations sought are issued. Mandamus and prohibition are granted. Full indemnity costs are awarded. The Court remains seized.

Court File No. T-2448-26

FEDERAL COURT

The Honourable Acting Chief Justice of the Federal Court of Canada

Tuesday, June 30, 2026

(Court Seal)

BETWEEN:**KEVIN ALEXANDER McLEAN**

Applicant

ROYAL CANADIAN MOUNTED POLICE, COMMISSIONER MICHAEL DUHEME,
ATTORNEY GENERAL OF CANADA, and HIS MAJESTY THE KING IN RIGHT OF
CANADA

Respondents

ORDER

THE APPLICANT’S NOTICE OF MOTION NUMBER ONE, NUMBER TWO AND APPLICATION,
made by the Applicant for the relief sought in those motions and in the Applicant were heard this Tuesday,
June 30, 2026, in Toronto or Ottawa.

UPON reading the Applicant’s Notice of Application, Notice of Motion #1, Notice of Motion #2, the supporting
affidavits and documentary evidence, and the Respondents having filed no Notice of Appearance, no Certified Tribunal
Record, no evidence, and no submissions;

AND UPON the Court finding that the Respondent has failed to comply with its mandatory statutory duties under Rules
317 and 318 of the *Federal Courts Rules*, the *Privacy Act*, and the principles of procedural fairness, natural justice, and
the Rule of Law;

AND UPON the Court concluding that structural relief is necessary to restore legality, ensure access to justice, and
enable the Commissioner of the RCMP to perform his statutory duty under s. 8(2)(m) of the *Privacy Act*;

THE COURT ORDERS AND DECLARES THAT:

A. PROCEDURAL RELIEF (NUNC PRO TUNC)

1. **Abridgment of Time (Rule 8):** All timelines relating to this Application and the Applicant’s motions are
abridged nunc pro tunc.

- 1280
2. **Dispensation of Compliance (Rule 55):** Strict compliance with any procedural rule is dispensed with nunc pro tunc where necessary to give effect to this Order.
 3. **Deeming of Filing (Rule 72.1):** All documents submitted by the Applicant are deemed filed on the date they were submitted to the Registry.
 4. **Dispensation of Proof of Service (Rule 73):** The Applicant is not required to provide further proof of service upon the Respondent.

B. DECLARATORY RELIEF

5. **Ultra Vires Conduct:** It is declared that the RCMP acted outside statutory limits, failed to discharge mandatory ministerial and executory duties, and acted unreasonably within the meaning of *Vavilov*.
6. **Contravention of Rule 318:** It is declared that the RCMP contravened Rule 318 by failing to transmit the Certified Tribunal Record.
7. **Breach of Procedural Fairness:** It is declared that the RCMP breached procedural fairness and natural justice.
8. **Administrative Bad Faith:** It is declared that the RCMP engaged in administrative bad faith, including silence where the law required action, half-truths, misstatements of law, and active concealment.
9. **Denial of Access to Justice:** It is declared that the RCMP's conduct constitutes a functional denial of access to justice.
10. **Public Interest Engagement:** It is declared that the Applicant's evidence raises urgent and compelling public interest concerns requiring the Commissioner's personal consideration under s. 8(2)(m) of the *Privacy Act*.
11. **Systemic Obligations:** It is declared that the RCMP is subject to the 31 proactive obligations set out in these Reasons when it has notice of potential falsification, mismatch, or irregularity in judicial or CPIC-related records.

C. MANDAMUS

12. **Mandatory Search Order:** The RCMP shall conduct a full search of all repositories containing the Applicant's personal information, including but not limited to:
 - o CPIC Foundational Metadata;
 - o CPIC Offline Historical Database;
 - o ADD/MODIFY/CLEAR/CANCEL logs;
 - o audit logs;
 - o access logs;
 - o hexadecimal dumps;
 - o PPU 005;
 - o cross-jurisdictional ingestion logs;
 - o administrative processing files;
 - o all internal communications relating to file P-2025-16999.
13. **Mandatory s. 8(2)(m) Consideration:** The Commissioner of the RCMP shall personally consider whether disclosure is required under s. 8(2)(m) of the *Privacy Act*.
14. **Mandatory Reasons:** The Commissioner shall provide written reasons explaining:
 - o whether disclosure is in the public interest;
 - o whether disclosure would benefit the Applicant;
 - o the statutory analysis;
 - o the factual basis;
 - o the public interest considerations.

D. CERTIFIED TRIBUNAL RECORD (RULE 318)

1281
15. **24-Hour Deadline:** The RCMP shall transmit the complete Certified Tribunal Record to the Registry and to the Applicant **within 24 hours** of this Order.

16. **Required Contents:** The CTR shall include all 18 categories of materials enumerated in the Schedule to NOM #2, including:

- administrative files;
- system logs;
- audit trails;
- metadata;
- judicial acts;
- warrants;
- endorsements;
- communications;
- ingestion logs;
- and all other materials specified therein.

E. PROHIBITION AND PRESERVATION

17. **Preservation of Metadata:** The RCMP is prohibited from deleting, altering, migrating, sanitizing, obfuscating, or archiving beyond rapid retrieval any metadata, logs, or audit trails relating to the Applicant.

18. **Prohibition Against Unauthorized Searches:** The RCMP is prohibited from conducting searches outside the scope of the Applicant's PII Access Request for the purpose of responding to that request.

F. JUDICIAL OVERSIGHT

19. **Court Seized:** The Court remains seized of this matter to supervise compliance, address issues arising from execution, and adjudicate any contempt proceedings.

G. CONTEMPT LEAVE

20. **Leave for Contempt:** The Applicant is granted leave to bring a motion for contempt under Rule 50 and Rules 466–467 if the RCMP fails to comply with this Order.

H. CROSS-JURISDICTIONAL ENFORCEMENT

21. **Enforcement Authorization:** The Applicant is authorized to seek recognition and enforcement of this Order in any court, tribunal, or administrative body in Canada.

I. COSTS AND INTEREST

22. **Costs:** Costs are awarded to the Applicant on a **full indemnity basis**, payable forthwith by the Respondent.

23. **Interest:** Pre-judgment and post-judgment interest are awarded on all costs.

J. RESIDUAL RELIEF

24. **Residual Authority:** The Court grants such further and other relief as may be just and equitable to give full effect to this Order.

SIGNED at Ottawa, Ontario, this ____ day of _____, 2026.

The Honourable Chief Justice (acting) of the Federal Court of Canada
Associate Chief Justice of the Federal Court of Canada Madam Justice St. Louis



 Print page

Your documents have been submitted to the Federal Court using the Electronic Filing System (E-Filing System).

Your document(s) have been submitted to the Federal Court.

- You have submitted **2 document(s)** to the **Ottawa Registry Office**.
- Your unique confirmation number for this submission is: **2026-06-25-8513946472091**.
- Date submitted: **06/25/2026 at 4:44:52 P.M. Eastern Time (ET)**.

Note that your document(s) will be **considered successfully filed after the Registry reviews, accepts and processes your submission**.

You will then receive an email that includes the Court File Number and a hyperlink to the stamped documents.

- [What's next](#)
- [Urgent matter](#)
- [Online access to documents](#)
- [Your submission](#)

What's next

You will receive an email from **noreply-nepasrepondre@cas-satj.gc.ca** with the unique confirmation number above.

Federal Court Registry personnel will review your submission and determine whether it can be accepted.

✓ Accepted document(s)

If your document(s) comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will accept and process your submission.
 - Your document(s) will be deemed as filed on the date and time of your submission to the E-Filing System, Eastern time (ET); unless you submitted on a Saturday, Sunday, or [holiday](#). If you submitted on a weekend or holiday, they will be deemed as filed on the next business day.
2. You will receive an email confirming that your document(s) have been accepted and filed. The email will include the Court File Number and a hyperlink to the stamped document(s).

✗ Non-accepted document(s)

If your document(s) do not comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will send you an email to inform you of the filing status and provide instructions for corrections.
2. Use the E-filing System and your unique confirmation number to submit the corrected document(s). The submission of a corrected document will not result in additional charges.
3. After you submit the corrected document(s), they will be reviewed. The Registry will send you an email indicating whether or not the corrected documents have been accepted.

1284

 Issues related to document type

If you selected the wrong document type(s) in the E-Filing System this may affect the applicable filing fee. The Federal Court Registry may contact you by phone or email for additional payment or a refund.

Urgent matter

If you have flagged your submission as urgent, please [contact the Registry](#). Submitting documents electronically does not guarantee that they will be reviewed immediately.

Online access to documents

If you have requested your submission be exempt from public online access, the documents mentioned will not be made available online until the Court makes a decision about your request and informs you.

►

Your submission

Share your feedback

Take 5 minutes to help us improve our service.

Start survey

Start a new submission

About the Court

[Jurisdiction](#)

[Careers](#)

[Liaison Committees](#)

[Reports and Statistics](#)

Law and Practice

[Acts and Rules](#)

[Practice Guides](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Court Costs](#)

[Deadlines Calculator](#)

[Checklists](#)

Online Access

[Forms](#)

[E-Filing](#)

[E-Motion](#)

Representing Yourself

- [Finding Legal Help](#)
- [Practice Guides](#)
- [Procedural Charts](#)
- [Procedural Roadmaps](#)
- [Checklists](#)
- [Court Costs](#)
- [Deadlines Calculator](#)
- [Resolving Your Case](#)
- [Registry](#)

Court Files and Decisions

- [Court Files](#)
- [Decisions](#)
- [Hearing Lists](#)
- [Generalittings](#)
- [Summer Recess](#)
- [Calendar of Hearings](#)

Media

- [Administration of the Court](#)
- [Court Files](#)
- [Decisions](#)
- [Calendar of Hearings](#)

Resources

- [Registry](#)
- [Court Costs](#)
- [Procedural Charts](#)
- [Procedural Roadmaps](#)
- [Resolving Your Case](#)
- [Finding Legal Help](#)
- [Checklists](#)

June 25, 2026

1286
VIA E-FILE — FEDERAL COURT OF CANADA (OTTAWA REGISTRY)

TO: Federal Court of Canada — Ottawa Registry 90 Sparks Street Ottawa, Ontario K1A 0H9

RE: *McLean v. RCMP et al.* — Court File No. T-2448-26 Filing of Draft Reasons for Order/Judgment (Tab 32) and Notice of Motion #2 Materials Matter Requiring the Attention of the Chief Justice / Acting Chief Justice

Dear Chief Administrator at the Principal Office and to by way of forwarding the Honourable Chief Justice of the Federal Court of Canada:

Please accept for filing the enclosed **Draft Reasons for Order/Judgment** (Tab 32) and associated materials relating to **Notice of Motion #2** and the underlying **Application for Judicial Review** in the above-noted proceeding.

Consistent with the **June 24, 2026 Direction** of Associate Judge Crinson, and in light of the procedural issues arising from that Direction, a copy of this filing is also being provided to the **Chief Administrator** of the Federal Court.

These materials are filed in the **Principal Office (Ottawa)** pursuant to Rule 25 of the *Federal Courts Rules*, and in light of the issues raised concerning:

- the Respondents' ongoing breach of **Rule 318** (Certified Tribunal Record);
- the procedural impossibility created by the **June 24, 2026 Direction**;
- the resulting **contempt-risk paradox**;
- the extinguishment of service rights under **Rule 305(2)**;
- the structural nature of the relief sought; and
- the engagement of the Court's **supervisory jurisdiction** under the doctrine of *primus inter pares*.

A fully indexed, hyperlinked, and bookmarked **2nd Updated Application Record** (Tabs 1–32) will be filed electronically later this evening, with Delivery Filing to follow tomorrow morning in accordance with Rule 25. A hyperlinked standalone copy of the Draft Reasons will also be provided for the Court's convenience.

For clarity, no service is effected on the Respondents with this filing. Consistent with Rule 305(2), the Respondents have not filed a Notice of Appearance and therefore are not entitled to service of any further step. To the extent that further procedural developments or documentary materials arise prior to the hearing of Notice of Motion #2 or Notice of Motion #1, and to the extent such materials assist the Court in understanding the issues raised, the Applicant will promptly provide them to the Court by filing them into the **Comprehensive NOM #2 / Application Record (which naturally incorporates NOM #1)**. This ensures that the Court has a complete and continuously updated record while maintaining the Applicant's **sub judice** obligations and the procedural integrity of these consolidated proceedings.

I also wish to draw the Court's attention to a technical anomaly encountered earlier today. A faxed letter addressed to the Ottawa Principal Office was successfully transmitted; however, the receiving fax ID displayed a **416-area-code identifier** associated with the Ontario Court of Justice. This may simply reflect shared telecommunications infrastructure, but given the issues raised in these proceedings concerning the integrity of judicial records and the separation of institutional systems, I respectfully note the anomaly for the Court's awareness.

Finally, I note that the *Federal Courts Rules* do not contain a prescribed form of **Draft Order**. In the public interest, and to assist the Court, I have taken the time to prepare a comprehensive set of **Draft Reasons for Order/Judgment** which, in substance, reflect the issues, statutory duties, jurisprudence, and procedural history underlying these consolidated matters. Should the Court prefer to issue a shorter order with reasons to follow, or briefer reasons, the enclosed Draft Reasons are intended solely to assist the Chief Justice / Acting Chief Justice and the Federal Court with a clear roadmap of the factual matrix, legal issues, enactments, and authorities engaged.

1287
Given the nature of the issues raised — including the Rule 318 breach, the procedural impossibility arising from the Direction and the need for structural mandamus — the Applicant respectfully submits that this matter properly requires the attention of the **Chief Justice or Acting Chief Justice**.

Please do not hesitate to contact me should the Registry (Principal Office) require any clarification.

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'K. McLean', written over a horizontal line.

Mr. Kevin A. McLean (BA, JD, CIM)

Applicant Toronto, Ontario Email: mcleansettlement@gmail.com Tel: 647-370-9354

TAB 37

Requisition for Hearing — Application

Court File Number: T-2448-26

FEDERAL COURT

B E T W E N:

KEVIN A. MCLEAN

Applicant

- and -

ROYAL CANADIAN MOUNTED POLICE, MICHAEL DUHEME, JEFF BALL,
AND STEPHANE BRISSON

Respondents

Requisition for Hearing

TO:

Manager of Court Operations/Judicial Administrator/Registrar of the Federal Court of Canada (City of Toronto)Manager of Court Operations / Judicial Administrator / Registrar
Federal Court of Canada — Principal Office (Ottawa)
90 Sparks Street
Ottawa, Ontario K1A 0H9**THE APPLICANT REQUESTS** that a date be set for the **Hearing** of this **Application**.**THE APPLICANT CONFIRMS THAT:**

1. The requirements of subsection 309(1) of the *Federal Courts Rules* have been complied with.
2. There is no requirement to serve a notice of constitutional question under section 57 of the *Federal Courts Act* in this application.
3. The hearing should be held at **Ottawa, Ontario**.
4. The Application should be determined entirely in writing under Rule 369, for the following reasons:

(a) **The Respondents have not appeared.**

No Respondent has served or filed a Notice of Appearance under Rule 305(1). Under **Rule 305(2)**, they are **not** entitled to service of any further step.

(b) The Respondents have not transmitted the Certified Tribunal Record.

Under **Rule 318(1)**, the CTR was due **20 days after service** (May 19, 2026). No CTR has been transmitted. No objection has been filed under Rule 318(2).

(c) The June 24, 2026 Direction created a procedural impossibility.

Associate Judge Crinson's Direction required the Applicant to "file" materials with "proof of filing" in circumstances where:

- the Respondents have not appeared;
- Rule 305(2) extinguishes their entitlement to service;
- Rule 306 presupposes an appearing respondent;
- the CTR has not been transmitted;
- the evidentiary record is defined by Rule 318, not by affidavits.

This created a **structural impossibility** and a **non-trivial contempt-risk**, requiring **supervisory intervention** by the Chief Justice / Acting Chief Justice.

(d) The issues are structural, institutional, and of national public importance.

They include:

- mandatory statutory duties under the Privacy Act and ATIA;
- the Rule 318 CTR breach;
- the integrity of judicial records;
- the constitutional doctrine of *primus inter pares*;
- the public interest in CPIC integrity;
- access to justice and the Rule of Law.

(e) NOM #1 is unopposed; NOM #2 is unopposed; and The Application is unopposed.

No Respondent has:

- filed a Notice of Appearance;
- filed a Notice of Intent to Respond;
- filed any evidence;
- filed any submissions;
- opposed the Rule 317 request;
- opposed the relief sought.

(f) Judicial review is intended to be summary (Rule 3).

Where Respondents do not appear, the Court may determine the matter entirely in writing.

(g) The Applicant has filed a comprehensive, hyperlinked, bookmarked record.

(h) The matter requires the attention of the Chief Justice / Acting Chief Justice.

Given:

- the Rule 318 breach;
- the procedural impossibility created by the Direction;
- the contempt-risk paradox;
- the structural nature of the relief;
- the constitutional issues raised;

the Applicant respectfully submits that this matter must be scheduled before the **Chief Justice or Acting Chief Justice**.

5. Representatives of the parties:

Applicant:

Mr. Kevin A. McLean (BA, JD, CIM) Self-Represented 68 Abell Street Toronto, ON M6J 0B1 Email: mclean@searchandseizure.ca

Respondents:

Nil (no Notices of Appearance served and filed, and no leave obtained; Rule 305(2) and 145 applies)

6. Availability

The Applicant is available at any time and respectfully requests that the hearing be scheduled at the time of the hearing of his NOM #2 which must be heard before the Primus Inter Pares of the Federal Court of Canada, the Honourable Chief Justice of the Federal Court of Canada, Madam Justice St. Louis.

7. Language

The hearing will be in English.

No interpreter is required.

All materials are in English.

DATED at Toronto, Ontario, this 25th day of June, 2026.



Mr. Kevin A. McLean (BA, JD, CIM)

68 Abell Street
Toronto, ON

TO:

Nil (as per the above and the evidence contained in the Applicant's most recent Motion Record for NOM #1 of June 11, 2026; NOM #2 on June 22 and 23, 2026, and NOM #2 Motion Record/Application Record (1st Updated) and the Respondents not being entitled to be served with this Requisition).

[SOR/2021-151, s. 23](#)



 Print page

Your documents have been submitted to the Federal Court using the Electronic Filing System (E-Filing System).

Your document(s) and payment have been submitted to the Federal Court.

- You have submitted **1 document(s)** to the **Ottawa Registry Office**.
- Your unique confirmation number for this submission is: **2026-06-25-7729905390960**.
- Date submitted: **06/25/2026 at 4:59:46 P.M. Eastern Time (ET)**.

Note that your submission will **only be considered filed** in Federal Court **after it has been examined, accepted and processed by the Registry**.

- [What's next](#)
- [Urgent matter](#)
- [Online access to documents](#)
- [Your submission](#)

What's next

You will receive an email from **noreply-nepasrepondre@cas-satj.gc.ca** with the unique confirmation number above.

Federal Court Registry personnel will review your submission and determine whether it can be accepted.

✓ Accepted document(s)

If your document(s) comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will accept and process your submission.
 - Your document(s) will be deemed as filed on the date and time of your submission to the E-Filing System, Eastern time (ET); unless you submitted on a Saturday, Sunday, or [holiday](#). If you submitted on a weekend or holiday, they will be deemed as filed on the next business day.
2. You will receive an email confirming that your document(s) have been accepted and filed. The email will include the Court File Number and a hyperlink to the stamped document(s).

✗ Non-accepted document(s)

If your document(s) do not comply with the *Federal Courts Rules, Act*, and formatting standards:

1. The Registry will send you an email to inform you of the filing status and provide instructions for corrections.
2. Use the E-filing System and your unique confirmation number to submit the corrected document(s). The submission of a corrected document will not result in additional charges.
3. After you submit the corrected document(s) by email, they will be reviewed. The Registry will send you an email indicating whether or not the corrected documents have been accepted.
 - If you paid filing fees for document(s) that the Court did not accept for filing, you will receive a refund.

1294

 Issues related to document type

If you selected the wrong document type(s) in the E-Filing System this may affect the applicable filing fee. The Federal Court Registry may contact you by phone or email for additional payment or a refund.

Urgent matter

If you have flagged your submission as urgent, please [contact the Registry](#). Submitting documents electronically does not guarantee that they will be reviewed immediately.

Online access to documents

If you have requested your submission be exempt from public online access, the documents mentioned will not be made available online until the Court makes a decision about your request and informs you.

►

Your submission

Share your feedback

Take 5 minutes to help us improve our service.

Start survey

Start a new submission

About the Court

[Jurisdiction](#)

[Careers](#)

[Liaison Committees](#)

[Reports and Statistics](#)

Law and Practice

[Acts and Rules](#)

[Practice Guides](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Court Costs](#)

[Deadlines Calculator](#)

[Checklists](#)

Online Access

[Forms](#)

[E-Filing](#)

[E-Motion](#)

Representing Yourself

[Finding Legal Help](#)

[Practice Guides](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Checklists](#)

[Court Costs](#)

[Deadlines Calculator](#)

[Resolving Your Case](#)

[Registry](#)

Court Files and Decisions

[Court Files](#)

[Decisions](#)

[Hearing Lists](#)

[General Sittings](#)

[Summer Recess](#)

[Calendar of Hearings](#)

Media

[Administration of the Court](#)

[Court Files](#)

[Decisions](#)

[Calendar of Hearings](#)

Resources

[Registry](#)

[Court Costs](#)

[Procedural Charts](#)

[Procedural Roadmaps](#)

[Resolving Your Case](#)

[Finding Legal Help](#)

[Checklists](#)

TAB 38



Mr. Kevin McLean <mcleansettlement@gmail.com>

Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Mr. Kevin McLean <mcleansettlement@gmail.com>

To: "Mathews, Curtis (RCMP/GRC)" <Curtis.Mathews@rcmp-grc.gc.ca>

Cc: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>, "Duheme, Michael (RCMP/GRC)" <Michael.Duheme@rcmp-grc.gc.ca>, "Brisson, Stéphane (RCMP/GRC)" <Stephane.Brisson@rcmp-grc.gc.ca>, "Ball, Jeff (RCMP/GRC)" <Jeff.Ball@rcmp-grc.gc.ca>, "mclean@searchandseizure.ca" <mclean@searchandseizure.ca>

(for ATIA Request #2 — May 7, 2026)

Subject: Re: ATIA Request A-2026-00761 — Final Search Position

Good afternoon Mr. Mathews,

Thank you for your correspondence.

I acknowledge your statement that *"our searches indicate that no records exist for this request"* and that the RCMP's searches were conducted *and resources within RCMP.*" I understand this to constitute the RCMP's final position on ATIA Request A-2026-00761.

For the record, I note the following procedural points:

1. **Your conclusion that "no records exist" is irreconcilable with the RCMP's prior representations** that the file was in a *"retrieval Primary Interest"* required further clarification (June 25, 2026). These positions cannot simultaneously be true.
2. **Your description of the search parameters confirms that the RCMP did not task the technical custodians of the requested records.** The request sought CPIC audit trails, hexadecimal mainframe logs, ORI routing metadata, offline historical data, and system-general *financial databases* cannot locate such records.
3. **Your conclusion that the RCMP has never used GrapeCity or MESCIUS software is inconsistent with the metadata contained in the request.** The request sought CPIC audit trails, hexadecimal mainframe logs, ORI routing metadata, offline historical data, and system-general *financial databases* cannot locate such records.
4. I acknowledge your reminder regarding the Information Commissioner's complaint process. As noted previously, the statutory 30-day Information Act expired on May 14, 2026, and no section 9 extension was invoked. Your present email will be added to the existing record.

Thank you for confirming the RCMP's final position.

Respectfully,

Mr. Kevin A. McLean

On Fri, Jun 26, 2026 at 2:41 PM Mathews, Curtis (RCMP/GRC) <Curtis.Mathews@rcmp-grc.gc.ca> wrote:

Good morning Mr. McLean,

I am writing to inform you that I have confirmed with those that worked on this request, that our searches indicate that no records exist for this request.

Our searches through contract and financial databases and resources within RCMP have concluded that we have no results for any records related to the use or procurement of "GrapeCity". RCMP has used software related to those listed in your request, and that is why our search has produced no records in response to your request.

Given the above, I consider our response to your request complete and accurate based on the information provided in your request parameters.

Lastly, as noted in our previous response letter dated June 18, 2026, that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request. To avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada

30 Victoria Street, 7th Floor

Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online: <https://www.oic-ci.gc.ca/en/you-submit-complaint>.

Thank you.

Curtis Mathews

Director, Access to Information Disclosure & Modernization / Directeur, Accès à l'information divulgation et modernisation

1298

Access to Information and Privacy Branch / Sous-direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP)

Royal Canadian Mounted Police / Gendarmerie royale du Canada

curtis.mathews@rcmp-grc.gc.ca Tel: 343-551-1037

From: Mathews, Curtis (RCMP/GRC)

Sent: June 22, 2026 11:52 AM

To: 'Mr. Kevin McLean' <mcleansettlement@gmail.com>; ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>; Duheme, Michael (RCMP/GRC) <Michael.Duheme@rcmp-grc.gc.ca>; Larkin, Bryan (RCMP/GRC) <Bryan.Larkin@rcmp-grc.gc.ca>; Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>

Cc: mclean@searchandseizure.ca

Subject: RE: Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Good morning Mr. McLean,

I want to acknowledge receipt of your email below and assure you that my team and I are looking into your concerns as they relate to the processing of your Access to Information Act request.

I want to ensure I fully address the issues you have noted below and will therefore need some time to address your concerns and legal assertions.

I commit to getting back to you with a response by the end of the week.

Thank you in advance for your patience, and I look forward to working with you to resolve the issues.

Curtis Mathews

A/Director General, ATIP Modernization / Directeur générale p.i, AIPRP modernisation

Access to Information and Privacy Branch / Sous-direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP)

Royal Canadian Mounted Police / Gendarmerie royale du Canada

curtis.mathews@rcmp-grc.gc.ca Tel: 343-551-1037

From: Mr. Kevin McLean <mcleansettlement@gmail.com>

Sent: June 22, 2026 8:29 AM

To: ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca>; Duheme, Michael (RCMP/GRC) <Michael.Duheme@rcmp-grc.gc.ca>; Brisson, Stéphane (RCMP/GRC) <Stephane.Brisson@rcmp-grc.gc.ca>; Larkin, Bryan (RCMP/GRC) <Bryan.Larkin@rcmp-grc.gc.ca>; Ball, Jeff (RCMP/GRC) <Jeff.Ball@rcmp-grc.gc.ca>; Mathews, Curtis (RCMP/GRC) <Curtis.Mathews@rcmp-grc.gc.ca>

Cc: mclean@searchandseizure.ca

Subject: Re: Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I received the below auto-reply from Mr. Brisson and a postmaster deliver from what I thought to be the email of Mr. Curtis Mathews but I appeared to have added one too many "t's" in surname. Apologies for the error.

Regards, Mr. Kevin A. McLean (BA, JD, CIM)

Appendix

Brisson, Stéphane (RCMP/GRC)

7:39 AM (46 minutes ago)

to me

1299

I am out of the office and will return on July 7, 2026. During my absence please contact Curtis Mathews, The Access of Information Director, at curtis.mathews@rcmp-grc.gc.ca

Regards

Stéphane Brisson

Bonjour,

Je suis absent du bureau et je serai de retour le 7 Juillet 2026. Pendant mon absence, veuillez communiquer avec Curtis Mathews, Directeur de l'accès à l'information, à : curtis.mathews@rcmp-grc.gc.ca

Sincèrement,

Stéphane Brisson

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Mon, Jun 22, 2026 at 7:37 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Date: June 22, 2026

Subject: RE: Formal Request under the ATIA - File No: A-2026-01933 (GrapeCity / MESCIUS SDK Procurement & Lifecycle Architecture)

CC:

Commissioner Michael Duheme (Michael.Duheme@rcmp-grc.gc.ca)

1300

Commissioner Bryan Larkin (Bryan.Larkin@rcmp-grc.gc.ca)

General Mr. Stephane Brisson (Stephane.Brisson@rcmp-grc.gc.ca)

Director, ATIP Branch of the RCMP, Mr. Curtis Matthews (Curtis.Matthews@rcmp-grc.gc.ca)

Director, Mr. Jeff Ball

SUBJECT: RESPONSE TO A-2026-01933 / F281

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I am in receipt of your correspondence dated June 18, 2026, signed by Director Curtis Matthews, asserting that a search was conducted and that the Royal Canadian Mounted Police (RCMP) is "unable to locate records" (A-2026-019... p. 1).

Please consider this transmission formal notification that the Applicant rejects this determination as a severe, bad-faith breach of the RCMP's explicit statutory obligations under the *Access to Information Act*. This position is non-compliant on the face of the statutory text, as detailed below:

1. DEFECTIVE NOTICE AND THE SECTION 10(1)(A) DISTINCTION

Parliament has strictly mandated under **Section 10(1)(a)** of the Act that when access is refused, the head of the institution must explicitly state that the record **"does not exist"** (RSC 1985, ... p. 8). Director Curtis Matthews stated that the RCMP was **"unable to locate records"** (A-2026-019... p. 2).

There is an absolute, immutable legal distinction between a record *not existing* and an institution being *unable to find it*. By admitting that you simply cannot find the records, you admit to a deficient search under Section 10(1) triggers an immediate **Deemed Refusal under Section 10(3)** of the Act (RSC 1985, ... p. 8).

2. BREACH OF SECTION 4(1) AND SECTION 4(2.1) (THE DUTY TO ASSIST)

The statutory mandate places a strict, non-discretionary duty on the head of the institution to make *every reasonable effort* to assist a requester and to respond *accurately and completely* (RSC 1985, ... p. 4). **GrapeCity.Documents for PDF v. 6.0.2.0** engine leaves undeniable, machine-readable digital traces (including Fast Web View linearization and custom XMP toolkits) on active data streams (Gmail - AT... p. 1).

Asserting that zero procurement contracts, software licensing supply arrangement (SLSA) call-ups, change-management tickets, or National Technology Onboarding Program (NTOP) security evaluations are a structural impossibility (Gmail - AT... p. 7). It represents a fatal failure of the mandatory duty to assist (RSC 1985, ... p. 4).

3. CHRONOLOGICAL RECORD OF CORPORATE AWARENESS

Senior executive command possesses documented, actual notice of this statutory delinquency, eliminating any defense of administrative oversight:

- **May 5, 2026:** The formal, multi-tiered ATIA request was validly submitted to the RCMP ATIP Branch (Gmail - AT... p. 1).
- **May 11, 2026:** Your office issued a boilerplate acknowledgment ("currently proceeding") that failed to cite specific statutory grounds or a definitive duration under Section 9(1), rendering your process procedurally defective (pp. 1-2).
- **June 8, 2026:** Upon the crystallization of your un-extended statutory deadline, I served a formal Notification of Statutory Non-Compliance establishing your state of deemed refusal (Gmail - AT... p. 3).
- **June 10, 2026:** Explicit notice of this ongoing delinquency was served directly to Commissioner Duheme, DG Brisson, and Acting Commissioner Deputy Commissioner Bryan Larkin (Gmail - AT... p. 4).

4. DIRECT FEDERAL COURT ESCALATION AND STATUTORY STRATEGY

To prevent the fragmentation of legal resources and avoid crossing up jurisdictions, **I will not be lodging at this time an administrative complaint with the Office of the Information Commissioner** on this matter.

Instead, because the RCMP's administrative failure to locate its own procurement data stands in direct contradiction to the objective forensic metadata, **this entire communication corpus—encompassing acknowledgment, the June 8 crystallization notice, and your June 18 refusal—is being filed directly into the Federal Court of Canada (Toronto Registry) as a unified Supplementary Application** (pp. 1, 9, A-2026-019... p. 1).

Pursuant to **Sections 30 and 31.1 of the Canada Evidence Act**, these direct electronic communications from the RCMP ATIP Branch function as self-authenticating, uncontradicted business records. They thereby rendering any cross-examination mechanisms under the *Federal Courts Rules* wholly inapplicable.

This objective, institutional record will be deployed as a primary evidentiary anchor for my upcoming Hearing (see: Federal Courts Rules, section 2) of my Application (see: Rule 300 and onwards) enabling me to seek an order under Rules 49 and 50 and issue an immediate order to conduct yet another search and then produce to avoid a multiplicity of hearings and proceedings (RSC 1985, ... p. 36).

Justice delayed is justice denied.

1301

view, this is a complete breakdown of government which underscores why the hearing of my unopposed and uncontested by the non-appearing Respondents in my Judicial Review Application must be held – Application”. This serves as formal notice that I reserve the right to rely upon this correspondence for any lawful purpose including emails generated by your operating and information technology.

Thank you.

Be guided accordingly.

Sincerely,

Mr. Kevin A. McLean (BA, JD, CIM)

On Wed, Jun 10, 2026 at 4:35 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I received the auto-reply from Mr. Duheme as per the Appendix. As such, Mr. Larkin is copied (see: Bryan.Larkin@rcmp-grc.gc.ca).

Appendix

Automatic reply: Access to Information Act request A-2026-01933 / F281, Your File N/A, Acknowledgment

Duheme, Michael (RCMP/GRC)

to me

Prenez note que je serai absent en devoir à compter du 21 mai au 19 juin. Sous Commissaire Bryan Larkin agira à titre de Commissaire par intérim. Vous pouvez le rejoindre à Bryan.Larkin@rcmp-grc.gc.ca

The 21st May to 19 June, I will be away on duty , Deputy Commissioner Bryan Larkin will be the acting Commissioner. He can be reached at Bryan.Larkin@rcmp-grc.gc.ca

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

1302

Wed, Jun 10, 2026 at 4:31 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

Dear Sirs/Mesdames/Other Gender-Neutral Pronouns:

I am copying the following to this email for self-evident reasons:

1. RCMP Commissioner Mr. Duheme; and
2. Director General Mr. Brisson

I will follow up more formally for the Head of the Institution and the chief privacy officer of the RCMP with a summary of status et al. However, in the interim, would you confirm or deny whether y purposed extension of time?

Thank you.

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Mon, Jun 8, 2026 at 9:47 AM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DELIVERY METHOD: Via Electronic Transmission

CLASSIFICATION: Private and Confidential

DATE: June 8, 2026

TO: Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca

Attention: Bryan, ATIP Coordinator

**SUBJECT: FORMAL NOTIFICATION OF STATUTORY NON-COMPLIANCE, CRYSTALLIZATION OF DEEMED REI
TO SUBSECTION 9(2), AND DEMAND FOR IMMEDIATE REMITTANCE OF ACTA CONCERNING REQUEST A-2026-01**

I. PRELIMINARY ASSERTIONS, ACKNOWLEDGMENT OF TRANSMISSIONS, AND THE CRYSTALLIZATION OF THE STATUTO

1. Reference is hereby systematically directed to the antecedent chain of communications and the underlying access request (the “**Access Request**”) effectuated upon the Royal Canadian I architectural mapping parameters previously supplied. Reliance is concurrently placed upon the three prior electronic transmissions exchanged with your directorate, all of which are inextr
2. It is formally asserted that today, June 8, 2026—representing the next juridical business day following the maturation of the thirty-day limit on June 6, 2026—constitutes the absolute, non-records. The failure to consummate disclosure by this temporal threshold operates to situate the Government Institution into an immediate state of deemed refusal.

II. SUBSTANTIVE DEFICIENCIES WITHIN THE ADMINISTRATIVE RESPONSE AND THE DOCTRINE OF ABSOLUTE NULLITY

3. The correspondence disseminated by the Government Institution on May 11, 2026 (the “**Administrative Response**”) fails to satisfy even the most rudimentary jurisdictional prerequec aforementioned communication purported to acknowledge the request whilst relying upon generalized, boilerplate vernacular—stating merely that the institution is “currently proceec window.
4. Specifically, the aforementioned correspondence is vitiated by the following fatal administrative omissions:

- a. The absolute failure to cite the exact statutory subsection being relied upon to delay disclosure, namely the omission of any reference to paragraphs 9(1)(a), 9(1)(b), or 9(1)(c) of the *Access to Information Act*.
 - b. The absolute failure to establish the duration or length of the purported extension, an omission that renders the correspondence *ultra vires* and deprives the requester of the statutorily prescribed extension.
5. Furthermore, the Government Institution has profoundly misconstrued the foundational parameters governing the provision of complaint rights (the “**Complaint Rights**”). The assertion that a request must be lodged “within 60 days of receipt of this notice” is a fundamental misstatement of law. Pursuant to the *Access to Information Act*, R.S.C. 1985, c. A-1, the right to advance a request containing the requisite statutory justifications and durations, whereas complaints regarding a refusal are commenced following the crystallization of a deemed refusal or the acknowledgement cannot autonomously trigger a limitation period for complaint rights absent strict adherence to the preconditions of section 9. Such a structural defect elevates the error to nullity *in limine*.

III. MANDATORY STATUTORY INQUIRY CONCERNING OVERSIGHT BY THE INFORMATION COMMISSIONER

6. In direct alignment with the imperative to ensure uncompromising adherence to the governing legislative framework, a formal inquiry is hereby advanced pursuant to subsection 9(2) of the *Access to Information Act* to formally apprise the independent parliamentary ombudsman serves as an indispensable systemic safeguard against institutional overreach and the arbitrary suppression of public records.
7. **FORMAL INQUIRY:** Has the Royal Canadian Mounted Police provided the requisite statutory notice to the information commissioner of Canada (the “**Information Commission**” threshold)?
8. **NOTA BENE (I) - REBUTTAL CONCERNING OVERSIGHT AVOIDANCE:** Should the Government Institution have neglected its non-derogable obligation to notify the Information Commissioner of Canada of the extension, to invalidate any presumed temporal extension. The immediate provision of the documentary evidence confirming this transmission to the Information Commissioner is demanded. The failure to do so *facie* as an admission of non-compliance.

IV. EXHAUSTIVE JURISPRUDENTIAL APPLICATION AND THE INVALIDATION OF THE PRESUMED EXTENSION

9. The obligations of a Government Institution regarding the unilateral protraction of disclosure deadlines are strictly circumscribed. The following exhaustive corpus of federal jurisprudence actions constitute a breach of statutory duties, rendering any presumed extension void *ab initio*:
- a. *Strict Procedural Notice Requirements:* As elucidated comprehensively in *Statham v. Canadian Broadcasting Corporation*, 2010 FCA 315, and its antecedent *Statham v. Canadian Broadcasting Corporation*, 2010 FC 1026, the failure of a Government Institution to statutorily notify an applicant that specific extensions are being claimed pursuant to section 9 of the Act strictly invalidates the attempted delay. A contemporaneous review is irreparably severed when a Government Institution obscures the exact grounds for that extension.
 - b. *Violation of Extended Deadlines:* This principle of rigid procedural stricture is further corroborated by *Hydro-Québec v. Canada (National Energy Board)*, 1997 CanLII 17697 (FC). The Federal Court emphatically held that an institution's failure to comply with the rigid notice requirements and time limits mandated by section 9 of the Act constitutes a breach of statutory duties.
 - c. *The Requirement to Specify Subsections:* A lawful extension cannot be assumed; it must be pleaded. Whether an extension is based upon paragraph 9(1)(a) (unreasonable delay) or 9(1)(b) (deemed refusal), the institution must explicitly cite the provision and ensure a serious effort is made to assess the required duration, as mandated in *Biogenie Canada Inc. v. Canada (Food Inspection Agency)*, 2015 FC 1026.
 - d. *Strict Scrutiny of Asserted Volumes:* While extensions for volume are statutorily permissible, they remain subject to strict judicial scrutiny for objective reasonableness. Any attempt to impose an excessive extension unequivocally struck down in *Canada (Attorney General) v. Canada (Information Commissioner) (T.D.)*, 2002 FCT 136—constitutes an actionable breach of statutory duties.
 - e. *Strict Scrutiny of Asserted Consultations:* Similarly, an extension under 9(1)(b) is not a carte blanche for perpetual internal delays. Jurisprudence such as *Bronskill v. Canada (Attorney General)*, 2011 FC 649, and *X v. Canada (Minister of National Defence) (T.D.)*, 1990 CanLII 13047 (FC) confirms that consultations must be conducted in a timely and meaningful manner.
 - f. *Mandatory Oversight and Accountability:* The Supreme Court of Canada in *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, 2006 SCC 13, alongside the *Minister of Health and Welfare*, 1992 CanLII 15386 (FC), affirms that the invocation of a section 9 extension is an extraordinary statutory mechanism requiring strict justification. The *Office of the Information Commissioner*, 2015 FC 776 further demonstrate that adherence to oversight notification is subjected to rigorous judicial scrutiny.
 - g. *Crystallization of Deemed Refusals:* As definitively ruled by the Federal Court of Appeal in *Canada (Information Commissioner) v. Canada (National Defence)*, 2014 FC 205, a Government Institution that fails to provide access by the exact date upon which its asserted deadline expires enters an immediate deemed refusal. If the deadline is lawfully extended, the Government Institution is in a state of deemed refusal today.
 - h. *Cost Consequences for Dilatory Conduct:* The failure to provide access within the statutorily mandated period constitutes actionable grounds for the awarding of costs. This principle is affirmed in *Dagg v. Canada (Industry)*, 2010 FCA 316 and *Dagg v. Canada (Industry)*, 2009 FC 1265.

V. REITERATION OF THE SUBSTANTIVE ACTA SOUGHT, LEGAL MAXIMS, AND THE DOCTRINE OF METADATA RELEVANCY

10. It is unequivocally assented to and averred herein that the substantive acta (the “**Requested Records**”) sought—namely, objective, administrative, and technological procurement data collection application programming interfaces, Azure cloud utilization logs, and structural metadata validations—must be disclosed systematically and without further delay.
11. The application of the foundational legal maxim codified by Herbert Broom, *expressio unius est exclusio alterius* (the explicit mention of one thing is the exclusion of another), dictates that within subsection 9(1) strictly excludes any non-enumerated reasons—including generalized “processing” backlogs—from possessing legal validity.
12. Furthermore, the maxim *quando aliquid mandatur, mandatur et omne per quod pervenitur ad illud* (when the law commands a thing, it commands the means to attain it) compels the Government Institution to query, filter, and extract the embedded database logs traversing the CPIC and cloud-based repositories. The extraction of these architectural logs is inextricably tethered to the *Commissioner v. Minister of National Defence*, 2011 SCC 25, wherein it was elucidated that an institution cannot evade disclosure by burying records within a complex administrative apparatus.
13. Finally, considering that the programmatic spoofing of a standard provincial court output irreparably de-authenticates the physical instrument under scrutiny, reliance must be placed upon the original source. The subversion of jurisdictional integrity via automated backend algorithms demands the uncompromising disclosure of the digital architectures that facilitated such anomalies to the public.

VI. TABULAR COMPUTATION OF TIME AND STRICT ENFORCEMENT

14. For the purpose of absolute administrative clarity, and to eradicate any ambiguity regarding the maturation of vested rights, the governing timeline is delineated below:

Procedural Milestone	Statutorily Recognized Date	Legal Consequence
Effectuated Delivery of the Access Request	May 7, 2026	Commencement of the thirty-day limitation period, triggering the statutory duty to assist.
Government Institution Acknowledgment	May 11, 2026	Confirmation of receipt; failure to articulate valid extension grounds or duration, rendering delay mechanism inoperative.

1304

Mandatory Disclosure Deadline	June 8, 2026	Crystallization of the absolute statutory deadline for unredacted remittance of records (thirty days mathemati

VII. CONCLUDING DIRECTIVES AND ANTICIPATED COMPLIANCE

15. It is respectfully submitted that, given the absolute nullity of the presumed extension, the failure to consummate complete, unredacted disclosure by today, June 8, 2026, operates *ipso facto*
16. Strict, uncompromising compliance with the *Access to Information Act*, R.S.C. 1985, c. A-1 is anticipated forthwith, alongside a prompt, substantive, and unambiguous response to the inquiry.
- The utilization of rolling disclosure for all discrete architectural logs and procurement matrices is expected immediately.
17. I look forward to receipt of the same by the end of the business day with thanks.

Sincerely,

Mr. Kevin A. McLean (B.A., J.D., CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Mon, May 11, 2026 at 3:03 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:

DELIVERY METHOD: Via Electronic Transmission **CLASSIFICATION:** Private and Confidential **DATE:** May 11, 2026

TO: Access to Information and Privacy (ATIP) Branch Royal Canadian Mounted Police 73 Leikin Drive, Mail Stop #61 Ottawa, Ontario K1A 0R2 Email: ATIP-AIPRP@rcmp-grc

FROM: Kevin A. McLean (B.A., J.D., CIM) Email: mcleansettlement@gmail.com

SUBJECT: FORMAL NOTIFICATION OF OIC COMPLAINT FILING, DEMAND FOR STATUTORY ADHERENCE, AND REITERATION OF UNAVOIDABLE SEARCH PARAMETERS

I. FORMAL NOTIFICATION OF COMPLAINT TO THE INFORMATION COMMISSIONER

1. Please be advised that, predicated upon the facially void and statutorily non-compliant administrative response transmitted by your office on May 11, 2026, a formal complaint was filed with the Information Commissioner of Canada (the "OIC").
2. The aforementioned complaint, promulgated pursuant to section 30 of the *Access to Information Act*, R.S.C. 1985, c. A-1, formally challenges the Government Institution's issuance of an unlawful extension devoid of statutory grounding, and the resulting state of constructive refusal.
3. Annexed hereto for your immediate administrative review are the complete, filed complaint documents, inclusive of the OIC Summary of Complaint corroborating the foregoing.

II. DEMAND FOR STRICT STATUTORY ADHERENCE AND CITATION OF GROUNDS

4. The Government Institution is hereby strongly urged to rectify its procedural posture and strictly follow the governing legislative framework. The reliance upon boilerplate "currently proceeding"—operates as an absolute nullity *ab initio* and subverts the foundational transparency mandates established by Parliament.
5. Should the Government Institution genuinely maintain that a temporal extension is necessitated, it is formally demanded that your office immediately cure this defect by providing statutory grounds relied upon pursuant to subsection 9(1) of the *Access to Information Act*, R.S.C. 1985, c. A-1 (specifically identifying paragraph a, b, or c).
6. The failure to articulate a crystallized statutory exemption and a definitive temporal boundary renders the current processing status legally void. Furthermore, explicit confirmation to the Information Commissioner pursuant to subsection 9(2) remains outstanding and is hereby re-demanded.

III. PRESERVATION OF THE ORIGINAL ACCESS REQUEST SCOPE

7. It is imperatively noted that the Government Institution must formally confirm that the access request is encapsulated and being processed precisely as it was originally submitted by internal administrative reductionism.
8. The scope of the request is immovably anchored to the extraction of objective, administrative, and technological procurement data concerning GrapeCity and MESCIUS. This inextricably includes the underlying application programming interfaces (APIs), Azure cloud utilization logs, vendor technical specifications, and structural metadata.
9. As elucidated in the foundational jurisprudence of *Canada (Information Commissioner) v. Minister of National Defence*, 2011 SCC 25, the Government Institution cannot exclude deeply integrated software supply chains and backend infrastructure. Any attempt to artificially bifurcate or narrow the parameters of this search away from the statutory duty to assist.

IV. CONCLUDING DIRECTIVES

10. The Government Institution is formally directed to integrate these uncompromising parameters into its search methodology and to promptly issue a statutorily compliant response meeting the above-stated extension criteria.
11. The prompt, unredacted, and comprehensive transmission of the requisite technological and architectural procurement logs remains anticipated by the crystallized statutory obligation.

Sincerely,

Mr. Kevin A. McLean (B.A., J.D., CIM)

ENCLOSURES:

1. Formal Complaint Filed with the Office of the Information Commissioner (May 11, 2026)
2. Summary of Complaint from the Information Commissioner of Canada

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

1305

Fax: 416.981.7117

Phone number: 647.370.9354

On Mon, May 11, 2026 at 12:03 PM Mr. Kevin McLean <mcleansettlement@gmail.com> wrote:**DELIVERY METHOD:** Via Electronic Transmission**CLASSIFICATION:** Private and Confidential**DATE:** May 11, 2026**TO:** Access to Information and Privacy (ATIP) Branch

Royal Canadian Mounted Police

73 Leikin Drive, Mail Stop #61

Ottawa, Ontario K1A 0R2

Email: ATIP-AIPRP@rcmp-grc.gc.ca

Attention: Bryan, ATIP Coordinator

FROM: Kevin A. McLean (B.A., J.D., CIM)Email: mcleansettlement@gmail.com**SUBJECT: NOTICE OF STATUTORY NON-COMPLIANCE, DEMAND FOR STRICT COMPUTATION OF TIME, AND MANDATORY INQUIRY PURSUANT TO SECTION 9****I. PRELIMINARY ASSERTIONS, ACKNOWLEDGMENT OF RECEIPT, AND LEGISLATIVE INTENT**

1. Receipt is hereby formally acknowledged concerning the electronic transmission dated May 11, 2026 (the "**Administrative Response**"), which purports to acknowledge (the "**Access Request**") promulgated under the statutory authority of the *Access to Information Act*, R.S.C. 1985, c. A-1. The aforementioned legislation is fundamental to the illumination of governmental administrative functions; therefore, Government Institution responses must strictly adhere to the legislative parameters designed to ensure transparency.
2. It is observed that the aforementioned Administrative Response is *prima facie* non-compliant, insofar as it ostensibly seeks to orchestrate an extension of time without exclusively upon generalized, boilerplate vernacular—stating merely that the Government Institution is "currently proceeding"—while conspicuously failing to explicitly justify the extension.
3. The imposition of vague processing notifications, devoid of concrete statutory anchoring, creates an impermissible ambiguity that severely prejudices the requester. In exemption, the Government Institution attempts to unilaterally rewrite the temporal constraints of the *Access to Information Act*, R.S.C. 1985, c. A-1, thereby insulating itself from scrutiny.

II. STRICT STATUTORY CONSTRUCTION, PROCEDURAL FAIRNESS, AND THE DOCTRINE OF NULLITY

4. The Government Institution obligations regarding the unilateral protraction of disclosure deadlines are strictly circumscribed by the *Access to Information Act*, R.S.C. 1985, c. A-1. The Act mandates that any extension must be inextricably tethered to the enumerated statutory preconditions, requiring the issuance of a formal notice of extension (the "guideline"), but rather a mandatory jurisdictional prerequisite for the lawful elongation of the processing continuum.
5. The failure to explicitly invoke paragraphs 9(1)(a), 9(1)(b), or 9(1)(c) within the Administrative Response precludes any lawful elongation of the thirty-day statutory window. *Broadcasting Corporation*, 2010 FCA 315 (and its antecedent *Statham v. Canadian Broadcasting Corporation*, 2009 FC 1028), a Government Institution's failure to strictly adhere to section 9 of the Act strictly invalidates the attempted delay. The Federal Court of Appeal's reasoning in *Statham* underscores that the right to see documents is a fundamental principle of administrative law. Any attempt to rely upon ambiguous administrative processing as a *de facto* extension operates to elevate this defect beyond a mere procedural irregularity; it is, unequivocally, an absolute nullity *ab initio*.
6. This principle of rigid procedural stricture is further corroborated by *Hydro-Québec v. Canada (National Energy Board)*, 1997 CanLII 5025 (FC) and *Hydro-Québec v. Canada (Attorney General)*, 2013 FC 1028. The Federal Court emphatically held that a Government Institution's failure to comply with the rigid notice requirements and time limits mandated by section 9 inherently vitiates the process. To permit a Government Institution to obscure the strict computation of time *in limine* without articulating the precise legal exemption framework, rendering the statutorily entrenched right of access entirely illusory and subjecting the requester to indefinite bureaucratic limbo.
7. Furthermore, the application of the legal maxim *expressio unius est exclusio alterius* (the explicit mention of one thing is the exclusion of another) dictates that by Par within section 9(1), all other non-enumerated reasons—including generalized "processing" delays or administrative backlog—are strictly excluded from legal validity.

III. MANDATORY STATUTORY INQUIRY CONCERNING OVERSIGHT BY THE INFORMATION COMMISSIONER

8. In direct alignment with the imperative to ensure uncompromising adherence to the governing legislative framework, a formal inquiry is hereby advanced pursuant to the *Access to Information Act*, R.S.C. 1985, c. A-1. The Supreme Court of Canada in *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, 2006 SCC 13, alongside the foundational parameters established in *1992 CanLII 15386 (FC)*, affirms that the invocation of a section 9 extension is an extraordinary statutory mechanism requiring strict adherence to systemic oversight by the Information Commissioner.
9. The statutory requirement to notify the Information Commissioner serves as an indispensable systemic safeguard against Government Institution overreach and the erosion of public trust. The independent parliamentary ombudsman maintains contemporaneous surveillance over departments that seek to deviate from standard disclosure timelines.
10. **FORMAL INQUIRY:** Has the Royal Canadian Mounted Police provided the requisite statutory notice to the Information Commissioner of Canada, as is strictly necessitated by the Act? The provision of such notice is a non-derogable obligation, as similarly demonstrated in the procedural chronologies of *Coderre v. Canada (Office of the Information Commissioner)*, 2015 FC 1028. Notification was subjected to rigorous judicial scrutiny.
11. Should the Government Institution be operating under the presumption of an extended temporal mandate, the immediate provision of the documentary evidence demanded. The failure to produce such corroborating documentation will be construed as an admission of non-compliance with subsection 9(2), further rendering any extension null and void.

IV. REITERATION OF THE SUBSTANTIVE ACTA SOUGHT, IMPERMISSIBLE NARROWING, METADATA RELEVANCY, AND THE DUTY TO ACCESS

12. It is unequivocally assented to and averred herein that the Royal Canadian Mounted Police Privacy and Access to Information Division has construed the Access Request substantively *acta* sought—namely, objective, administrative, and technological procurement data concerning GrapeCity and MESCIUS software development kits (the "substantive acta"). The request is not for the evasive administrative reductionism.
13. The extraction of these precise procurement and architectural logs is predicated upon cryptographically sound forensic metadata extrapolated from a facially void container. Such embedded technological records, reliance is firmly placed upon the jurisprudential framework established in *Canada (Information Commissioner) v. Minister of Health*, 2015 FC 1028.
14. In *National Defence*, the Supreme Court of Canada elucidated that the *Access to Information Act*, R.S.C. 1985, c. A-1 mandates a robust and expansive interpretation of the Act. The Court explicitly rejected the premise that a Government Institution could circumvent the Act by burying records within a complex administrative apparatus, provided the Government Institution maintained the legal right to access and govern the records.
15. The application of the law to the facts dictates that the Government Institution cannot artificially narrow the scope of the search to exclude backend application programs simply because they are subsumed within macro-vendor architecture (e.g., Microsoft Azure cloud environments or Axon evidence ecosystems). To obfuscate these records from the requester, the Government Institution must demonstrate a compelling and lawful basis for withholding, such as the protection of personal information or the prevention of the disclosure of information that could harm the national defense or the security of Canada.
16. Furthermore, the foundational legal maxim codified by Herbert Broom, *quando aliquid mandatur, mandatur et omne per quod pervenitur ad illud* (when the law commands a thing to be done, the law commands everything by which it is done), is applicable. The statutory mandate to provide access *ipso facto* compels the Government Institution to proactively deploy the requisite internal technological means to ensure the CPIC and cloud-based repositories. The Government Institution cannot passively rely upon superficial search methodologies when the requested records reside in a complex, multi-layered system.
17. Additionally, should the Government Institution locate responsive records incrementally, the doctrine of rolling disclosure must be rigidly applied. As affirmed in the *1992 CanLII 15386 (FC)*, *Public Service Commission (Re)*, 2011 CanLII 47546 (NL IPC), and *Public Service Commission (Re)*, 2011 CanLII 47547 (NL IPC), a Government Institution's failure to release records that are ready for release until the entirety of the archival corpus has been processed. Responsive records, particularly those that are ready for release, must be systematically remitted as they become available to prevent the weaponization of delay.

1306

V. PREEMPTIVE REBUTTALS TO POTENTIAL STATUTORY EXTENSIONS AND ABUSE OF DISCRETION

18. To preclude any subsequent, retroactive attempts to legitimize a delay or to unilaterally impose an extension *ex post facto*, the following preemptive rebuttals are for the *Access to Information Act*, R.S.C. 1985, c. A-1, supported by an exhaustive corpus of federal jurisprudence:
- **NOTA BENE (I) - Rebuttal to Section 9(1)(a) (Unreasonable Interference/Large Volume):** Should the Government Institution attempt to leverage section 9(1)(a) to necessitate a search through a voluminous repository, such an assertion is preemptively neutralized. While extensions for volume are statutorily permissible (see *Sheldon v. Canada (Health)*, 2015 FC 1385), they are subject to strict judicial scrutiny for objective reasonableness, as determined in *Burlacu v. Canada (Access Request)*. The Access Request provides highly targeted, discrete parameters (specifically, Software Licensing Supply Arrangements, National Technology Onboarding Program). The utilization of modern enterprise querying tools, SQL database filtration, and automated discovery algorithms renders the identification of these specific records reasonably be construed as an interference with Government Institution operations when the parameters are this technologically precise. Therefore, any attempt to extend the excessive three-year extension unequivocally struck down in *Canada (Attorney General) v. Canada (Information Commissioner) (T.D.)*, 2002 FCT 136—was an act of administrative bad faith.
 - **NOTA BENE (II) - Rebuttal to Section 9(1)(b) (Necessity of Consultations):** Should the Government Institution purport that external consultations are necessary, litigated in cases such as *Bronskill v. Canada (Canadian Heritage)*, 2011 FC 983, *Public Service Alliance of Canada v. Canada (Attorney General) (T.D.)*, 1990 CanLII 13047 (FC)—it is respectfully submitted that such assertions are facially invalid in this context. The records sought—internal Information Technology architectural deployment schematics—are inherently intra-departmental records. They are autonomously managed by the Shared Services Canada liaison branch and directorates. The internal routing of inquiries between divisions of the same Government Institution apparatus does not satisfy the legal threshold for "consultations." The software license or the retrieval of a procurement matrix does not trigger a mandatory consultative burden involving third-party intelligence agencies or foreign governments.
 - **NOTA BENE (III) - Rebuttal Concerning Deemed Refusals upon Expiration of Self-Extended Deadlines:** It is imperatively noted that a Government Institution's sequential extensions to effectively perpetually embargo information (see the admonitions in *University of New Brunswick (Re)*, 2021 NBOMB 4). As definitively established in *Commissioner v. Canada (National Defence)*, 2015 FCA 56 (upholding *Canada (Information Commissioner) v. Canada (National Defence)*, 2014 FC 205), a Government Institution upon which its asserted extension expires enters an immediate state of deemed refusal. Furthermore, the failure to provide access within the statutorily extended deadline against the Government Institution, as evidenced in *Dagg v. Canada (Industry)*, 2010 FCA 316 and *Dagg v. Canada (Industry)*, 2009 FC 1265. The Federal Court's recalcitrance once a self-imposed deadline has lapsed.

VI. TABULAR COMPUTATION OF TIME AND STRICT ENFORCEMENT

19. For the purpose of absolute administrative clarity, and to eradicate any Government Institution ambiguity regarding the maturation of rights, the governing timeline is as follows:

Procedural Milestone	Statutorily Recognized Date	Legal Consequence
Effectuated Delivery of the Access Request	May 7, 2026	Commencement of the thirty-day limitation period, triggering the statutory duty to assist
Government Institution Acknowledgment	May 11, 2026	Confirmation of receipt; failure to articulate valid extension grounds, rendering delay moot
Mandatory Disclosure Deadline	June 6, 2026	Crystallization of the absolute statutory deadline for unredacted remittance of records

VII. CONCLUDING DIRECTIVES AND ANTICIPATED COMPLIANCE

20. It is respectfully submitted that any failure to consummate the complete, unredacted disclosure by the statutorily mandated temporal threshold of June 6, 2026, will be deemed to necessitate immediate escalation, potentially encompassing the filing of a formal complaint with the Office of the Information Commissioner or the initiation of an application for judicial review.
21. Strict, uncompromising compliance with the *Access to Information Act*, R.S.C. 1985, c. A-1 is anticipated, alongside a prompt, substantive, and unambiguous response to the Information Commissioner. The utilization of rolling disclosure for all discrete architectural logs and procurement matrices is expected forthwith.

Sincerely,

Mr. Kevin A. McLean (B.A., J.D., CIM)
Enclosures

APPENDICES

Appendix #1: Statutory and Prescribed Sections: Extension of Time Limits

Access to Information Act, R.S.C. 1985, c. A-1

9 (1) The head of a government institution may extend the time limit set out in section 7 or subsection 8(1) in respect of a request under this Part for a reasonable period of time if

- (a) the request is for a large number of records or necessitates a search through a large number of records and meeting the original time limit would unreasonably interfere with the operations of the government institution;
- (b) consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit, or
- (c) notice of the request is given pursuant to subsection 27(1)

by giving notice of the extension and, in the circumstances set out in paragraph (a) or (b), the length of the extension, to the person who made the request within thirty days after the day on which the person has a right to make a complaint to the Information Commissioner about the extension.

Notice of extension to Information Commissioner

(2) Where the head of a government institution extends a time limit under subsection (1) for more than thirty days, the head of the institution shall give notice of the extension to the person who made the request within thirty days after the day on which the person has a right to make a complaint to the Information Commissioner about the extension.

R.S., 1985, c. A-1, s. 92019, c. 18, s. 41(E)

Access to Information Regulations, SOR/83-507

Procedures

4 (1) A request for access to a record under Part 1 of the Act must be made by forwarding to the appropriate officer of the government institution that has control of the record

- (a) a completed Access to Information Request Form; or
- (b) a written request that provides sufficient detail to enable the officer to identify the record.

(2) If the information contained in the request is insufficient to establish that the person making the request has a right of access under section 4 of the Act, the government institution may require the person to provide further information in order to confirm their right of access.

SOR/85-395, s. 1 SOR/93-114, s. 1 (F) SOR/2023-156, s. 1

5 If access is to be given to a record that contains personal information about the person who requested access, the government institution must require the person to provide identifying information to disclose unless the person's identity has already been confirmed.

Appendix #2: List of Authorities

1307

1. *Albatal v. Canada (Citizenship and Immigration)*, 2014 FC 1026 (CanLII)
2. *Bronskill v. Canada (Canadian Heritage)*, 2011 FC 983 (CanLII), [2013] 2 FCR 563
3. *Burlacu v. Canada (Public Safety and Emergency Preparedness)*, 2022 FC 1290 (CanLII)
4. *Canada (Attorney General) v. Canada (Information Commissioner) (T.D.)*, 2002 FCT 136 (CanLII), [2002] 4 FC 110
5. *Canada (Information Commissioner) v. Canada (National Defence)*, 2014 FC 205 (CanLII), [2015] 2 FCR 786
6. *Canada (Information Commissioner) v. Canada (National Defence)*, 2015 FCA 56 (CanLII), [2016] 1 FCR 213
7. *Canada (Information Commissioner) v. Minister of National Defence*, 2011 SCC 25 (CanLII), [2011] 2 SCR 306
8. *Coderre v. Canada (Office of the Information Commissioner)*, 2015 FC 776 (CanLII)
9. *Cyanamid Canada Inc. v. Canada (Minister of Health and Welfare)*, 1992 CanLII 15386 (FC)
10. *Dagg v. Canada (Industry)*, 2009 FC 1265 (CanLII)
11. *Dagg v. Canada (Industry)*, 2010 FCA 316 (CanLII)
12. *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, 2006 SCC 13 (CanLII), [2006] 1 SCR 441
13. *Hydro-Québec v. Canada (National Energy Board)*, 1997 CanLII 5025 (FC)
14. *Hydro-Québec v. Canada (National Energy Board)*, 1997 CanLII 17697 (FC)
15. *Public Service Alliance of Canada v. Canada (Attorney General)*, 2011 FC 649 (CanLII)
16. *Public Service Commission (Re)*, 2011 CanLII 47545 (NL IPC)
17. *Public Service Commission (Re)*, 2011 CanLII 47546 (NL IPC)
18. *Public Service Commission (Re)*, 2011 CanLII 47547 (NL IPC)
19. *Sheldon v. Canada (Health)*, 2015 FC 1385 (CanLII)
20. *Statham v. Canadian Broadcasting Corporation*, 2009 FC 1028 (CanLII), [2010] 4 FCR 216
21. *Statham v. Canadian Broadcasting Corporation*, 2010 FCA 315 (CanLII), [2012] 2 FCR 421
22. *University of New Brunswick (Re)*, 2021 NBOMB 4 (CanLII)
23. *X v. Canada (Minister of National Defence) (T.D.)*, 1990 CanLII 13047 (FC), [1991] 1 FC 670

Warm regards,

Mr. Kevin A. McLean (BA, JD, CIM)

Chartered Investment Manager

Email: mcleansettlement@gmail.com

Fax: 416.981.7117

Phone number: 647.370.9354

On Mon, May 11, 2026 at 10:40 AM ATIP / AIPRP <ATIP-AIPRP@rcmp-grc.gc.ca> wrote:

Dear Kevin McLean:

This is to acknowledge receipt of your request under the Access to Information Act, which was received by this office on May 8, 2026, for:

Formal request under the Access to Information Act (ATIA) - software procurement, licensing, NTOP onboarding, embedded it architecture, and azure cloud u

**This request is strictly focused on objective, administrative, and technological procurement data regarding specific enterprise-grade software capabilities de
Technology (IT) ecosystem, specifically intersecting with the RCMP's "Cloud-First" regulatory framework and backend server-side document manipulation in**

Please be advised that we are currently proceeding with your request. The Royal Canadian Mounted Police is committed to assisting you with your request and we will er complete, accurate and timely response.

Please be advised that you are entitled to lodge a complaint with the Information Commissioner concerning the processing of your request within 60 days of receipt of this notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street, 7th Floor
Gatineau, Quebec K1A 1H3

For additional information on the complaint process, or to file a complaint online: <https://www.oic-ci.gc.ca/en/you-submit-complaint>

Should you wish to discuss this matter further, please contact us at ATIP-AIPRP@rcmp-grc.gc.ca. Please quote our file number appearing in this email.

Regards,

Bryan
Access to Information and Privacy Branch
Mailstop #61
73 Leikin Drive
Ottawa, Ontario K1A 0R2

CONFIDENTIALITY NOTICE:

This e-mail message, including attachments, is confidential and is only directed to the recipient listed above. If you have received this e-mail by error or you are not the ir disclosure, or other) of this e-mail is strictly forbidden. You are requested to immediately advise me of the error and destroy the e-mail on your computer.

TAB 39

Tab A

Ottawa

These restaurants are finding the recipe for success in a pandemic

With low overhead and a steady appetite for curbside pickup, business is booming

[Hallie Cotnam](#) · CBC News · Posted: May 06, 2020 4:00 AM EDT | Last Updated: May 6, 2020



Listen to this article ⓘ

Estimated 6 minutes



No big points for plating or presentation, but patrons of a brand new restaurant in Westboro are snapping up dinner to go nonetheless. (Francis Ferland/CBC)

It's not fine dining, it's takeout in a brown paper bag. But the new business model is turning out to be a lifeline for some restaurants shuttered by COVID-19.

Pre-ordered, prepaid, prix fixe menus are selling out fast. Overhead costs are way down. And if the profits aren't setting records, at least they're paying the bills.

Here's how two restaurateurs are surviving, and maybe even thriving, through the pandemic.

NeXT

Owner-chef Michael Blackie and his wife Jillian were celebrating their 25th anniversary in Southeast Asia when COVID-19 hit. That cut their trip short, but it also

gave Blackie an idea.

"In Bangkok they were doing daily temperature checks every time we came in the [hotel]," he said. "So [I said to my staff at Stittsville's NeXT], 'Guys, I want daily temperature checks. I want somebody at the door.' And they said, 'I don't think Ottawa is ready for that, chef.'"

Blackie closed his restaurant March 15, with a plan to revisit the decision every two weeks. "We'd just come off one of the best years that NeXT had ever seen. We had a bit of a war chest. So I thought, let's just chill."



Owner-chef Michael Blackie of NeXT in Stittsville works alongside his colleagues in the kitchen. This photo was taken before physical distancing rules took effect. (Nicole Farough)

About three weeks ago, Blackie reached out to his executive chef with a better idea: "Let's do NeXT 2.0. Let's figure this out."

The restaurant opened for takeout on April 23, offering curbside pickup.

"We put it in your vehicle. There's no risk," Blackie said. "I've had people come up with Post-its on their windows and full vapour barriers inside their car. I'm like, 'You're just

missing a biohazard suit, dude."

But they keep coming.

"I've blown my expectations out of the water," Blackie said. "I would say I'm within 80 per cent of my normal [dine-in] revenue. My best night was \$10,250" — similar to a great night pre-pandemic, but "minus a lot of the overhead," he said.

"I have no front of the house service staff," Blackie said. "There are no glasses to clean. There's no cutlery to clean. There are no tables to reset. There are no toilets to have to clean up because the guests can't come into the building."

**“I could actually go all the way
until the vaccine's found.”**

- Michael Blackie, NeXT

He's also working fewer hours per day than his typical pre-pandemic 13. "We're going into work around noon and we're leaving at 8 p.m."

Blackie said customers seem to prefer to pick up their orders rather than use a food delivery app. "[Patrons] show up as a couple," Blackie said. "I say, 'How was the drive date?'"

On the downside, weddings and corporate functions that used to represent a big part of Blackie's business have been cancelled or postponed.

"Am I going to be in the hole for thousands and thousands of dollars? I don't think so," he said. "Am I going to have the same profit as 2019? Absolutely not."

Blackie and his wife are so buoyed by the takeout success, they're opening a "ghost" restaurant next week called Dirtyburger. It'll be run out of the same kitchen, but with a different website and menu.

"I could do this for another year. I could actually go all the way until the vaccine's found," Blackie said.



Arup Jana and Maggie Von Zur-Muehlen in front of their newly opened Westboro eatery, Brassica. Prepaid pickup orders are placed on an overturned milk crate, while chalk Xs on the sidewalk mark off two-metre spaces where customers can wait. (Francis Ferland/CBC)

Brassica

It's been a rough 14 months for Arup Jana and his wife, Maggie Von Zur-Muehlen. Their Holland Avenue restaurant Allium burned down in March 2019. While waiting for reconstruction, they partnered with the owners of Vittoria in the Village, who were also waiting for a post-fire rebuild of their main restaurant in the ByWard Market.

Brassica opened at the end of January. Less than two months later, COVID-19 struck.

At first, Jana shut it all down. "I didn't really want to draw people out of their house, into the public. It felt really like it was important for people to stay home," he said.

But, "being home for three weeks and doing nothing was terrible," Jana said. "I mean, the first few days [it was] nice to be off. We had just opened the restaurant, so that was two months of craziness. But then it just got really old, very fast."



How one Ottawa restaurant is adapting to physical distancing

May 6, 2020 | 1:32

Arup Jana and Maggie Von Zur-Muehlen, co-owners of Brassica in Westboro, say they've reduced their volume, cut staff and created a system for picking up takeout orders that limits contact between customers.

Jana was also feeling financial pressure with the expensive Westboro rent. Their landlord had delayed their rent by a month, but they were still expected to pay in instalments.

So they figured out a way to offer takeout safely without using delivery apps. Jana takes orders and preps on Wednesdays and Thursdays, and they're open for pickup Friday through Sunday.

Jana is at capacity preparing about 80 portions a day. They post the menu on Tuesday morning on Instagram, and by 1 p.m. it's all sold out.

Still, that represents far fewer customers than their pre-pandemic business, when they could serve 120 in a night. "Our sales are down about 60 per cent or 70 per cent," he said.

“I think we could do it for another couple of months.”

- Arup Jana, Brassica

So, too, is their payroll. From a staff of nine, they're down to just two: Jana and Von Zur-Muehlen. But what they're saving in staffing costs, they're losing because of their reduced prices.

"We're not charging the same as we would if people were in the restaurant," Jana said. "We can't put thought and presentation into the [dishes]. It's less detailed."

So how long can they keep it up?

"I think we could do it for another couple of months," Jana said. "We really need to sit down and see where we are financially. We're definitely making some money, but I'm not sure exactly where we stand."

Nor is he sure what the future of his business will look like once restaurants are allowed to reopen.

"Will people want to be so close together? Our tables aren't far apart. Will people feel comfortable in that same area? I don't even know if I'm going to feel comfortable in that scenario."



More than the headlines. Subscribe to You Otta Know, the CBC Ottawa weekly newsletter.

Email address:

Subscribe

Popular Now in News

- 1

ANALYSIS
Carney confronts our national home reno nightmare at 24 Sussex
- 2

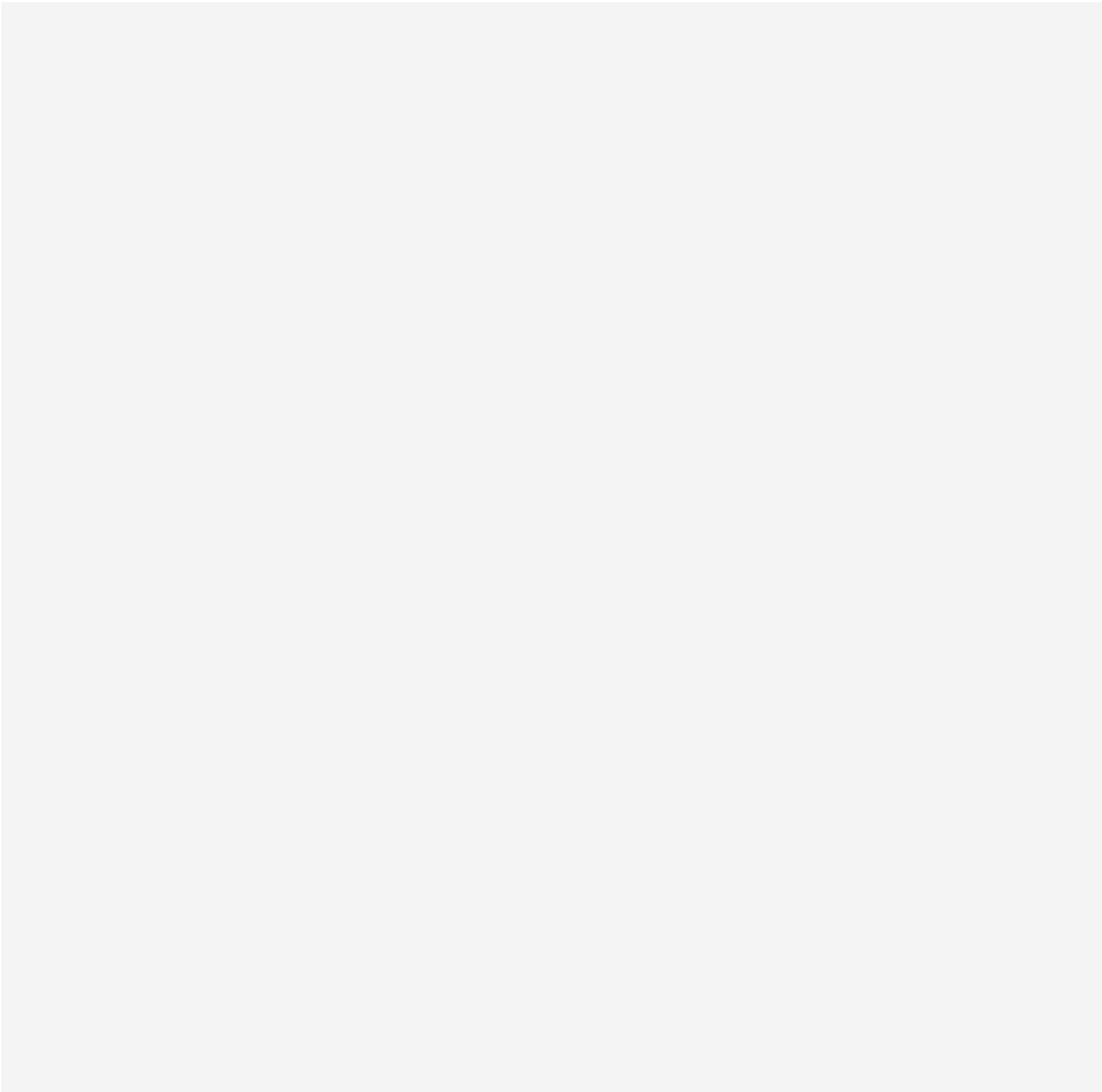
IN PHOTOS | Here's what the run-down 24 Sussex looks like inside
- 3

UPDATED
Maple Leafs make forward Gavin McKenna first pick of NHL draft
- 4

Canada's most wanted fugitive, a Quebecer, arrested in Spain
- 5

Ex-husband found guilty of murdering Tatjana Stefanski in B.C. Interior





Ottawa

Some restaurants pivoting to takeout for New Year's Eve

Restaurateurs say cancellations, staff safety and rising case counts factor into decisions

[Matthew Kupfer](#) · CBC News · Posted: Dec 30, 2021 4:00 AM EST | Last Updated: December 30, 2021



Listen to this article ⓘ

Estimated 3 minutes



Maggie von zur-Muehlen, co-owner of the Brassica restaurant in Westboro, says concerns about transmission among in-person diners and the climbing case counts in Ottawa led to the decision to only offer take out this New Year's Eve. (Olivier Periard/CBC)

Few people are as ready to say goodbye to 2021 as those in the restaurant industry and some establishments have taken the extra step of opting to go takeout-only for what's typically one of the biggest nights of the year.

Emily Ienzi, co-owner of two six {ate} in Little Italy, said the decision came after a week of cancellations and seeing case counts climbing in Ottawa.

"Every restaurateur that I speak to is a little on-edge, their staff are nervous and we're nervous. It's not a comfortable feeling to go to work feeling scared," she said.

- [Restaurants facing 'lockdown by stealth' call for government for support](#)

Ienzi said the small restaurant just couldn't accommodate New Year's revellers safely given the increased transmissibility of Omicron.

The take-home option has sold out in the meantime, Ienzi said — with 90 orders set to go out Dec. 31 — though that won't include the same kind of alcohol spending that comes with a typical New Year's Eve.

"It definitely has been a rough December. Not the December we were hoping for," Ienzi said.

Brassica co-owner Maggie von zur-Muehlen said seeing Ottawa's case counts break records had the team looking to adapt ahead of the curve — they've sold out their special takeout menu.

"Rather than being told that we had to shut down, we kind of wanted to make the decision to shut down and thus not waste a bunch of food and restructure what we're offering for take out," von zur-Muehlen said.

"There was more a sense of gratitude that we're trying to keep everybody safe."

Some dining rooms still open

Even restaurants that are offering diners an in-person experience have had to scale back the festivities as people cancel reservations at the last minute.

"We're just doing our regular menu, takeout, deliveries and people who wish to come in — it's a safe place to come in," said Joe Thottungal, chef and owner at Thali.



Thali chef and owner Joe Thottungal, shown here in 2019, said recent last-minute cancellations have led him scrapping plans for a special New Year's Eve menu, but he will be opening his dining room following public health guidelines. (Evan Bergstra)

New Year's Eve is a major day in the calendar for restaurant owners, Thottungal said, especially ahead of a seasonal drop in business in January.

"These are one of the best dates we should have," he said.

Fairouz Cafe in the ByWard Market is encouraging people opt for takeout, they will be offering their New Year's Eve menu for two cohorts of about 20 customers who will be seated according to public health protocols on Dec. 31.

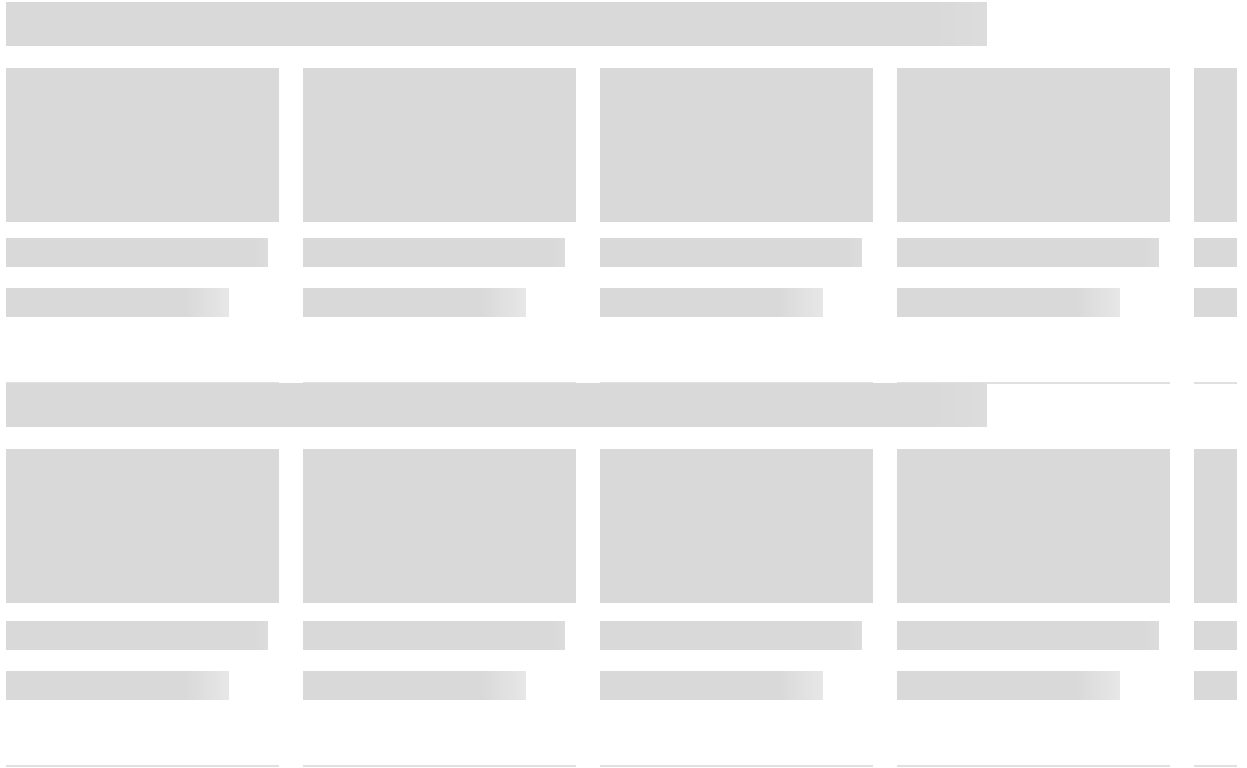
Co-owner Tony Garcia said closing down in recent days allowed the restaurant time to adapt to reduce capacity and accommodate people with health concerns who didn't feel comfortable serving customers.

"There were a lot of nerves the last few weeks. The Christmas break closing kind of gave people an opportunity to step back," Garcia said.



Fairouz Café in the ByWard Market said it is encouraging people order takeout, but it is offering limited dine-in space for New Year's Eve. (Kevin Belanger)

Garcia said remaining open gives people who do need to work the option to do so at an important time of year.





What's new?

Published on March 8, 2020

Share

Inspir
Cor



on



Ottawa has some new gems on the dining front that are turning heads not only for the calibre of their food, but also for their genuine and comprehensive approach to hospitality.

Grunt

It might seem like an unusual neighbourhood for haute cuisine, but Chef Jason McLelland intentionally chose Mechanicsville when he opened Grunt last May. A native of Scotland who has cooked at some of the top spots around the world, Jason says that he wants to show people that fine dining doesn't need to be expensive and flashy to be intriguing.

With just 22 seats, Grunt offers a cozy, modest environment with rustic barn board throughout and interesting art on the walls. You can watch this genial chef at work in the open kitchen; he might ferry your plates to your table, or it might be his gracious, friendly wife Marie.

A short but well-chosen wine list complements the equally-brief food menu, which changes every two weeks. Among the many popular dishes that have been featured are an inventive take on the porchetta sandwich and a gnocchi Parisienne in carbonara sauce. Vegan and vegetarian options are always available. Dessert is always a standout; recent selections have included sticky toffee pudding, upscale bread and butter pudding, and a gorgeous squid ink meringue with strawberry ice cream and peppered strawberries.

With a name like Grunt you might think it's a meat-centric restaurant but there's more to the story. "This is my time," says Jason. "I worked for others at a very high level for so long, making outstanding food and helping sell excellence. But when you're grunting it out for others, there's a lot that goes on that guests never know about. Now I get to do things my way and be open and transparent about it. I want people to see it doesn't have to cost a fortune to eat well and I want this place to be a springboard for making change in the industry."

Gitanes

While the name of this new Elgin Street eatery might conjure up notions of French sophisticates, rest assured that Gitanes is a comfortable, welcoming spot.

Ottawa native Mitch Lacombe serves as the chef de cuisine at Gitanes, leveraging his experience at Riviera and Restaurant e18hteen. He helped develop the menu with executive chef Luke Reyes, who is one of the restaurant's owners. It reflects classic French culinary traditions, fused with local, Canadian ingredients. "We serve dishes that people can recognize as comfort food and which are accessible, yet elevated with unusual touches," says Mitch.

The cold seafood bar is a highlight of any visit to Gitanes—from oysters to sea urchin to king salmon crudo, there is an ever-changing array of delights. Popular entrees include French onion soup—complete with bone marrow on top to scoop out into the dish—as well as vegetarian options such as mushroom Bolognese on vegan pasta or a delicate celery salad with spicy pickled raisins, toasted hazelnuts and

Quebec blue cheese. For a real indulgence, the chef's table in the kitchen seats six for a lively, interactive experience.

After 10 pm, a late night menu takes over, making Gitanes popular among workers in the restaurant industry. "It's a homage to the original OZ Kafe which was in this space for many years and was a bustling late-night spot," explains Mitch.

Don't miss a chance to try one of Gitanes' creative cocktails. If you're lucky, you might even be seated at the one table which features a "press here for champagne" button, summoning a cart full of interesting bottles of bubbly. It's a casual, fun place, offering diners a culinary experience that is unique in Ottawa.

Brassica

Chef Arup Jana gained legions of fans with his first restaurant, Allium, which is due to reopen this summer after a devastating fire in February 2019. Together with his wife Maggie Von zur-Muehlen, Arup has just opened a new spot in Westboro called Brassica. It is the genus name for the plant family which includes kale, Brussels sprouts, cabbage and broccoli—all among the chef's favourites. Plus, as Arup points out, it offers continuity with the Allium name (allium being the genus name for the garlic family).

The 68-seat restaurant has understated decor; it's the menu that really sets the atmosphere for Brassica. Arup has created a comprehensive bill of fare which acknowledges the current desire for foods that are lower in carbs and contain less gluten, along with dairy free options and an emphasis on vegetables and fish. It's a diverse, seasonal menu with reasonable-sized portions and pricing. All the food is made in-house, and reflects what Arup and Maggie themselves enjoy, along with a concise and interesting wine list.

"Brassica offers the kind of experience that I want when I go out to eat or when I am cooking at home. It's not just a protein, a side and a starch; we are encouraging sharing and trying as many things as possible. We believe we have the right formula to make people happy and feel like they got good value."

Brassica is open Tuesday through Saturday for dinner, with both lunch and casual day-long and drop-in menus also available on Fridays. In addition, there's an innovative, appealing brunch on offer both Saturdays and Sundays.



Paula Roy

Looking for more food articles?

[ARCHIVE](#)

Other News



[Custom Details](#)



[New and Notable](#)



[Hockey & Humility, Then](#)



[Seasoned with Personal](#)

Looking for more?

SEARCH ARCHIVE

Sign up for our
Newsletter



Name

Email

SIGN UP

1327

Homes

Food

Living

Editor's Note

Blog

Sponsored Content

Advertise With Us

Where to Find Ottawa At Home

Magazine

Ottawa At Home Contributors

Contact Us

E-Edition

READ IT TODAY



Ottawa At Home is published by Ottawa At Home Media Inc.

Copyright 2026 Ottawa At Home

Website Design by Lightswitch Creative

Challenge your brain with PUZZMO's daily puzzles. [Start playing >>](#)

Challenge your brain with PUZZMO's daily puzzles. [Start playing >>](#)

News Tariffs Opinion Public Service Fixing Byward Sports Life Newsletters Shopping Ottawa Citizen Store

Home / Food



Wellington Gastropub celebrates its second birthday

By **The Ottawa Citizen**

Published Sep 15, 20083 minute read

[Join the conversation](#)



This advertisement has not loaded yet.



SEP 15 – 8:10 AM — A who's-who list of well-wishers and gastronomes (in this case, one and the same) got a taste Sunday night of first-class food and drink as chef Christopher

Deraiche and his business partner, Shane

Waldron (*photo right*) celebrated two great

Despite having the city road ripped up in front of their business for what seems an eternity, the gastropub has continued to be a resounding success with locals and others who see it as a destination dining-out location that offers dependable quality in unpretentious yet still respectable surroundings. Small wonder the place is heralded by critics as one of the top tables in Ottawa.

STORY CONTINUES BELOW

“The time has gone fast,” says Rob Beardall, wine merchant and one of an estimated 100 to 125 guests who attended the celebration, beginning at 7 p.m.

It's been two years and they're still hot,
despite the road construction outside



Gastropub is a British term for a pub that specializes in high-quality food. It typically delivers a relaxed atmosphere and eclectic menu. The Wellington Gastropub opened on Sept. 6, 2006.

Among the regulars is Michael McCracken, chairman and c.e.o. of Informetrica, an economic forecasting firm, and discriminating foodie who estimates he visits “at least” once a month.

“This is one of my favourite places,” Michael says, as he sampled a succulent, fall-apart tender barbecued baby back rib, delivered by server Maggie von zur Muehlen (*photo, left*).

“It has consistently imaginative dishes, with a small menu that gives you enough choices without getting in the way of your eating time.”

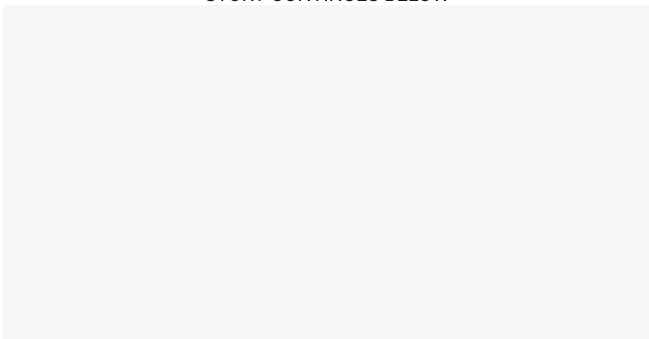


TRENDING 🔥



Also spotted last light were restaurateurs Stephen Beckta and his wife, Maureen Cunningham.

STORY CONTINUES BELOW



(Photo right, TV producer and food writer Chris Knight, restaurateur Joshua Bishop of The Whalesbone Oyster House)

My favourite nibbles — and there were so, so many superlative tastes — were Christopher's lightly breaded and quickly deep-fried morsels of halibut with homemade tartar sauce (*photo, below left*). The delicate coating

2  Ottawa
police Chief

We have a problem with cops running the plates of attractive women | Opinion

3  Canadian
Forces

Senior Canadian Forces officer in Ottawa charged with sexual assault

4  Global
Eye Saab

GlobalEye deal expected to cut procurement timetable for surveillance aircraft

Subscribe \$1 for 6 months

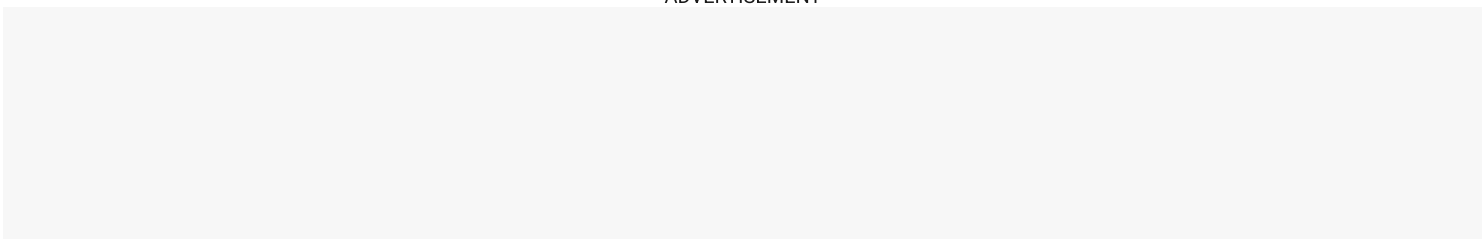
wonderful.



Melt-in-your mouth tender and satisfying were plates of panko and nori-encrusted albacore tuna sashimi, embellished with chili and soy aioli with pickled radish for zing. Scrumptious.

Of course, there was *foie gras* torchon with plum-raspberry coulis served on a rosemary-scented graham cracker. (Torchon describes a French method of cooking *foie gras* by wrapping it in a cylinder, usually in plastic food wrap, then gently poaching it to make the fat disarmingly more tender and utterly rich — if it's possible to make *foie gras* more rich than it already is.)

ADVERTISEMENT



My friend, Michael McCracken, recommended the venison tartare that was rich and refreshing at the same time. Seldom have I enjoyed such an uninterrupted cavalcade of superlative hors d'oeuvres with not a single ho-hum entry in the lot.

This advertisement has not loaded yet.



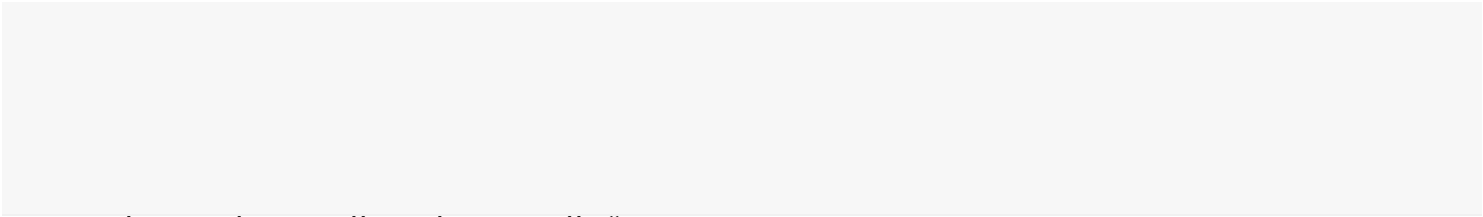
“Practically everyone here tonight is a regular customer,” Shane says of the party.

(Photo right, panko and nori-encrusted raw tuna with chili and soy aioli)

“We decided that every year we’re in business is a year worth celebrating, and we’ve got all these people to thank for that. A lot of them are local, and it’s an amazingly supportive community.”

His partner, Chris, had similar words of gratitude: “I’m over the moon how things

have happened since we opened,” Chris says.



rewarding professionally and personally.”

(Photos by Ron Eade)



Grand summer memories start here.

Grand pool. Grand sunsets. Grand memories. 10 restaurants, 17 bars, and pristine beaches. An all-...

Palladium Hotel Group | Sponsored

[Book Now](#)

'Good riddance': Senators set social media ablaze with Brady Tkachuk trade to Panthers

The best reactions on X from reporters and fans following the shocking deal that sent Ottawa's captain to Florida to play with his big bro.

Ottawa Citizen

The Surprising Kindle Hack 15 Million Readers Already Know

Every day, huge New York Times bestsellers are discounted to \$2 - and readers with the inside scoop are filling their libraries with these deals.

BookBub | Sponsored

[Learn More](#)

Gifts for the Foodie Dad

Spoil Dad with an Ooni pizza oven this Father's Day, and enjoy restaurant-quality pizza together all summer long.

Sign in

Create an Account



JOIN THE CONVERSATION



Postmedia is committed to maintaining a lively but civil forum for discussion. Please keep comments relevant and respectful. Comments may take up to an hour to appear on the site. You will receive an email if there is a reply to your comment, an update to a thread you follow or if a user you follow comments. Visit our [Community Guidelines](#) for more information.

If Your Aging Parent Still Uses a Towel Bar to Get Out of the Shower, Read This!

trendieproducts.com | Sponsored

How to dress yourself this summer with Simons

Build a compact, interchangeable wardrobe that carries you from day to night.

La Maison Simons | Sponsored

Learn More

Canada’s economy has been lagging behind U.S. for years. Here's why

Lutnick delayed Gordie Howe Bridge debut to seek bigger cut of toll revenue: sources

Ottawa Citizen

Understand your health insurance options

Public vs. individual health insurance: make an informed choice.

Blue Cross Health | Sponsored

Subscribe \$1 for 6 months

News Tariffs Opinion Public Service Fixing Byward Sports Life ePaper Subscribe

Follow Ottawa Citizen



[Advertise With Us](#) [Advertising Solutions](#) [Postmedia Ad Manager](#) [Savings](#) [Digital Ad Registry](#) [Site Map](#) [Contact](#)
[Privacy Policy](#) [Terms of Use](#) [FAQ](#) [Copyright & Licensing](#) [My Account](#) [Manage My Print Subscription](#)

© 2026 Ottawa Citizen, a division of Postmedia Network Inc. All rights reserved. Unauthorized distribution, transmission or republication strictly prohibited.

Mind and Money

f (<https://www.facebook.com/EcivdaFinancial>)

t (<http://twitter.com/EcivdaFinancial>)

✉ (<mailto:podcast@ecivda.com>)

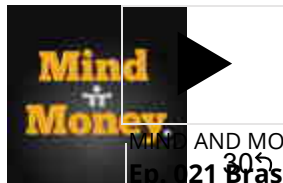
📡 (<http://feeds.libsyn.com/233075/rss>)

🎵 (<https://www.deezer.com/show/2444222>)

🎧 (<https://open.spotify.com/show/1JsOPBAZE1IFm5dCobcME9>)

All Episodes (/) / Ep. 021 Brassica, The Great Food Experience & Adventure in the Kitchen

Ep. 021 Brassica, The Great Food Experience & Adventure in the Kitchen (<https://mindandmoney.libsyn.com/ep-021>)



MIND AND MONEY

Ep. 021 Brassica. The Great Food Experience & Adventure in the Kitchen

00:00:00 / 01:03:23

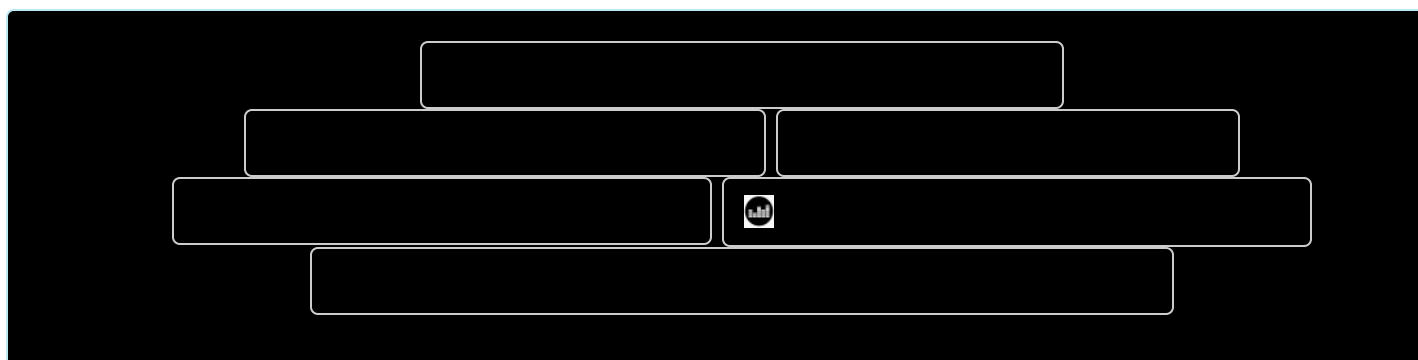
30



Feb 26, 2021

Corey Butler and Shawn Todd have an opportunity to speak with Arup Jana and Maggie Von Zur-Muehlen - owners of Brassica in Westboro. Arup and Maggie get into talking about what they learned from opening a restaurant in 5 days, what people stole after the Allium fire, how COVID has brought adventure into the kitchen, and where Brassica is heading. Connect with Corey, Shawn, and Ecivda Financial on Instagram, FB, LinkedIn, YouTube & Twitter.

Mind and Money



All Episodes (/) / 2021 (/2021) / 02

Ep. 022 Vodkow, Omid McDonald, Creativity & Innovation

(<https://mindandmoney.libsyn.com/ep-022-vodkow-omid-mcdonald-creativity-innovation>)



(<https://mindandmoney.libsyn.com/ep-022-vodkow-omid-mcdonald-creativity-innovation#comments>)

Feb 28, 2021

Corey Butler and Shawn Todd learn all about how Omid McDonald - and Diary Distillery in Almonte, Ontario - made an award winning vokda or vodkow from milk by product. It's an incredible conversation on innovation, change, and building a remarkable local brand. Omid talks about his business successes and failures,...

[Read More](https://mindandmoney.libsyn.com/ep-022-vodkow-omid-mcdonald-creativity-innovation) (<https://mindandmoney.libsyn.com/ep-022-vodkow-omid-mcdonald-creativity-innovation>)

1341 Ep. 021 Brassica, The Great Food Experience & Adventure in the Kitchen (<https://mindandmoney.libsyn.com/ep-021>)



(<https://mindandmoney.libsyn.com/ep-021#comments>)

Feb 26, 2021

Corey Butler and Shawn Todd have an opportunity to speak with Arup Jana and Maggie Von Zur-Muehlen - owners of Brassica in Westboro. Arup and Maggie get into talking about what they learned from opening a restaurant in 5 days, what people stole after the Allium fire, how COVID has brought adventure into the kitchen,...

[Read More \(https://mindandmoney.libsyn.com/ep-021\)](https://mindandmoney.libsyn.com/ep-021)

Ep. 20 Respect in Business, Ray Licari, Work Ethic & Legacy (<https://mindandmoney.libsyn.com/ep-20-respect-in-business-ray-licari-work-ethic-legacy>)



(<https://mindandmoney.libsyn.com/ep-20-respect-in-business-ray-licari-work-ethic-legacy#comments>)

Feb 22, 2021

Corey Butler and Shawn Todd get into business success and work ethic with well know Ray Licari - President of Bassi Construction. Ray opens up about self-discipline, work ethic, and what pivoting really is. Topics discussed - fostering a team culture, overcoming adversity, what he learned from SARS and H1N1, how to...

[Read More \(https://mindandmoney.libsyn.com/ep-20-respect-in-business-ray-licari-work-ethic-legacy\)](https://mindandmoney.libsyn.com/ep-20-respect-in-business-ray-licari-work-ethic-legacy)

Ep. 019 GameStop, Preet Banerjee, Willful, & Finances after COVID (<https://mindandmoney.libsyn.com/ep-019-gamestop-preet-banerjee->

1342 willful-finances-after-covid)



MIND AND MONEY

Ep 19

00:00:00 / 00:46:09

130

19 GameStop, Preet Banerjee, Willful & Finances after COVID



(<https://mindandmoney.libsyn.com/ep-019-gamestop-preet-banerjee-willful-finances-after-covid#comments>)

Feb 3, 2021

Corey Butler and Shawn Todd jump into the biggest news surrounding GameStop in the news, Preet breaks down what a squeeze looks like, the credit cycle, interest rates, Willful & why you really need to get your will done, and how how to bolster your finances post COVID-19. Preet always makes finance sound so easy - a...

[Read More](https://mindandmoney.libsyn.com/ep-019-gamestop-preet-banerjee-willful-finances-after-covid) (<https://mindandmoney.libsyn.com/ep-019-gamestop-preet-banerjee-willful-finances-after-covid>)

© Copyright - Ecivda

Tab B

www.linkedin.com/in/arup-jana-08ab192a0 (LinkedIn)

Top Skills

Staff Development

Project Management

Cross-functional Team Leadership

Arup Jana

Executive Chef and Restaurant Operations Consultant
Ottawa, Ontario, Canada

Experience

AJ Hospitality Consultant

Executive Chef and Restaurant Operations Consultant
May 2024 - Present (2 years 2 months)

Ottawa, ON

Personality based unique food and beverage development

Long term followup and quality standards

Training in problem solving and staff development

Creating high level standards and regulation

Menu development and pricing

Kitchen design and workflow

Cost control and profitability

Staff training and management systems

Restaurant openings and concept development

Marketing and customer experience

Operational efficiency

Brassica Food & Drink

Executive Chef

January 2020 - May 2025 (5 years 5 months)

Ottawa, Ontario, Canada

Chef/Managing Partner

Allium Restaurant

Executive Chef

August 2004 - March 2019 (14 years 8 months)

Ottawa, Ontario, Canada

Chef/Owner/Operator

1345

[Try Premium for CA\\$0](#)

Arup Jana

Executive Chef and Restaurant Operations Consultant

AJ Hospitali

Ottawa, Ont

56 connecti

+ Connect

Open to v

Ontario, C

Show deta

Activity

56 followers

Arup has

Recent post

Experien

Ex

AJ

Ma

Ot

Personality based unique food and beverage development

Long term followup and quality standards... more

Culinary Arts, Project Management and +5 skills



Executive Chef

Brassica Food & Drink · Self-employed

Jan 2020 - May 2025 · 5 yrs 5 mos

Ottawa, Ontario, Canada · On-site

Open to Work



Arup Jana

is Open to Work

Job titles

Chef

Location types

On-site · Hybrid

Locations

Ontario, Canada · Ottawa, ON · Berlin, Germany · Kelowna, BC

Start date

Immediately, I am actively applying



Looking for a new job too?

Get support from the community by joining millions of members who are sharing they're open. [Get started](#)

Share profile

Message



Arup Jana

✓

Executive Chef and Restaurant Operations Consultant

AJ Hospitality Consultant

Ottawa, Ontario, Canada · [Contact info](#)

56 connections

Connect

Message Arup

More

Open to work

Ontario, Canada +3 more | On-site · Hybrid

[Show details](#)

Activity

56 followers

Arup has no recent posts

Recent posts Arup shares will be displayed here.

+ Follow

Show all posts →

Experience

Executive Chef and Restaurant Operations Consultant

AJ Hospitality Consultant · Freelance

Mar 2024 - Present · 2 yrs 2 mos

Tab C

Files

Tools



File List



Give us your feedback

Metadata Details Of Your File

The following table shows all EXIF data and metadata we could extract from your file using our free online metadata and EXIF viewer.

The data shown is all the metadata we could automatically extract from your file.

It may be incomplete or inaccurate.

Metadata may have been changed or deleted in the past. Please note that the metadata is provided without liability.

- DF
- CSV
- TXT
- JSON
- HTML

checksum
ba452569353d970bcd40948d480818fc

file_name



Download



Export As

Share



Delete

Done

Get a subscription to skip the queue, use PRO features, and process your files faster.

Get Premium

Current Task



View Metadata



Start over



Change options

Notification

Get notified when the task is done



Email



Push notification

Continue with

Clarification requested June 25...



Metadata Remover



Clarification
requested June
25, 2026 A-
2026-
00761.docx

file_size
31 kB

file_type
DOCX

file_type_extension
docx

mime_type
application/vnd.openxmlformats-
officedocument.wordprocessingml.do

zip_required_version
20

zip_bit_flag
0x0006

zip_compression
Deflated

zip_modify_date
1980:01:01
00:00:00

zip_crc
0x62b8538b

zip_compressed_size
411

zip_uncompressed_size
2230

zip_file_name
[Content_Types].xml

title

subject

creator
Von Zur-
Muehlen,
Margarethe
(Maggie)
(RCMP/GRC)

keywords

description

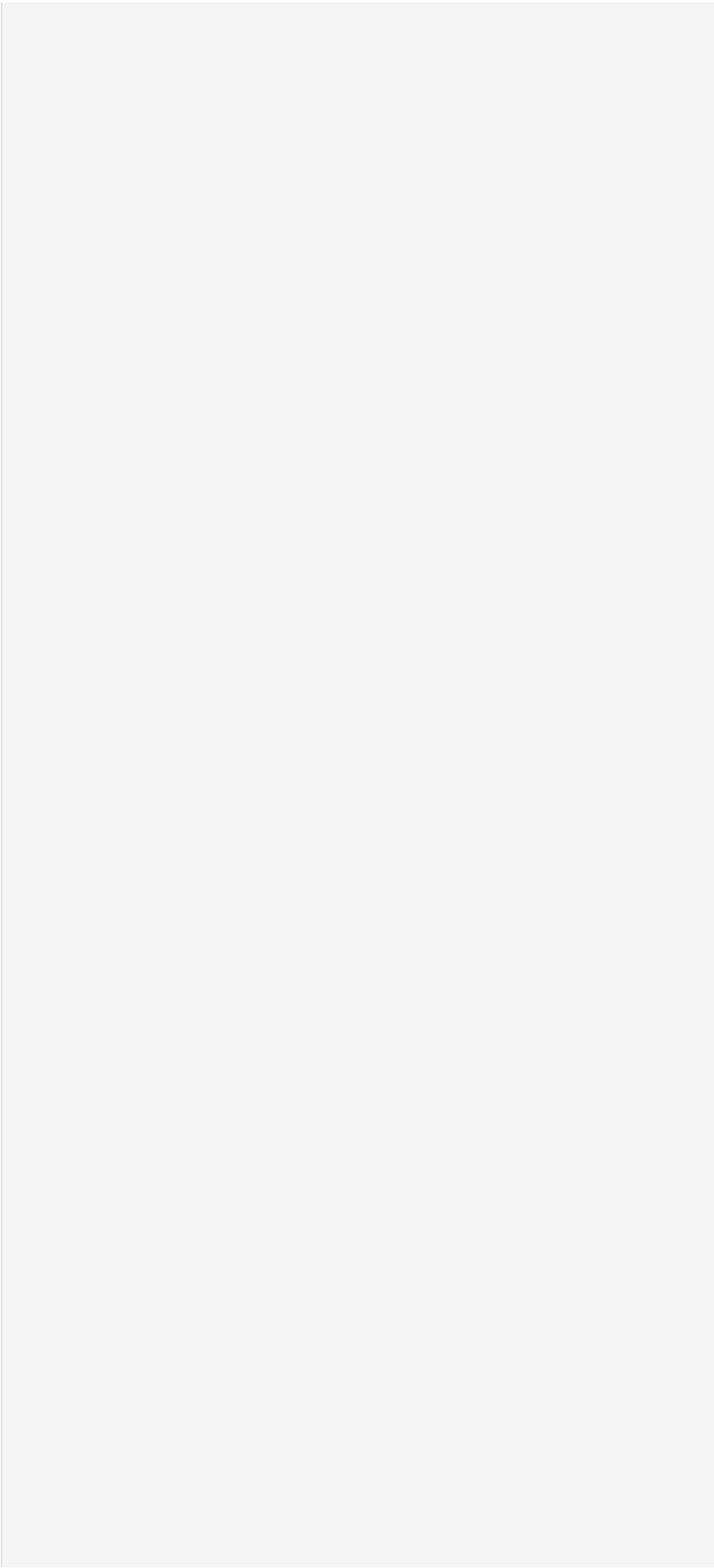
last_modified_by
Beaudoin, Tina
(RCMP/GRC)

revision_number
3

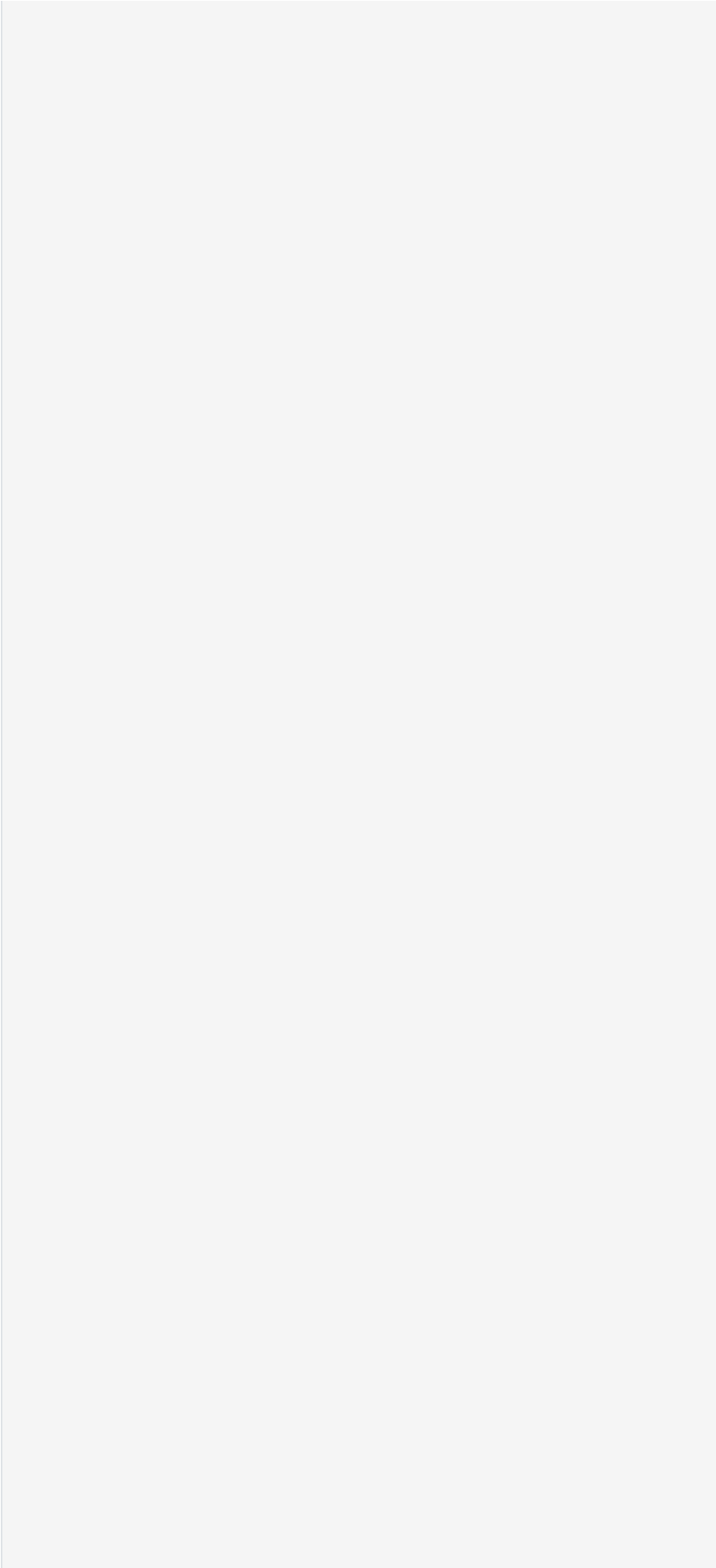
create_date
2026:06:25
18:01:00Z

modify_date
2026:06:25
18:24:00Z

template



Normal.dotm	
total_edit_time	45 minutes
pages	2
words	487
characters	2778
application	Microsoft Office Word
doc_security	None
lines	23
paragraphs	6
scale_crop	No
company	RCMP-GRC
links_up_to_date	No
characters_with_spaces	



3259

shared_doc

No

hyperlinks_changed

No

app_version

16

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36__enabled
true

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36__set_date
2026-06-
16T19:11:39Z

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36__method
Standard

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36__name
PROTECTED A -
Protégé A

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36__site_id
2ebaed2f-af63-
45af-a67b-
ec24f2eeb7ef

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36_action_id
69d42943-85b0-
4f3e-b741-
1d43601fca82

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36_content_bits
0

msip_label_17a7f32d-
f4c1-4d09-9e83-
eb989c840e36_tag
10, 3, 0, 1

content_type_id
0x010100B403DADD6B0D90458B59A4

eda9d87a301242459f38eefd06719ac5
Active|0b3dfebb-
5ec2-4343-96ff-
408e79fa6281

rcmp_sensitivity
2;#Protégé
A|67e4ddaf-
c1d9-44bc-
97d8-
c9760332edb8

media_service_image_tags

rcmp_fiscal_period
3

rcmp_record_status
19

rcmp_language

1;#Anglais|49431515-
c2d7-4fd7-9af8-
2c97aaf3b244

rcmp_document_type

lcf76f155ced4ddcb4097134ff3c332f

business_process

16

tag_dlc_doc_id_item_guid

5a17e05b-bab3-
4d4f-ae09-
a66f7db7bed5

category

application

raw_header

50 4B 03 04 14
00 06 00 08 00
00 00 21 00 8B
53 B8 62 9B 01
00 00 B6 08 00
00 13 00 08 02
5B 43 6F 6E 74
65 6E 74 5F 54
79 70 65 73 5D
2E 78 6D 6C 20
A2 04 02 28 A0
00 02 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00

00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00 00 00
00 00 00

title
f39e107c9db8740f6063cc7a9557ae73

author(s)
Von Zur-
Muehlen,
Margarethe
(Maggie)
(RCMP/GRC)
[Von Zur-
Muehlen,
Margarethe
(Maggie)
(RCMP/GRC)]

publisher
RCMP-GRC

languages
eng

Save this data as

PDF

CSV

Advertisement

1349

TAB 40

1350

Tab A

www.linkedin.com/in/derek-santosuosso-15a826289 (LinkedIn)

Top Skills

Law Enforcement Technology
Security Operations
Law Enforcement Operations

Derek Santosuosso

RCMP Assistant Commissioner (Ret'd) | 32+ Years in Policing
Leadership | Technical Operations | National Recruiting |
Commanding Officer | Major Crime & Organized Crime
Ottawa, Ontario, Canada

Summary

32 years of policing leadership — from homicide investigations in BC to commanding national technical programs from Ottawa. I retired in May 2026 as Assistant Commissioner, Technical Operations (RCMP National HQ), where I oversaw seven national program branches delivering advanced investigative and operational capabilities to law enforcement across Canada: covert electronic surveillance, digital forensics, lawful access, protective security, counter-drone operations, airborne law enforcement, missing persons, and the responsible onboarding of emerging technologies. Prior to that I served as Chief National Recruiting Officer, leading the transformation of the RCMP's national recruitment program — modernizing the process, improving diversity and representation, and steering the 2026–2029 National Recruitment Strategy. Earlier career highlights:• Commanding Officer, PEI RCMP (L Division) — led 200+ personnel delivering province-wide policing• Superintendent, B Division NL — commanded 600 people across Support Services and Criminal Operations; Silver Commander, 2021 Nova Scotia Fishery Dispute• Inspector, NL — led serious and organized crime and the integrated CFSEU• Sergeant/Corporal, BC — Major Crime Special Projects, IHIT, North District Major Crime• MCM Team Commander (Accredited) | Canadian Police College Instructor• Captain, Canadian Armed Forces — Military PoliceOpen to consulting, board, advisory, and volunteer roles in public safety, law enforcement governance, technology oversight, or organizational leadership.

Experience

none
Retired
May 2026 - Present (2 months)

Royal Canadian Mounted Police | Gendarmerie royale du Canada

28 years 2 months

Assistant Commissioner of Technical Operations, Specialized Policing Services

January 2025 - May 2026 (1 year 5 months)

Ottawa, ON

As Assistant Commissioner of Technical Operations, I led seven national program branches delivering advanced investigative and operational capabilities to law enforcement across Canada and select international partners.

Programs under my command:

Sensitive & Specialized Investigative Services (SSIS) — behavioural sciences, missing persons, polygraph, and high-risk offender support

Technical Investigative Services (TIS) — lawful access, covert entry, electronic surveillance, digital forensics, and counter-explosives

Protective Technical Services (PTSB) — physical and electronic security systems, counter-drone capabilities, and VIP/asset protection

Air Services Branch (ASB) — fixed-wing, rotary-wing, and drone law enforcement support for surveillance, transport, and critical incident response

National Lawful Access Centre (NLAC) — national coordination of lawful access processes, standards, and infrastructure

Strategic Services Branch (SSB) — governance, policy, HR, and operational support

National Technology Onboarding Program (NTOP) — rigorous assessment and compliance oversight for emerging operational technologies

Drove modernization, fostered interagency collaboration, and advanced public trust through transparent and responsible technology adoption.

Chief National Recruiting Officer, Assistant Commissioner

October 2023 - January 2025 (1 year 4 months)

Ottawa, ON

As Chief National Recruiting Officer, I held national executive responsibility for attracting, selecting, and onboarding Regular Members to meet the RCMP's current and future workforce needs.

Key responsibilities and achievements:

Chaired Executive-level steering committee on recruitment, established by the Senior Executive Committee to sustain organizational focus on this strategic priority

Directed the development of the RCMP National Recruitment Strategy.

Led efforts to increase representation of Indigenous peoples, Black Canadians, and other under-represented groups in the Regular Member complement

Collaborated with Human Resources, divisional leadership, and business lines to align recruitment with long-term workforce planning needs

Established performance measures and accountability frameworks to track progress against recruitment targets

Worked with the Canadian Police College and divisional training programs to strengthen onboarding and retention for new Regular Members

Advanced bilingual recruitment and the attraction of candidates with specialized skill sets to support federal policing priorities

Commanding Officer “L” Division, Chief Superintendent

June 2022 - October 2023 (1 year 5 months)

Charlottetown, PE

As Commanding Officer of L Division, I was the senior RCMP officer responsible for all RCMP operations in Prince Edward Island, leading more than 200 regular members, civilian members, and public service employees across Headquarters in Charlottetown and three operational districts through six service centres.

Key responsibilities and achievements:

Held full executive accountability for provincial policing: general duty, criminal operations, federal policing, traffic services, and Indigenous policing
PEI RCMP consistently achieved among the highest citizen satisfaction ratings with police services in Canada

Advanced L Division's Reconciliation Strategy through sustained engagement with Mi'kmaq First Nations communities — Lennox Island and Abegweit First Nations — promoting culturally sensitive service delivery

Partnered with the Government of PEI, provincial justice stakeholders, and the PEI Association of Chiefs of Police to advance public safety priorities

Managed divisional HR, budget, and strategic planning in alignment with national RCMP priorities

Served as the RCMP's senior provincial representative in interagency and government forums

Support Services Officer, Superintendent

April 2019 - June 2022 (3 years 3 months)

St John's, NL

Led, managed, supervised, motivated, coached, and directed approximately 100 personnel in 27 individual programs within the Support Services portfolio including: major crimes, traffic services, critical and emergency response, high risk investigation oversight and community and Indigenous engagement.

Administered and managed a \$12.5M policing budget.

Established, served on and chaired internal and external committees with RCMP members and provincial ministerial officials including police partnership, provincial prisoners and major case management.

Partnered with the Royal Newfoundland Constabulary, Provincial Corrections and Sheriffs on improving Provincial service delivery in law enforcement.

Collaborated with the Government of Newfoundland and Labrador Provincial Justice and Public Safety to modernize service delivery and legislation.

Acting as the Officer in Charge of Criminal Operations in NL, including the Support Services portfolio and uniform policing for the Province. Led and managed 600 employees and provided oversight and approval to all provincial and municipal policing activities in RCMP, NL jurisdictions.

Issues Management Team, H Division, Nova Scotia, April to July 2020.

Ensured the appropriate collection and disclosure of material for the various inquiries and investigations and provided support to the Province, the Division and National HQ in relation to the various issues which arose as a result of the mass murders.

Silver Commander, Fishery Dispute, H Division, Nova Scotia, May to August and October 2021. Led the operational RCMP Unified Command contingent in collaboration with Provincial Justice and Public Safety, Department of Fisheries and Oceans, Canadian Coast Guard and First Nations groups to establish treaty right fishing while maintaining order and keeping the peace.

Officer in Charge of Federal and Serious Organized Crime, Inspector
November 2018 - April 2019 (6 months)

St John's, NL

Led, managed, supervised the serious and organized crime teams in investigations into drugs, organized crime, economic crime with a focus on inter-jurisdictional links often reaching beyond Provincial borders.

Administered and managed a \$12M policing budget.

Acted in the role of the Federal Officer in Charge of Criminal Operations.

Led, managed and supervised 80 personnel in specialized areas such as intelligence, covert electronic surveillance, covert operations and cultivation of confidential informants to the RCMP and our partners in law enforcement.

Officer in Charge Combined Forces Special Enforcement Unit of
Newfoundland and Labrador, Inspector
July 2017 - November 2018 (1 year 5 months)

St John's, NL

Led, managed, supervised an integrated team of 50 persons with half from the Royal Newfoundland Constabulary in the investigation, detection and disruption of serious and organized crime and internet child exploitation. Provincial investigations led to operations spanning Atlantic region, Canada and internationally.

Administered and managed a \$3.5M policing budget.

The Atlantic representative to Canadian Association of Chiefs of Police Drug Advisory Committee. Advancing the Atlantic Region's issues and needs and providing advice, through the Chair, to the Government of Canada in relation to the legalization of cannabis, the opioid crisis, decriminalization and legalization of other drugs and substances among other issues.

Established the Accredited Team Commander program in NL establishing policing standards for complex, high risk investigations.

Team Leader "E" Division Major Crime Special Projects Unit, Sergeant
June 2014 - July 2017 (3 years 2 months)

Surrey, BC

Led, managed, supervised investigative team which supported and/or had conduct of homicide and other major crimes within BC. The investigations were project based, often involved vulnerable victims and required complex investigative skills and strategies, specialized expertise, or dealt with extraordinary circumstances.

Established relationships with special interest groups and the leadership of Indigenous and/or marginalized communities associated to the victims.

Worked with members of various BC municipal police departments/services.

Obtained Accreditation as a Major Case Management Team Commander.

Taught leadership and Major Case Management Team Commanding at the Canadian Police College to members of the RCMP, Canadian and American municipal and Military Police departments/services beginning in 2015 to the present.

Senior Investigator Chilliwack Serious Crimes
January 2011 - June 2014 (3 years 6 months)

Chilliwack, British Columbia, Canada

Senior Investigator Integrated Homicide Investigation Team
March 2008 - January 2011 (2 years 11 months)

Surrey, British Columbia, Canada

Investigator "E" Division Major Crime North District
July 2005 - March 2008 (2 years 9 months)
Prince George, British Columbia, Canada

General Duty Policing
July 2000 - July 2005 (5 years 1 month)
British Columbia, Canada

Surrey Detachment from 2000 to 2003
Bella Coola Detachment from 2003 to 2005

General Duty Policing
April 1998 - July 2000 (2 years 4 months)
Lloydminster, Saskatchewan, Canada

Canadian Armed Forces | Forces armées canadiennes
Captain, Military Police
May 1993 - October 1997 (4 years 6 months)
Canada

Education

Royal Military College of Canada/Collège militaire royal du Canada
Bachelor of Arts - BA, History · (May 1993)



Unlock exclusive tools and conversations with industry leaders

[Try Premium for CA\\$0](#)

Connection

Grow your network

1



Derek Santosuosso ✓ • 3rd+

RCMP Assistant Commissioner (Ret'd) | 32+ Years in Policing Leadership | Technical Operations | ...

1yr • 🌐

[+ Follow](#)



As the new year has come so has change for me to take on a new role. I'm happy to share that I'm starting a new position as Assistant Commissioner of Technical Operations, Specialized Policing Services at [Royal Canadian Mounted Police | Gendarmerie royale du Canada](#).

<https://lnkd.in/ecRcW9ts>



Tab B



Royal Canadian Mounted Police Gendarmerie royale du Canada

Royal Canadian Mounted Police

[RCMP.ca](https://rcmp.ca) > [News](#)

News release

RCMP formally reaffirms its partnership with Missing Children Society of Canada

May 22, 2026 - Ottawa, Ontario

From: RCMP National Headquarters

On this page

- [Content](#)
- [Quotes](#)
- [Quick facts](#)
- [Associated links](#)
- [Contacts](#)

Today, the RCMP's National Centre for Missing Persons and Unidentified Remains (NCMPUR) renewed their Memorandum of Understanding (MOU) with the Missing Children Society of Canada (MCSC), reaffirming a long-standing partnership dedicated to supporting missing persons investigations across Canada. The renewal comes ahead of National Missing Children's Day on May 25, highlighting a shared commitment to collaboration, prevention and public awareness.

1360

renewed MOU reflects the strength of a long-standing partnership built on trust, shared expertise and a common goal to assist investigators, provide meaningful support to families, and work together to help bring missing persons home. This agreement ensures that families of missing persons receive coordinated, compassionate, and consistent support, combining investigative expertise with dedicated family services so no family has to navigate the search for a loved one alone.

Neither organization alone can fully meet the needs of families. NCMPUR brings national coordination and investigative expertise to law enforcement, while MCSC provides dedicated family support and advocacy; together, they deliver a more humane, effective response. This renewed MOU underscores the importance of the RCMP and MCSC working together to improve outcomes for families of missing persons.

NCMPUR plays a vital role in coordinating and supporting missing persons and unidentified remains investigations in Canada as well as internationally. The NCMPUR assists law enforcement agencies, medical examiners and chief coroners by providing access to national databases, analytical support and expertise that strengthen investigative efforts and help advance complex cases.

MCSC focuses on supporting police services and families affected by missing children cases by providing investigative assistance, family support services and public awareness initiatives. As part of its continued evolution, MCSC will transition from its current child-focused model toward a broader program by 2027 that supports missing children, youth and adults, further strengthening its ability to respond to the evolving needs of communities.

1361

Together, NCMPUR and MCSC will continue to serve as Canada's representatives to the Global Missing Children's Network, linking Canadian investigators and organizations with international partners who work collaboratively to locate missing children around the world and share best practices, tools and intelligence.

Quotes

Our partnership with MCSC is rooted in a shared commitment to collaboration, compassion and results. This agreement reflects our shared dedication to ensuring investigators have the support they need and that families facing the unimaginable know they are not alone. Together we are working towards our common goal of bringing missing persons home.

Chief Superintendent Richard Burchill, Acting Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police

Renewing this MOU reinforces the strength and importance of our partnership with MCSC. By working together and sharing expertise, we are better positioned to support investigators, assist families during incredibly difficult times. Together we strengthen Canada's response to missing persons cases.

Sergeant Lana Firth, Officer in Charge, National Centre for Missing Persons and Unidentified Remains, Royal Canadian Mounted Police

1362

If you are not in a safe place, life changes, and that truth has guided MCSC's work for 40 years. We are grateful for the opportunity to partner with and support NCMPUR because we believe that hope is present in every single case, and this partnership is what that shared hope looks like in action: united by purpose, bringing the best of our combined resources and expertise to every investigation and family. As MCSC evolves to serve missing children, youth and adults across Canada, this is how we honour 40 years and build toward a future of safety and protection for all who need us.

Amanda Pick, Chief Executive Officer, Missing Children's Society of Canada

Quick facts

- In 2025, 34,189 children were reported missing in Canada
- [Canadasmissing.ca](https://canadasmissing.ca) is Canada's first national public website designed to solicit tips and information from the public for missing children, missing persons, and unidentified remains cases
- Visit canadasmissing.ca to review the cases and learn how to submit a tip
- Investigators review every tip that comes in, and even a small detail could be the key to bringing another child home.

Associated links

- [Canada's Missing](#)
- [Missing Children Society of Canada - Family Support](#)

1363 About the National Centre for Missing Persons and Unidentified remains (YouTube).

Contacts

RCMP Media Relations

rcmp.hqmediarelations-dgrelationsmedias.grc@rcmp-grc.gc.ca

613-843-5999

Date modified:

2026-05-13

Tab C



← **Post**



The Guy

@ProGamerGov



RCMP Witness Richard Burchill just tried to claim that mandatory metadata retention isn't mass surveillance, at today's [#SECU](#) Committee.

[#encryption](#) [#encryptedmessaging](#) [#privacy](#) [#backdoors](#) [#c22](#) [#lawfulaccess](#)
[#cdnpoli](#) [#canpoli](#) [#canadianpolitics](#)

9:16 PM · Jun 16, 2026 · **11** Views



Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Tab D

1365

LIGHT

Global NEWS

**Register now**

alteryx.com

IT maintains security, visibility,
& cost control on Google Cloud.

Open

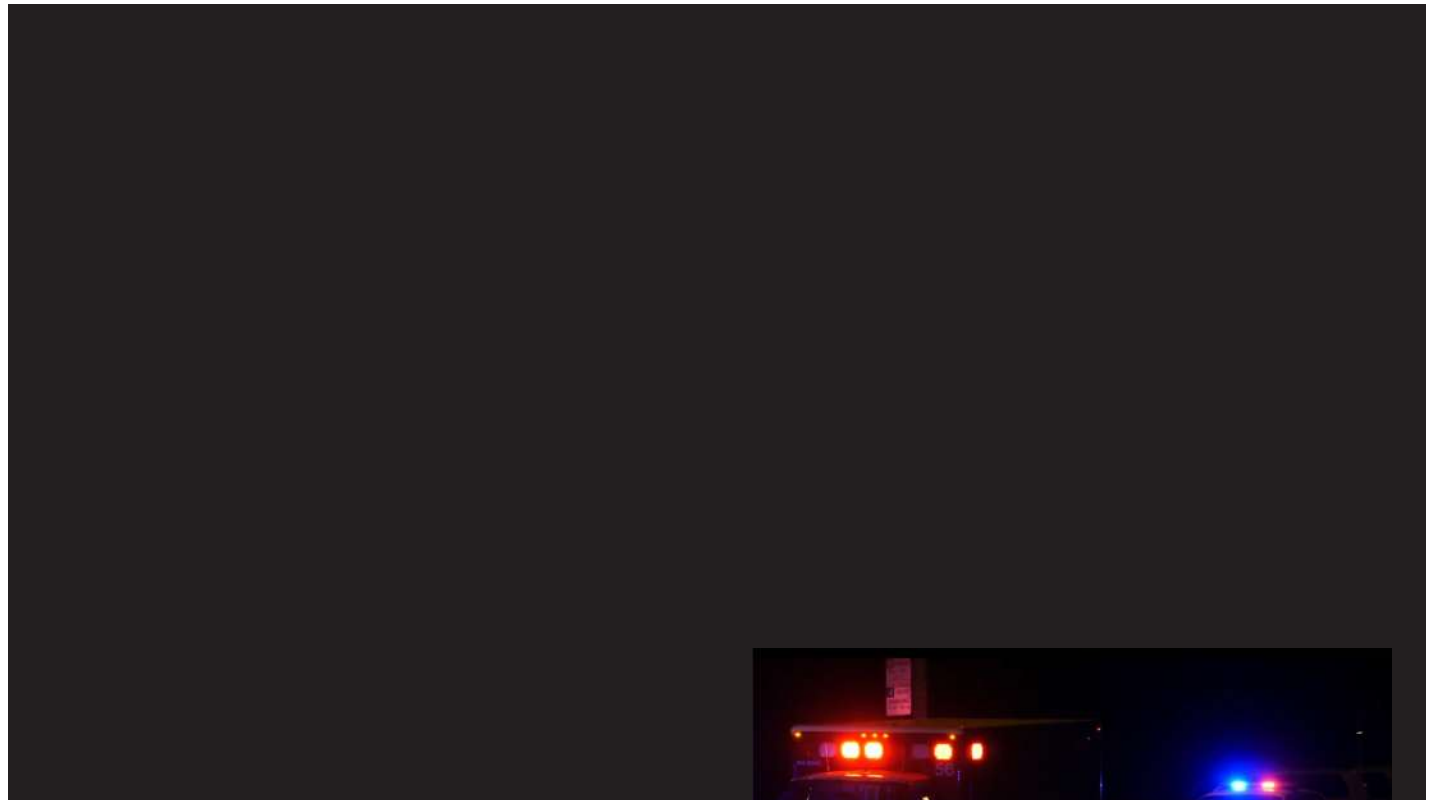
TECH

Your metadata may be kept for a year under lawful access bill. What to know

By **Sean Boynton** • Global News

Posted May 21, 2026 6:00 am

7 min read



RELATED: Liberals table tweaked 'lawful access' bill after



AdChoices

1366

The federal government's proposed **lawful access** bill is raising concerns about the potential lengthy retention of Canadians' **metadata** that could then be accessed by law enforcement, which **privacy** experts warn is risky and "unprecedented."

Concerns about the legislation have already spurred multiple service providers, including VPN operators, **to say they would pull out of Canada rather than comply** with the controversial proposals that seek to give investigators access to company-held data.

Bill C-22 includes a new provision that would allow the government to make regulations for "core" telecommunications providers to retain certain types of metadata — including transmission and location data — "for reasonable periods of time not exceeding one year."

The bill would then allow the minister of public safety to order other electronic service providers to comply with that regulation, subject to approval of the federal intelligence commissioner, for the purposes of a criminal or national security investigation.

STORY CONTINUES BELOW ADVERTISEMENT

Printable PDF (Free)



Open



While government officials insist the data that would be collected does not include actual online content like search histories or emails, and that the metadata itself can only be collected by investigators through a judicial warrant, experts warn the retention policy alone is concerning.

AdChoices

1367

The government's building this massive haystack of data with the thought that they might need to find the needle every once in a while," said Michael Geist, a professor at the University of Ottawa and the Canada research chair in internet and e-commerce law.

"But in doing so, they're creating huge privacy risks for Canadians."



Stick to the Facts

Add Global News as a Preferred Source on Google to see more of our stories in your search results.



Add as a preferred
source on Google

What is metadata?

Metadata is broadly defined as "data about data," or what Geist calls "the information around" something like an online communication rather than the content itself.

1368



This includes dates, times and locations those messages were sent, the IP addresses used to send them, and broad identifiers like the names of senders and receivers and what type of file or message it was.

It also involves tracking data and transmission data that is collected every time a cellphone connects to a cell tower, Geist explained, “which is all the time” because most people’s phones remain turned on even when not in use.

“Anytime you communicate with someone, what device did you use? Where were you located? When did you communicate? All of those things about your activities. That’s what metadata is,” he said.

Robert Diab, a law professor at Thompson Rivers University in Kamloops, B.C., who focuses on online privacy, said courts have recognized for decades that “the mosaic of information that you can assemble through metadata can really reveal quite a lot about a person’s life.”

“What it is they’re doing, their movements, their communications — it connects you with people and places in time, and from that you can draw a number of inferences about a person.”

Both experts noted the metadata provision was “quietly” added to **Bill C-22, which stripped out and updated the lawful access section** of the more broad Bill C-2, after **that earlier legislation raised widespread privacy concerns.**

1369

STORY CONTINUES BELOW ADVERTISEMENT



What does the bill seek to do?

Police and intelligence officials have said while speaking about Bill C-22 that metadata can be useful to investigators when trying to, for instance, link a kidnapping suspect to multiple locations where they may have taken a victim.

1370

Get breaking and local news on Bluesky

Stay up to date with news from across Canada, sign up to follow Global News on Bluesky.

[CLICK TO SIGN UP](#)

Richard Burchill, director-general of technical investigative services for the RCMP, told the House of Commons public safety committee this month that internet transmission data and cell tower signalling data would be of particular interest.

STORY CONTINUES BELOW ADVERTISEMENT

He said the reason for the one-year time limit was to create a “consistent” data retention standard for major telecommunications providers that investigators could rely upon.

“If they keep it for three days, but you’re one week into a kidnapping investigation, that data is gone whether you are judicially authorized or not, whereas some companies have it readily available,” he said.

Liberal MP Sima Acan noted during the same hearing that historical metadata could be “essential for establishing timelines and connections that are not

AdChoices

1371 immediately obvious,” particularly when offences are reported long after they occur.

Government officials told the committee that regulations on what specific metadata must be retained and for how long — as well as what a “core” provider is — will be developed after the legislation becomes law, through consultations with law enforcement and security agencies as well as the telecommunications sector.

Those regulations could then be redrafted as needed in the future without having to introduce new legislation.

“This is heavily based in technology, and using terms (that) could be obsolete within a number of years ... would render the whole bill actually useless,” said Shannon Hiegel, the national security policy director general at Public Safety Canada.

Simon Lafortune, a spokesperson for Public Safety Minister Gary Anandasangaree’s office, told Global News the bill “only allows for limited retention requirements strictly for metadata” and “does not permit the retention of content, web browsing history, or social media activity.”

STORY CONTINUES BELOW ADVERTISEMENT

Some police chiefs, however, have called for even broader and lengthier data retention, though government officials insisted they are not currently looking

AdChoices

1372 to further expand lawful access authorities beyond Bill C-22.

Thunder Bay Police Chief Darcy Fleury told the committee at a separate hearing this month that the one-year limit for metadata retention was “a good start” but that two or even three years “would be ideal.”

[MORE ON TECH](#)[MORE VIDEOS](#)

- [Apple is hiking prices and blaming AI. How much will it cost Canadians?](#)
- [Sinking AI stocks leading Wall Street towards a losing week](#)
- [Is BlackBerry 'back'? Former smartphone maker hits key earnings milestone](#)

Why are experts concerned?

Diab noted that **under existing Canadian law**, police must seek a warrant asking a telecommunications provider to retain a specific person’s metadata for only a limited amount of time, such as a month or 90 days, for an investigative purpose.

AdChoices

“The reason Parliament has done that ... is that it recognizes that the creation of a record is itself an interference” of privacy, he said.

“In this case, the minister tells Telus, ‘go and save it for a year.’ ... The idea is the same: if you create a record, if you order a third party to preserve a citizen’s records of their communications, you are interfering with their privacy because you’re conducting a form of surveillance. You are creating a situation in which their movements, their communications are being watched or are being made watchable in a sense. And that’s what matters.”

He said the law, if passed as currently written, could be challenged in court for running afoul of Section 8 of the Charter of Rights and Freedoms, which protects Canadians against “unreasonable search or seizure.”

The metadata retention provision is not mentioned in the government’s Charter statement on the bill, which outlines how it is consistent with Charter rights and freedoms.

A Department of Justice spokesperson told Global News this is because the provision “does not itself require metadata retention” and only creates a regulation-making authority.

“Any future regulation made under that authority would have to comply with the Charter, including Section 8 protections,” and be subject to a separate

AdChoices

1374

Charter statement and other safeguards, Ian McLeod said.

STORY CONTINUES BELOW ADVERTISEMENT

“It would also need to be assessed based on what data is covered, who must retain it, for how long, for what purpose, and what safeguards apply.”

Hiegel told the House of Commons committee that the government does not equate a company’s retention of data with a “seizure” as defined by the Charter because there is no production order involved until a judicial warrant is approved.

Experts noted the broad retention of data also poses cybersecurity risks, particularly if hackers exploit regulations created under Bill C-22 for providers to give law enforcement access to information — a provision critics have called a “backdoor” into online platforms, which the government has denied.

1375



How do other countries compare?

The government and police chiefs have repeatedly said Canada is lagging behind its Five Eyes and G7 allies that already have lawful access powers in place.

STORY CONTINUES BELOW ADVERTISEMENT

Those countries differ in their metadata retention policies, however.

While Australia mandates companies retain metadata for up to two years, the United States has no broad retention timeline in law and has sought to limit_{AdChoices}

1376 the scope of such abilities in recent years.

The European Union also doesn't have a standard data retention timeline for member nations, and some that have their own lawful access regimes, like Germany, have seen their metadata provisions struck down by the courts as unconstitutional.

"We have choices, and we don't really face any particular requirements to make these changes," Geist said.

Diab said the disparity points to the trouble governments face when trying to justify broad data retention to the public.

"If you were told that the government is going to tell Telus and Freedom and Fido and whoever to keep a record of when and where you made calls, and where you used your cellphone for a year, for a potentially prosecutorial purpose — how would you feel?" he asked. "Would you feel you were being surveilled? Would you feel that your privacy is interfered with?"

"I think most reasonable Canadians would say, yeah, that would feel kind of creepy. I don't want to know that that's happening."

 JOURNALISTIC STANDARDS

 REPORT AN ERROR

 COMMENT

© 2026 Global News, a division of Corus Entertainment Inc.

More to Explore



AdChoices

TAB 41

Tab A

1378



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

45th PARLIAMENT, 1st SESSION

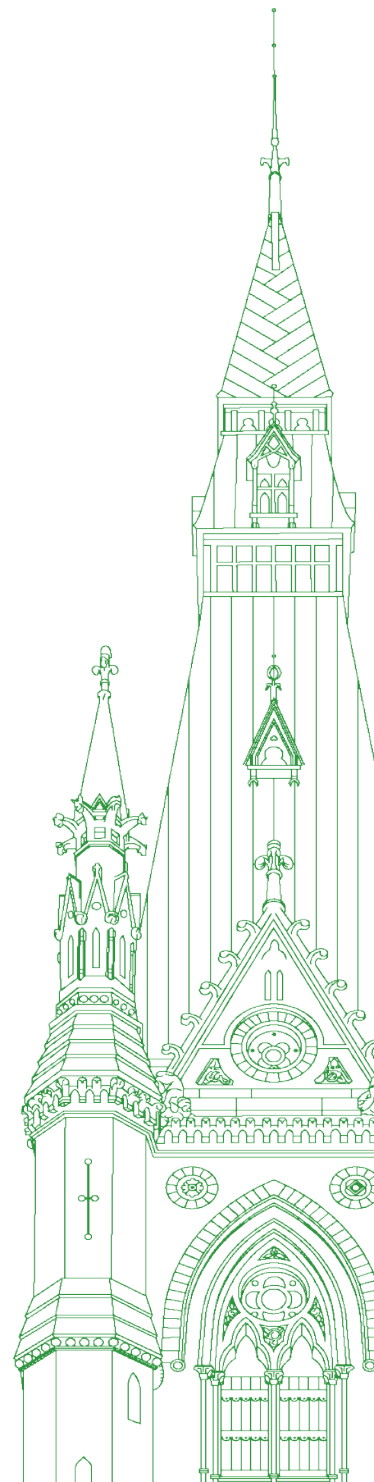
Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 036

Tuesday, May 5, 2026

Chair: Jean-Yves Duclos



Standing Committee on Public Safety and National Security

Tuesday, May 5, 2026

• (1555)

[Translation]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): I call this meeting to order.

I want to thank everyone for joining us.

First of all, I apologize for all the emotions you may have gone through over the past few hours. I'm thinking in particular of the clerk. There were changes in schedules, votes, assigned seats, unassigned seats, reassigned seats and so on. I thank you all for your kindness and indulgence.

Welcome to meeting number 36 of the Standing Committee on Public Safety and National Security.

We're meeting today as part of our study on Bill C-22, an act respecting lawful access.

First, I'd like to welcome the witnesses, who are all senior officials. The ministers will be joining us in about an hour.

We have with us, from the Canadian Security Intelligence Service, Ramzi Nashef, director general; from the Department of Justice, Kimberley Gibner, Normand Wong and Anne-Marie LeBel; from the Department of Public Safety and Emergency Preparedness, Shannon Hiegel, Mike McGuire and Fenton Ho; and from the Royal Canadian Mounted Police, Richard Burchill.

Mr. McGuire, we'll start with you, please. You have the floor for five minutes.

[English]

Mike McGuire (Director General, International and Border Policy, Department of Public Safety and Emergency Preparedness): Thank you, Mr. Chair and honourable members of the committee, for having us here today.

My name is Mike McGuire. I'm the director general of international and border policy at Public Safety Canada. I'm pleased to be here with colleagues, as was just mentioned, from the Department of Justice, the Department of Public Safety, the RCMP and CSIS to answer technical questions on Bill C-22, an act respecting lawful access.

Lawful access is a familiar issue that has been studied by Parliament in the past, most recently by the National Security and Intelligence Committee of Parliamentarians, which issued a special report last year calling for lawful access legislative reform.

[Translation]

Bill C-22 seeks to address fundamental and well-documented gaps in Canada's lawful access framework. The online environment has facilitated, if not fostered, the communication, coordination and concealment of criminal activities and those of threat actors. The widespread use of mobile devices, Internet-based communications, messaging platforms and other emerging technologies has fundamentally transformed how crimes and threats to national security are planned, executed and investigated.

At the same time, Canadian police services and CSIS face increasing challenges in obtaining information critical to investigations in a timely manner. Bill C-22 seeks to address these challenges while maintaining strong safeguards, including respect for the Canadian Charter of Rights and Freedoms and the protection of Canadians' privacy.

[English]

The provisions in Bill C-22 are grouped under two key themes. First, part 1 of the bill modernizes Canada's legal authorities to support police and CSIS in obtaining timely and lawful access to digital information needed for investigations, with each tool carefully designed to take into account the type of information that will be collected and the privacy interest it engages.

This includes the creation of a new confirmation of service demand, which would allow police to confirm whether a telecommunications service provider offers or has offered service in relation to a specific identifier, for example a specific telephone number or IP address. The scope of this tool has been deliberately limited to a yes-or-no confirmation, and it pertains only to telecommunications service providers.

Part 1 would also create a new production order from narrowly defined subscriber information, such as name, address and basic information about the services provided, and update existing search warrant powers to better reflect computer searches.

In addition, it would establish new authorities to facilitate lawful requests from Canadian law enforcement to foreign electronic service providers and enhance international co-operation in criminal matters involving electronic data.

These measures are intended to ensure that where lawfully authorized, investigators are able to act in a timely and effective manner, bearing in mind that delays can result in serious and ongoing harm to victims in particular cases and circumstances.

• (1600)

[Translation]

Part 2 of the bill establishes a clear and modern legislative framework to ensure electronic service providers have the technical capacity to effectively respond to lawful access requests, meaning access already approved under existing legislation, such as the Criminal Code or the Canadian Security Intelligence Service Act.

Canada is the only western democracy without a comprehensive legal framework requiring electronic service providers to develop and maintain such technical capabilities. With the exception of an antiquated licensing regime dating back to the 1990s, collaboration in this area remains largely voluntary and uneven.

Part 2 of Bill C-22 sets for core providers minimum technical capability requirements aligned with international standards and provides the Minister of Public Safety with the authority to issue targeted and flexible ministerial orders when specific capabilities are required to meet operational needs.

[English]

Safeguards related to this new framework are embedded in the bill. For example, ministerial orders would be subject to approval by the intelligence commissioner and would be proactively reported to NSIRA. Privacy and cybersecurity considerations are explicitly included in the legislation. Data retention obligations are restricted, and public annual reporting is required.

This part does not create new powers for law enforcement or CSIS to intercept communications or obtain information, nor does it allow direct government access to electronic service providers' systems. It also explicitly prohibits the creation of systemic vulnerabilities, to ensure that a regulation or ministerial order does not weaken encryption or create back doors.

Finally, part 2 establishes tools to promote compliance, including inspections and administrative monetary penalties.

[Translation]

Together, these mechanisms aim to ensure Canadian law enforcement and intelligence agencies have the tools they need to do their important work while maintaining strong accountability and transparency.

Mr. Chair and members of the committee, my colleagues and I would be happy to answer your questions.

The Chair: Thank you, Mr. McGuire.

Mr. Caputo, you have the floor for six minutes.

[English]

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you very much, Chair.

Thank you to all of our witnesses. It's so great to have so many people here around the table for such a complex issue. We're going

to get to know each other very well in the coming two parliamentary weeks.

I never know who to direct my questions to, because there is a lot of expertise here. Whoever is best to answer this, please let me know.

I've looked at the definitions. I've looked at the definitions of "systemic vulnerability", at how it incorporates the definition of encrypted data to some degree, and at the provision, in part 2, that says a service provider does not have to do anything that would create a systemic vulnerability. I'm going to ask a very direct question. Will this bill cover encrypted data? Secondly, is it intended to be that way? I assume that would be yes. Will this bill cover encrypted data? Could somebody please help me with that?

Shannon Hiegel (Director General, National Security Policy Directorate, Department of Public Safety and Emergency Preparedness): Thank you very much for the question. I'm Shannon Hiegel, director general of national security policy at Public Safety Canada.

The bill is in fact encryption-neutral. We want to make sure that, where encryption is used.... There are different ways encryption can be used and different ways in which companies employ it. Therefore, we don't want to leave out the possibility for those companies that may employ encryption where there are keys available and it can be decrypted in a simple fashion.

Frank Caputo: Okay, but with all due respect, Ms. Hiegel, you say "where keys are available". This bill, as I read it, would require a key to be available, would it not?

Shannon Hiegel: Some companies already employ a type of encryption where they have the key. We're not asking for keys to be made if a company already has one.

• (1605)

Frank Caputo: Perhaps we're on different planes here, because my understanding of part 2, in reading it, particularly in proposed section 5, is that it talks about a base level that providers need to come up to. Am I making sense so far?

Shannon Hiegel: Yes.

Frank Caputo: If providers need to come up to that base level and they're not there yet, how do they not then have to create a key to come up to the base level that proposed section 5 says they have to come up to? Does that make sense?

Shannon Hiegel: Are you talking about somebody coming up to a level where they don't even have encryption? That's what I'm hearing you say.

Frank Caputo: No, I meant where there is a service of encryption provided. My question was, will that provider of encryption...?

Company A provides an end-to-end encryption service in messages. Will this bill require company A to create some sort of mechanism by which that data can be intercepted and by which the government or the state—when I say “state”, I think you know what I mean, law enforcement—can access that encrypted data?

Is that clear?

Shannon Hiegel: Absolutely.

If a company has end-to-end encryption as part of its business service and its model, we are not forcing the company to decrypt that communication.

Frank Caputo: Okay. That's unclear at this point. When I read the bill, I thought, “Okay, that's it”, but we've also seen correspondence here. If the target of this bill is not encrypted data, my suggestion is that we say flat out, “For greater clarity, this part does not apply to encrypted data”, and then have a definition.

Does it make sense to do something like that?

Shannon Hiegel: I think we want to be a bit flexible when we talk about encryption. I apologize if the front part of my answer wasn't clear, but there are different types of encryption. If we talk about encryption without any qualifiers, that means that when companies do have keys and could decrypt for the purposes of an investigation where there's a warrant and a production order being provided, they could in fact still use those keys for that purpose.

Frank Caputo: What I'm talking about is a company whose “secret sauce”, if you'll forgive my vernacular, is providing an encryption service. That is what it does. Company A provides a service that says terminal one to terminal two or contact one to contact two will be encrypted. That is its business model.

What I'm asking is this: Will Bill C-22 require it to be able to plug into that encryption and decrypt it for law enforcement?

Shannon Hiegel: No. If there are no keys and there's no way to decrypt it, and that's its business model, then the expectation is that this would be a systemic vulnerability for the entirety of its system, and there would have to be some discussion with government. The end of it is that we would not force it to put into its system a systemic vulnerability.

Frank Caputo: That is exactly what I was looking for, but based on my reading of the bill, when I went through the one definition and then into systemic vulnerability, that wasn't clear to me. My exhortation is this: As officials, please turn your minds to this, because I think there should be, one, an encrypted data definition and, two, something that very clearly says what you just said—that a decryption of encrypted data is a systemic vulnerability—or put it right in the definition of systemic vulnerability.

I know this is technical. I hope I'm being clear here.

The Chair: That may be very clear, but unfortunately we won't know what Ms. Hiegel thinks, because we need to turn to Madame Acan for six minutes, please.

Sima Acan (Oakville West, Lib.): Thank you very much, Mr. Chair.

Mr. McGuire and Ms. Hiegel, my questions will be on the technical side, so I believe you will be answering.

As we examine the evolving landscape of public safety and national security, it's essential to clearly understand the role of metadata. Metadata is often described as data about data that does not capture the content of communications but rather provides contextual information such as time, location, duration, origin or destination of digital interactions.

While it differs from content data, metadata can, in specific circumstances, support analytical insights and help identify patterns that are relevant to operational needs. This makes metadata a valuable operational tool for law enforcement and intelligence agencies, and it plays a critical role in enabling threat detection, risk assessment and investigative efficiency, particularly in an era when digital activity is deeply embedded in our daily lives.

Please correct me if I was wrong about or missed anything regarding metadata, but given this context, could you please clarify the scope of the information that law enforcement would be authorized to access under the legislation, and specifically confirm how metadata is distinguished from the content of communications in practice?

• (1610)

Shannon Hiegel: I'll start off and, if you don't mind, I'll turn it over to my colleague, Fenton. Then, if you'll give me a few minutes, I'll turn to the RCMP and maybe CSIS to explain how important metadata can be in their operations.

As you can see within the bill as it currently stands, we have not given a lot of specificity to what elements of metadata we plan on regulating. That's because we need to take the time to assess that with our investigative bodies and speak with industry about the ability to retain various types and for how long. We certainly do not assume.... Where we note that it's up to a period of one year, the expectation is not that all metadata points will be kept for up to one year. That's why there's a time period.

We've looked at international comparisons on this front, and we've come in about the middle. Australia holds its metadata for two years, and the U.K. holds it for about a year. There's always a bit of small print there, but generally that's what it is.

Through that process, we expect to narrow down what very specific types of metadata are the most important for investigations and then apply a timeline to that within the regulatory process. We will do our charter challenge at that point.

Fenton, is there anything you might like to add?

Fenton Ho (Director, Intelligence Policy, Department of Public Safety and Emergency Preparedness): Thank you.

I think the key idea here is that we're linking the metadata to capabilities that will support law enforcement. That's how we actually generate and derive what we need. The whole thing is that, as Shannon was saying, we'll be working very directly with law enforcement and with CSIS to determine what fields and how they support investigations, so that we can basically have a good, strong argument for why that is proportionate and why that's necessary to keep.

Ramzi Nashef (Director General, Canadian Security Intelligence Service): I have one quick operational point.

What we're talking about here is a better understanding of the pattern of communications, essentially. Through regulations, we'll work through the specific details of the types of metadata we'd be capturing. Generally speaking, from our perspective, the reason we would be doing that is to establish patterns of communication, in a warranted way, to be a building block for an investigation. Obviously, there are many other elements, but that's the sort of pattern we'd be looking for on our side.

Sima Acan: The next question could be probably answered again by you or by CSIS.

Bill C-22 introduces a new confirmation of service demand authority. This amendment to the CSIS Act is intended to allow authorities to continue obtaining necessary information in support of complex and advanced investigations.

How does this yes-or-no confirmation of service process introduced in Bill C-22 balance privacy considerations with investigative requirements? In what way does limiting disclosure to the existence of a service, rather than to subscriber identity, affect the nature and scope of information available to law enforcement?

Richard Burchill (Director General, Technical Investigation Services, Royal Canadian Mounted Police): The confirmation of service demand is very front-end, at the beginning of an investigation, to enable us to gather basic information to pursue an investigation. We have very little information—for instance, a phone number or an IP address. Just that yes-or-no confirmation from a telecommunications service provider gives us the ability to verify that this person is with this company. Then, we can start doing investigative work around that to get enough grounds to bring forward a production order to get subscriber information as a next step. We still have to build those investigative grounds in order to bring forward a production order to get subscriber information from a justice.

Although there are various ways that law enforcement and intelligence folks are able to get that information traditionally, that confirmation of service demand codifies that process and makes it disclosable. We have to document a confirmation of service demand. It goes on our file, is disclosed in court and can be questioned. We have reasonable grounds to suspect and to ask for the confirmation of service. Once it's obtained, then we still have to build investigative capacity around a production order to go to a justice or a judge.

• (1615)

The Chair: Thank you very much.

[Translation]

Mrs. DeBellefeuille, you have the floor for six minutes.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Thank you, Mr. Chair.

Ms. Hiegel, the minister told us consultations were held with certain groups between Bill C-2 and Bill C-22.

Can you confirm the current chair of the National Security and Intelligence Review Agency, Ms. Deschamps, was consulted on Bill C-22?

Mike McGuire: I can talk a little bit about the consultations.

Claude DeBellefeuille: I just need a yes-or-no answer. Do you know if Ms. Deschamps was consulted on Bill C-22?

Mike McGuire: Different types of consultations were held. The minister himself met with certain people, and there were also round tables.

Claude DeBellefeuille: To your knowledge, was Ms. Deschamps consulted? It's a pretty simple question, Mr. McGuire.

Mike McGuire: To my knowledge, she was not part of the round tables we organized.

Claude DeBellefeuille: This means the current chair of the National Security and Intelligence Review Agency wasn't consulted on Bill C-22, but a former chair was. That's what I understood from my readings.

Mike McGuire: For the round tables we organized, yes, but there were other consultations.

Claude DeBellefeuille: Don't you find it a bit odd that the current chair wasn't consulted on a lawful access bill?

When we see what's being done in the countries to which Canada compares itself, and that the agency's counterparts have an important role to play in lawful access legislation, don't you find that a bit odd?

Mike McGuire: We took a lot of information into consideration in our analysis. We also held various consultations and received various letters from stakeholders. Different methods were used to establish stakeholders' positions.

Claude DeBellefeuille: I'm just surprised, Mr. McGuire, because this is an important office. I'm surprised the agency's current chair wasn't consulted.

Did you consult the Privacy Commissioner?

Mike McGuire: Yes, absolutely.

Claude DeBellefeuille: You chose to consult the Privacy Commissioner, but not the current chair of the National Security and Intelligence Review Agency. That's my understanding.

Mike McGuire: We consulted the Privacy Commissioner.

Claude DeBellefeuille: However, you didn't consult the current chair of the agency.

I'm going to ask a question I've asked the Department of Justice team many times in the House. I'm not a lawyer, so I'd like to understand why you chose the lowest threshold for obtaining information.

I think reasonable grounds to "suspect" something seems like a very, very low threshold for obtaining information. Reasonable grounds to "believe" something would be a higher threshold. I don't understand why you chose this one.

Could you give us some examples of what reasonable grounds to suspect something might be? I have a hard time imagining what wouldn't be acceptable. I think any reason to suspect something can be reasonable. That part of the bill worries me. Could you give us tangible examples of what might be reasonable grounds to suspect something?

Anne-Marie LeBel (Counsel, Criminal Law Policy Section, Department of Justice): Thank you for that very good question.

Yes, we can give you some practical examples, and I may turn to my colleague from the RCMP to help out.

Before I do, I can explain why we chose that threshold. This is a legal threshold that already exists in the Criminal Code for other specific production orders, which target specific types of data whose privacy nature is less sensitive than others, including content obtained with a general production order.

Claude DeBellefeuille: Could you tell us what would be reasonable grounds to suspect something so I can clearly see the difference between this threshold and other thresholds and understand what your intention is?

Anne-Marie LeBel: Before my colleague gives you a tangible example, I'd like to add that reasonable grounds to suspect something is not just suspicion. There have to be observable facts. A police officer must have notes related to these facts when they decide they have reasonable grounds to suspect that an offence has been or will be committed.

In both of our tools, the condition is that there are reasonable grounds to suspect an offence has been or will be committed, but also that the information requested will be useful to the investigation.

• (1620)

Claude DeBellefeuille: Thank you, Ms. LeBel.

I would need that. I'm not a lawyer, and I'd like to get a better understanding, if I could.

I'd like to use the time I have left to understand something else. In part 1 of the bill, it says that "telecommunications service provider has the same meaning as in subsection 2(1) of the Telecommunications Act", whereas part 2 of the bill talks about an

electronic service provider and a core provider. However, there is no definition in the schedule.

I want to understand why this very broad regulatory power is being given in definitions. People are wondering whether they'll be affected. Can you explain why there's no definition, why there's nothing in the schedule and why everything will be decided by regulation?

Anne-Marie LeBel: I think the question relates more to part 2, so the new act and schedule. I'll let my colleague answer it.

Shannon Hiegel: Yes, that's a question for me.

You're right to say that, in part 2, there's just a definition for an "electronic service provider".

It's a very broad definition, and that's important, because technology is evolving quickly.

The Chair: Unfortunately, I have to interrupt you, because the time's already up and I think it might be a long answer. We may come back to that later.

Mr. Lloyd, you have the floor for five minutes.

[English]

Dane Lloyd (Parkland, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for being here today.

I'm going to start with Mr. McGuire.

Something I find contradictory in this bill—maybe you can explain how it's not contradictory—is that you're requiring electronic service providers and telecoms to create the systems to enable the interception of communications within their networks, yet later you say that nothing in this bill seeks to undermine the integrity of encryption networks. That seems very contradictory to me.

In light of the Salt Typhoon hack we saw in the United States.... It was later found that it was exactly the vulnerabilities created by the requirements under U.S. law to create these encryption back doors that allowed hackers to access this information.

Can you explain what this contradiction appears to be?

Mike McGuire: I'll start quickly and then turn it over to Ms. Hiegel.

The intent of part 2 is to ensure that electronic service providers have the technical capabilities to respond to lawful access requests that are authorized for law enforcement and for CSIS.

Shannon, do you want to add anything?

Shannon Hiegel: I'll start off and then I'll flip it over to Fenton.

We've taken a look at a multitude of other countries that have this type of legislation in place and have found ways to work with companies to pull the information out so that it can be provided to investigators for their specific investigations.

I don't feel that there's necessarily a contradiction between the two parts, because we are going to set objectives. We, the government, are not going to tell companies—or core providers, essentially—what and how they need to create—

Dane Lloyd: I understand what you're saying, which is that the government isn't dictating how the companies are to do it, but it is mandating the companies to do it, and in order to comply, companies may have to create vulnerabilities in their system that can be exploited by hackers. Wouldn't you agree?

Shannon Hiegel: I would say that companies create all sorts of changes within their systems for purposes that they see fit. Through this piece of legislation, we're hoping and we expect to find safe ways to maintain their cybersecurity, as Canada expects.

Canada, first and foremost, puts priority on cybersecurity—

Dane Lloyd: I'll interrupt you there.

If it comes to a choice between a company complying with the legislation and creating a vulnerability that can be exploited by hackers, what is the end goal or outcome of the Government of Canada?

Shannon Hiegel: I think the expectation is that, in consultation with government, we will find solutions to this. It is a problem that desperately needs a solution. Working with industry to be able to get information to the investigators to investigate so many crimes that are now going unsolved—

• (1625)

Dane Lloyd: If you can't find a solution, at least in the short term, is it acceptable to the government that telecommunications companies be forced to create systemic vulnerabilities in order to comply with the legislation?

Shannon Hiegel: There are partners we already work with right now, so I would question the idea that there's no way to be able to put solutions in place.

Dane Lloyd: The Canadian Chamber of Commerce has said that this legislation is going to force their members to create vulnerabilities in their systems. That's a pretty big stakeholder, including many stakeholders that the Government of Canada works with.

This is a big concern, so I just I want it clear: If the only way to comply with this legislation is to create systemic vulnerabilities, does the government still think companies need to comply with this legislation?

Fenton Ho: We're talking about various capabilities. It's not one universal capability. Also, these capabilities already exist right now. A lot of the major telecoms, because of the licensing regime, already have the capability to address certain requests from law enforcement or CSIS, so in that case, the bill basically creates a level playing field for what exists.

However, if you're looking at a particular application, a particular capability that doesn't exist, if it hits a systemic vulnerability, the answer would be no.

Dane Lloyd: I have 45 seconds left, so if I can get that in writing from you, please send that in writing.

In my last 45 seconds.... The Secretary of State for Combatting Crime said that many stakeholders are calling this an essential first step and that they need to broaden this legislation. Is the Department of Public Safety working on or envisioning a follow-up piece of legislation to expand the powers given under Bill C-22 at this time?

Shannon Hiegel: No, not at this time.

Dane Lloyd: Can you say that the department has done any studies on what the next steps would be, should this legislation pass, for follow-up legislation in this area?

Shannon Hiegel: No, we are very focused on the regulatory step that would follow, if we are successful in getting royal assent.

Dane Lloyd: Thank you.

The Chair: Thank you very much, MP Lloyd.

MP Powlowski, you have five minutes, please.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): I have a letter before me entitled “Joint Call for the Withdrawal of Bill C-22”, which is signed by a number of seemingly pretty reputable organizations, such as the British Columbia Civil Liberties Association, the Canadian Association of University Teachers, the Canadian Civil Liberties Association and the Canadian Council for Refugees. In it, they talk about the “enormous overreach of Bill C-22 and the unprecedented, open-ended powers it introduces”. Then it goes on.

There's one specific provision I want to ask you about, but let me read the whole paragraph. It says:

Bill C-22 makes some improvements to Bill C-2's proposal for wide-ranging warrantless access to sensitive subscriber information. The warrantless demand power can now only be used to require telecommunications service providers to confirm if someone is a customer. However, Bill C-22's approach to subscriber data remains flawed, dropping the judicial authorization standard for a warrant from “reason to believe” to the far lower “reason to suspect” threshold despite Supreme Court decisions recognizing the significant privacy interests engaged by this form of data access.

If we're worried about overreach and if we're worried—as they are—about mass surveillance of all Canadians, I would tend to agree that “reason to suspect” seems a very low threshold for accessing potentially personal data. Does somebody want to answer this accusation?

Kimberly Gibner (Deputy Assistant Deputy Minister, Policy Sector, Department of Justice): I'll take that question.

I think my colleague touched on that and highlighted that there are all sorts of Criminal Code provisions that use the reasonable grounds to suspect standard. In this case, what you're looking at in terms of the subscriber information is essentially a name and an address. On the balance of that type of information with the privacy concerns, reasonable grounds to suspect was chosen as the appropriate standard.

Just to speak to your point about Spencer, what the decision said was that it was critical that there be lawful authorization, so since 2014, police have been calling for lawful authorization. That's what Bill C-22 does. It provides lawful authorization.

Marcus Powlowski: Now, for end-to-end encrypted services, like Signal, where the providers never possess the unencrypted data or decryption keys, these providers would not be expected to degrade their encryption to comply. Is that correct?

• (1630)

Shannon Hiegel: That is correct.

Marcus Powlowski: Okay.

Lastly, you talk about collecting metadata. What sort of metadata? If I'm on the Internet and if I'm sympathetic to the people of Gaza and searching about Gaza and inadvertently something comes up on Hamas, is there a reason for the government to further investigate me because of the possibility that I may be somehow doing things to promote a terrorist organization? What sort of metadata are you looking for? Metadata seems pretty broad. I mean, that's everything we do. If you put it into computer AI, you'd find something on Marcus Powlowski.

Shannon Hiegel: It's understandable to be concerned about that. What I would like to do is turn it over to my RCMP colleague, who, along with his team, is going to help define the very specific elements of metadata that are required. They will be regulated, but my colleague can give some specific examples.

Richard Burchill: I can give four examples of metadata retention that are helpful for law enforcement in an investigation. One is Internet transmission data, which includes time-stamps, IP addresses and device identifiers. As you can appreciate, we don't start an investigation immediately when something happens. When something happens and there's online activity, there generally needs to be a report made and an investigation generated. If we're looking to get metadata, there has to be a judicial authorization; there's criminality involved, and there are victims involved at the front end of this. By the time we get to the point where we're seeking the metadata, it's to try to link people to places. That's Internet transmission data.

Tower signalling data is also helpful to locate folks at a point in time when there is an offence that happened or a call, if it's a kidnapping or something, where we need to find the location of somebody who had a vehicle or a phone at a certain time.

The Chair: I'm sorry, but I have to interrupt you abruptly so we can move to Madame DeBellefeuille.

[Translation]

Mrs. DeBellefeuille, you have the floor for two and a half minutes.

Claude DeBellefeuille: Thank you very much, Mr. Chair.

Ms. Hiegel, Bill C-22 still gives the intelligence commissioner an important role. Have you assessed the additional work the adoption of this bill could cause them?

Shannon Hiegel: Thank you for the question.

[English]

I apologize. I'm going to speak in English.

We actually have met with the intelligence commissioner himself and his staff to talk about the role. Once it is approved, he will be the second key. He has spoken to the fact that.... We have given some sense of what we expect and how many ministerial orders there may be on an annual basis.

[Translation]

Claude DeBellefeuille: [Inaudible—Editor] your assessment. How much do you think they'll be solicited with the adoption of Bill C-22? As you know, they tabled their annual report, which contains a record 14 decisions. Now, I wonder if there will be a lot of decisions. Did you assess the number of decisions the commissioner might have to issue?

[English]

Shannon Hiegel: His role is specific to the ministerial order approval process. He will be reviewing all of the information that was given to the minister when the minister made his or her decision on a ministerial order, which is a very specific request to put in place certain capabilities for a company that would not be included as a core provider.

[Translation]

Claude DeBellefeuille: That means it's exceptional. It's not going to be common. There aren't going to be a lot of decisions. The intelligence commissioner isn't going to be overwhelmed with decisions.

[English]

Shannon Hiegel: No, and he has confirmed that. We gave him some initial numbers around how many ministerial orders would come to him, and he was sufficiently satisfied that he could manage it.

[Translation]

Claude DeBellefeuille: Okay.

I know his office's budget wasn't increased to meet its obligations in Bill C-22, so I was wondering what the workload would be like.

You may not have time to answer this, but why didn't you include in part 2 a clear definition of "core provider"?

• (1635)

[English]

Shannon Hiegel: For a core provider, we do have a definition. What we expect to do is run through the regulatory process, where there will be classifications or classes—

[Translation]

Claude DeBellefeuille: There is none in the bill, Ms. Hiegel. It'll be dealt with in the regulation.

[English]

Shannon Hiegel: Yes, it will be in regulation.

[Translation]

The Chair: Unfortunately, I have to cut you off there. I apologize.

Mr. Caputo, you have the floor for five minutes.

[English]

Frank Caputo: Thank you very much.

It's been helpful to have the officials. One thing I will say at the outset is that I feel like we need three hours with you. I don't say this in jest. This is a highly technical bill. We can't rush this. I have a list of about eight things I want to ask you about.

I'm looking up case law further to Madame DeBellefeuille's earlier point about the threshold of "reasonable grounds to suspect" versus "reasonable grounds to believe". I haven't studied reasonable grounds to suspect in years. With regard to reasonable grounds to believe, I'm familiar with the Storrey decision that a person must subjectively believe that what they're doing is reasonable and that it must be objectively reasonable.

That probably means nothing to a lot of people, but these are difficult things to comprehend. When we're wrapping our heads around this, I think having you here for only one hour prior to clause-by-clause consideration is inadequate. I think we need you here a whole lot more, to be very candid. I'll leave that with you and with the chair and with my Liberal colleagues, because we have lots of questions, and I know I've just burned a minute here.

This is an important question that comes to the requirement for an electronic service provider to retain data for one year. Is that a de facto seizure that runs contrary to section 8? I understand that a search warrant is required, and that would be the search aspect. Normally there's the search and then the seizure. Is the compulsion to retain data a seizure in itself?

Shannon Hiegel: I'll attempt to just simply say that we have not equated the expectation of the retention by a company to a seizure within the context of an investigation, because there has been no production order or warrant approved by a judge. That would be my simple assessment of the scenario.

Do any of you have thoughts?

Richard Burchill: As you said, we need a judicial authorization in order to access that data. The timeliness of it is.... There are companies that already retain this metadata. There's not a consistent application of how that happens among telecommunication providers, which is what security and law enforcement would look for. When

we're looking to access that data, the reason for the timeliness is that if they keep it for three days but you're one week into a kidnapping investigation, that data is gone, whether you are judicially authorized or not, whereas some companies will have it readily available.

Frank Caputo: I understand that. I'll tell you where I'm coming from on this. In this instance, the state or the government is compelling an action, and that action relates to information over which there is a reasonable expectation of privacy. That's why you need a warrant. The moment you say to provider A that they need to keep this, there's a reasonable expectation of privacy over what must be kept. Is everybody with me so far? Okay.

Does that not engage section 8? I might be out to lunch here, but I've been asked this question, so it's something I'm looking to explore.

Shannon Hiegel: Just as a point of clarity, when you say section 8, do you mean with regard to part 2 of the bill?

Frank Caputo: Yes.

Shannon Hiegel: Fenton, do you want to jump in?

Fenton Ho: Obviously, we've had discussions around charter statements and stuff about that. Part of the analysis on that point will be how we actually circumscribe our use of metadata. In this case, we are clearly not looking.... The maximum is one year. We're not saying it's blanket retention. In the process of developing the regulations, we would have to prove that they're necessarily in proportion with that amount of time. At that point, we can come to an understanding of what charter obligations arise from that.

Frank Caputo: Let's go along that line here. The one year is kind of the benchmark. Are you saying...? We could talk about this for the next 15 minutes—this is, again, very important—and I have 33 seconds. What you're saying is that one year is the maximum. It's not the minimum. It's not just the drop-dead date. It's only one year. Obviously, any date is arbitrary. Why is it a year? Why is it not nine months or 15 months or two years?

Can you offer anything to help out this committee in terms of why a year was picked?

• (1640)

Shannon Hiegel: As I mentioned earlier, we have done a lot of country comparisons within our analysis. One year was actually quite common in being the average. As I said, Australia is on the higher end, with two years.

We also want to make sure that we're clear that what we are expecting to retain within the metadata context still needs to be defined. The expectation is that there is some level of rationale. Maybe the metadata of me speaking with Fenton is really important, because now I know who was talking to whom, so it would be kept for a year, while something around—

The Chair: I'm sorry to interrupt, Madame Hiegel.

We need to move to MP Housefather for five minutes, please.

[Translation]

Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chair.

[English]

It's always fascinating to listen to my colleague Mr. Caputo.

First of all, let me start by saying thank you so much for being here.

Obviously, I'm strongly in favour of this bill. As I said in the House, I think we need a modern access regime. I think we need to deal with Bykovets and Spencer and have proper legislation that allows us to deal with things like that.

I also had a couple of questions, if that's okay, with respect to the way systemic vulnerabilities interplay in this bill, in proposed subsections 5(5) and 7(5) of the bill versus proposed sections 12 and 13. Basically, what I understand from proposed subsections 5(5) and 7(5) of the bill is that a provider is not required to comply if a systemic vulnerability would be created. I think I have that right. However, proposed section 12 says, "An electronic service provider that is subject to an order made under subsection 7(1) must comply with it." Then proposed section 13 specifies that orders take primacy over the regulations that will be made.

I don't really understand, personally, the interplay here, where we're saying that somebody is not required to comply if it creates a systemic vulnerability, but then if there's an order, they're required to comply with it, and then the order supersedes regulations.

Can you talk me through this so that I understand how 5(5) and 7(5) actually work?

Shannon Hiegel: Sure. I'll start off, and then I'll turn to my expert, Fenton.

We have to consider this as a bit of a continuum, where the baseline has to be that you as a core provider—if it's regulation or if you're being tapped through a ministerial order—need to comply with this. Then there is the exception. If, as we go through this process with you to determine how to get that information off your networks, it is determined that it is a systemic vulnerability, then there is the right for a company to push back and say, "No, we can't give you the information you need because of a systemic vulnerability."

Anthony Housefather: If we want to say that, why would the bill itself not...? Right now, we agree that an order is paramount, and they must comply with the order. Is that correct?

Shannon Hiegel: Yes. That is the baseline.

Anthony Housefather: If the company believes that it would create a systemic vulnerability, under what circumstances is the

company then able—unless it convinces the minister or representatives of the minister—to push back and say, "No, this would create a systemic vulnerability"? How come the bill as drafted doesn't say that the order must be complied with except to the extent that the company believes that, using reasonable commercial efforts, it cannot do this without creating a systemic vulnerability, or something like that?

If the company believes this, but the minister's office is not accepting that argument, what happens to the company?

Shannon Hiegel: Within the context of a ministerial order specifically.... I'll stay away from those who are—

Anthony Housefather: I'm only asking about the ministerial order.

Shannon Hiegel: Okay. The expectation is that Public Safety would be responsible for actually completing the analysis that the minister considers. Therefore, we intake information from the operating agency that has flagged the issue or the threat existing within a company's system. We actually are required to consult with that particular firm and satisfy a number of factors that are listed in the bill. As the company is with us through this process, they are able to voice their views.

Once we get to the final stage, if the minister then approves the process, the intelligence commissioner has full disclosure of all the information the minister had, and if he also agrees with the process to advance, the company does have the right to a judicial review.

● (1645)

Anthony Housefather: At what point? The company is told at that point that the minister and the commissioner have said they must go forward, regardless of their claim. Then they would go to judicial review.

What happens until that review is heard? Are you saying there would be a stay on carrying out the order?

Shannon Hiegel: That's correct.

Fenton, do you have anything to add?

Fenton Ho: No, I don't have anything to add.

Anthony Housefather: I appreciate that.

The Chair: Unfortunately, there is no more time.

Thank you, MP Housefather, for this intervention.

We will now move to MP Caputo for five minutes, please.

Frank Caputo: Thank you.

I want to pick up on the one-year retention period. If I understand it correctly.... The metadata is generally what we're talking about here, or whatever is contemplated in proposed section 5. Let's just say it's data that can be compelled to be kept. My understanding of what was said before is that one year is the maximum, and one year was chosen because it's like an international standard. There's nothing magic about one year. I understand that. Every number is arbitrary. However, not everything will be kept for one year. Am I clear on that?

Shannon Hiegel: Yes, that's correct.

Frank Caputo: Who decides what type of metadata will be kept for how long? Say, this type of data, an IP address or whatever, only needs to be kept for six months. Who decides that?

Shannon Hiegel: That will be achieved through the regulatory process, for which we will develop an analysis with the agencies as to what is most valuable when it comes to the investigative processes, as well as with companies. When we carry out the regulatory process, we have to consider things like the cost to industry of implementing new regulations. They would definitely be involved. As Rick mentioned, sometimes they already have that data in their holding, and there is no new delta cost to them. In other cases, it may be significant. We need to take the time to do that analysis and come back with a thoughtful scheme.

Frank Caputo: On first blush, I have an issue with that, because you only have to consider costs; you don't have to make your decision based on cost. It is a consideration.

The other issue is that one of the principal discussion points surrounding this bill is how much is left to regulation. Essentially, 90% of this bill could operate on regulation with ministerial orders and things like that. Should we not be spelling things out more in the bill when it comes to certainty? If you're a small electronic service provider trying to implement part 2, wouldn't you be shaking right now and thinking, "Oh my gosh, how much is it going to cost me to comply?" There is no certainty regarding what they'll have to comply with.

Shannon Hiegel: Let me tackle the last part of your question right up front. Core providers are also expected to go through a process by which we look at considerations of things like how big they are or how many customers they serve. It is unlikely that we would be regulating small business owners and operators through the core provider portion of this bill.

Frank Caputo: Again, I'll go back to my prior point. That falls to regulation and it falls to somebody else's decision where there is a consideration about the size and the cost. Ultimately, just because it is considered, that doesn't mean the core provider won't have to do what a ministerial order says. Does that make sense?

Shannon Hiegel: I understand what you're saying. Part of why the bill has a higher level of detail than others you may be thinking of is the fact that it is heavily based in technology. Using terms that could be obsolete within a number of years would render the whole bill useless.

• (1650)

Frank Caputo: I appreciate that. I know that some things have to be left to regulation. My view is that a bill like this should be as

prescriptive as possible, where it can be, because there is so much left to regulation.

For instance, every ministerial order, as I see it under proposed section 7 in part 2, has to be approved by the intelligence commissioner. Is that accurate?

Shannon Hiegel: That's accurate.

Frank Caputo: Why not a Federal Court judge? I get it. They're both presumed independent. I assume the intelligence commissioner is presumed independent; I can't imagine why. Both are government-appointed. Both are presumed to have perfect knowledge, and I think you know what I mean by perfect knowledge. They are both presumed to have all the knowledge. A Federal Court judge, however, is not beholden to the government. They aren't "hired". Their term isn't renewed or anything like that. They can sit until they're 75.

Why not have a Federal Court judge play the role of gatekeeper, rather than the intelligence commissioner, when there is at least a reasonable perception of connection to government?

Shannon Hiegel: Before I flip it to Fenton, I just want to say that within the ministerial order process, we have the Department of Public Safety doing the analysis. We have the minister approving. We have the intelligence commissioner, who is independent, also approving. We have a quasi-judicial oversight body, and then there can be a judicial review. Literally, on the judicial side, that's the only entity we've left out.

Fenton Ho: I would add that, at the end of that, we have NSIRA.

I think the intelligence commissioner is well versed because they are used to doing lots of things like ministerial authorization for CSE and the justification framework for CSIS. They're well versed in these particular issues. They have the knowledge, and from that point, they can actually do that function well.

The Chair: Thank you.

I'm sorry, MP Caputo. We have run over the time.

We are going to suspend now, since, as we have seen, the minister has entered the room.

Thank you, officials. Many of you will stay.

[Translation]

We will resume the meeting in a few minutes. The meeting is suspended.

• (1650) _____ (Pause) _____

• (1655)

The Chair: I call the meeting back to order. Thank you, everyone, for coming back.

I'd like to welcome the two ministers and the officials accompanying them, starting with Minister Gary Anandasangaree, MP and Minister of Public Safety. I would also like to welcome Minister Sean Fraser, MP and Minister of Justice.

Welcome to both of you, ministers. We'll begin with an opening statement from the Minister of Public Safety, followed by the Minister of Justice.

Mr. Anandasangaree, you have the floor.

Hon. Gary Anandasangaree (Minister of Public Safety): Thank you, Mr. Chair.

[English]

I would like to start by acknowledging that we're meeting on the traditional and unceded territory of the Algonquin Anishinabe people.

[Translation]

Thank you for inviting me to appear today to speak about the proposed Bill C-22.

[English]

I also want to acknowledge my colleague, the Honourable Sean Fraser, as we've been working on this bill for a number of months, and also the officials who are here to support us.

As Minister of Public Safety, my top priority is to ensure that every Canadian remains safe and secure. Since my appointment, I've heard clearly from law enforcement at all levels—municipal police services and the RCMP—as well as victims groups such as the Canadian Centre for Child Protection. They've all said that Canada needs modern tools to take on the wide array of illicit activities that are facilitated by the global digital environment.

Technology has fundamentally changed the nature of crime and threats globally. Criminals are continuously exploiting the digital space we all use, in order to facilitate a wide array of offences. This includes extortion, childhood exploitation, auto theft, terrorism and human trafficking. Furthermore, this environment is being used to facilitate foreign interference and violent extremism.

Our laws have simply not kept pace with our digitally driven world. This has created a significant gap between today's crimes and threats and what our current laws can meaningfully address.

[Translation]

We have a duty to Canadians to address these new threats.

[English]

This is what Bill C-22 aims to do.

It's worth taking this opportunity to highlight that Bill C-22 does not aim to regulate the Internet, police activity on the Internet or re-

quire Internet service providers to become agents of the government, as some of the debate in the House has suggested.

As our officials have confirmed, Bill C-22 is encryption-neutral. It is simply to address gaps in our legal framework that present challenges to timely access to information and intelligence that are vital to conducting investigations. It will give our officers the tools they need to keep Canadians safe in the 21st century, while ensuring we continue to uphold Canadians' charter and privacy rights.

• (1700)

[Translation]

We listened to the concerns of stakeholders and other parliamentarians after the tabling of Bill C-2.

[English]

Part 1 of Bill C-22 includes important safeguards, such as limiting the scope of confirmation of service demand to telecommunication service providers; a narrow definition of subscriber information; and strong judicial oversight. Police will still require court approval to obtain personal details like names, addresses and phone numbers.

Under part 2 of the bill, we'll ensure that electronic service providers can fulfill lawful access requests. Let's be clear: This part does not create new authorities for law enforcement agencies and CSIS to intercept communications or obtain information. Its focus is to ensure that electronic service providers are able to comply with existing legal orders, which are found in the Criminal Code and the Canadian Security Intelligence Service Act. Key elements include a new compliance framework that will require core providers to have the technical capability to comply with legal authorization to obtain information, such as warrants and production orders.

It would also give new ministerial order powers to the Minister of Public Safety. Only with approval from the intelligence commissioner, the minister could order an electronic service provider to develop specific technical capabilities: for example, to address new technologies that are developed but not captured in the regulations.

Finally, it introduces regulatory enforcement tools, such as administrative monetary penalties for any provider that does not comply.

Once again, I wish to underscore the safeguards that would be in place under this part of the bill. As I mentioned, all ministerial orders will require prior approval from the intelligence commissioner to ensure they are reasonable.

This part also includes an explicit safeguard to prevent the introduction of systemic vulnerabilities in electronic protections. Our government does not support the creation of back doors.

We want Canadians to see exactly how these powers are being created and used to ensure that their implementation is subject to the highest levels of democratic scrutiny. Under our current laws, our police and intelligence officers are trying to fight tech-savvy criminals and state actors with tools that are decades old. Bill C-22 would bridge that gap, while upholding the charter rights and the privacy of all Canadians.

[Translation]

Thank you. I look forward to your questions.

The Chair: Thank you, Minister Anandasangaree.

Minister Fraser, the floor is yours for five minutes.

Hon. Sean Fraser (Minister of Justice): Thank you, Mr. Chair.

Before I begin my opening statement, I'd like to thank everyone for being here to take part in this very important debate.

I think it's important to understand the context of this bill. To improve public safety, we have a strategy built on three pillars. The first is to strengthen criminal laws, particularly with Bill C-9, Bill C-14 and Bill C-16.

That said, we recognize it's not enough just to make changes to criminal laws. We also need to support those working on the ground in our communities, such as community organizations and police officers. It's not enough to increase the number of people working in the communities. We also have to give them the tools they need so they can meet the expectations we have for the officers on the ground.

We also need to invest to prevent crime and violence in the long term. That includes making investments in affordable housing, making investments so people with mental health issues can have medication and making investments to support young people who have issues in their lives.

[English]

This bill is focused on that second pillar, supporting those who are on the front lines trying to make Canada safer every day. We can't expect people to address modern challenges with outdated technologies. That's where this bill comes in.

When we compare Canada with other partners around the world, we are significantly behind when it comes to addressing modern challenges, particularly in a digital context. Technology has changed. The world has changed. Crime has changed. It is faster-moving. It crosses borders. It is digital on an increasing basis. We've seen that other jurisdictions have embraced what we are discussing and calling "lawful access". Very simply put, it's the ability of law enforcement to get access to the evidence they need that may be digital in nature, the same way we would allow them to get access to evidence that exists in the physical world. You can't arrest an IP address or a phone number.

We need to give tools to ensure that law enforcement has the ability to figure out, where there is a criminal investigation going

on, who is the person behind it and how they can advance that investigation. When I look at the actual process we've laid out, I think it's important that we demonstrate to Canadians that we have put significant thought into ensuring that privacy rights are protected, in the same way that we embrace the recommendations of law enforcement to make it easier for them to do their jobs.

In particular, to start off, what we're allowing under this legislation is for law enforcement, when they have an investigation involving a phone number or an IP address, to make a simple request of a service provider: "Is this on your network?" If the network comes back and says it is, that would allow us to move forward with a process, which would be approved by a judge, to say, yes, there is a person with a name and an address attached to this. Currently, this process can take months. When we're dealing with people who are involved in criminal organizations—engaging in child sexual exploitation, engaging in drug trafficking and human trafficking, organizing home invasions and auto theft rings—you can appreciate the need to move quickly. It is essential if we're going to reduce the ultimate consequences of crime to Canadian communities.

This bill, in my view, provides the appropriate framework that empowers law enforcement to have the tools they need to keep Canadians safe, but it puts protections in place to ensure that, where appropriate, judicial authorization remains essential, and we put a system in place so that service providers actually do hold the information that will help facilitate these investigations.

Let me perhaps sum it up simply: We are not going to solve Netflix problems with Blockbuster technology. We have to join the advanced economies in the world that have been working to solve these problems for many years. With the support of different parties at this committee, I think we have the potential to send a strong signal to Canadians that when it comes to public safety, we will make absolutely sure that law enforcement has the tools they need to keep Canadians safe.

• (1705)

[Translation]

Thank you, Mr. Chair.

The Chair: Thank you, both.

Mr. Caputo, you have the floor for six minutes.

[English]

Frank Caputo: Thank you, Mr. Chair.

Thank you to the ministers and officials.

I'll note that we have two Kamloopsians at the table today. That's always wonderful.

Minister Anandasangaree, you're off the hook today. We won't be asking you about visas and who gave people from the IRGC a visa. We'll stick to Bill C-22 here.

I want to go into something you mentioned, Minister. You talked about this being encryption-neutral. One of the greatest concerns I'm hearing about is encryption. Please don't defer to the analysts. I want to hear your perspective on this. This bill could threaten encrypted communications, based on the way it is written or the way some people are reading it.

Can you confirm that the purpose of this bill is not to go after end-to-end encryption, as in party A is using a program to deal with party B that is encrypted and there's no way to decrypt it? Can you confirm that this is neither in this bill nor the intent of this bill?

Hon. Gary Anandasangaree: I can confirm that, yes.

Frank Caputo: I'll just ensure one step further: that there's no requirement for company A, then, from point one to point two, to create what some would call a back door, a mechanism by which that information can be accessed. Is that accurate as well?

Hon. Gary Anandasangaree: I addressed that in my initial opening.

Frank Caputo: If there's any ambiguity on that, I trust you would support an amendment to close that, because this is a game-changer when it comes to that bill.

I take that to be the case.

Hon. Gary Anandasangaree: I would say what I told you privately, Mr. Caputo. We brought this bill forward with a number of engagements, including with colleagues in different parties. We will work in collaboration to strengthen the bill. If there are specific recommendations that this committee comes up with, we will certainly take them under consideration. We look forward to that engagement to get to the right result.

● (1710)

Frank Caputo: I'll be blunt, Minister. The Liberal government now has a majority. There is a concern that, if there is room there, it won't be addressed.

That's why I'm asking you, on the record, if there's a chance that encrypted communications can be targeted by this bill. If that's not the intent of the bill—that's what you said—I don't think it's too much to say, “Yes, Mr. Caputo, I would support an amendment to ensure that our intent is clear.” For instance, that could be an amendment that includes a definition of encrypted data in part 2 or an amendment that says that “systemic vulnerability” includes a key to encrypted data and the creation thereof.

With all due respect, Minister, I don't think it's difficult to say, “Yes, that's our intent.” Do you not agree?

Hon. Gary Anandasangaree: What I will repeat is that we are willing to work together in collaboration in advancing the bill.

I was at the Senate yesterday on Bill C-8, and 75% of the amendments that were passed were opposition amendments. They weren't government amendments.

On this bill, I think we have been very clear, both of us, that we will work with the opposition, as we have on every other bill, to advance and strengthen the bill.

Frank Caputo: The difference with Bill C-8, though, Minister... If you want to get into Bill C-8, that is exactly my cautionary tale. The Liberals voted against just about every amendment that was of consequence. It was the Conservatives and the Bloc that voted for those amendments, that swayed those amendments, with the government often voting against them. Now things have changed. With all due respect, Bill C-8 is not a great example to use. That's why I'm trying to get it on the record.

I think I've made my point. You've made your point. Let's move on.

The ministerial order is one of the biggest things. One of them, as I said, is encryption; another major issue is the degree to which enforcement and definitions are left to regulation. That's one of the primary criticisms of this bill.

I look at proposed section 5, for instance. This is sweeping powers. Proposed paragraph 5(2)(b) says, “the installation, use, operation, management, assessment, testing and maintenance of any device”. Proposed paragraph 5(2)(d) says, “the retention of categories of metadata”. Minister, I get why the government wants things to be broad; it's because then you can account for things. However, should we not be defining things where we can define them? I'm pretty sure we're going to have experts who say, “Do you know what? We can define categories of metadata.” I'm sure we can define categories of metadata. Those don't change every day.

Would you be open to an amendment that says that when we're looking at taking information from people over which there's a high expectation of privacy...? I trust you would support an amendment that would define those types of things.

Hon. Gary Anandasangaree: I'm going to go back to my initial position, Mr. Caputo. We will consider specific amendments that you propose. I will personally engage with you on this. However, I don't think I am going to pre-emptively agree to amendments that you're proposing here.

Frank Caputo: Just [*Inaudible—Editor*].

Hon. Gary Anandasangaree: It would be irresponsible for me to say that I will accept all of these amendments. I think what's important is that we look at them and at the implications for the bill. We'll be more than glad to give you our feedback—as I always have.

The Chair: Thank you for that respectful and useful exchange.

Madame Sodhi, you have six minutes, please.

Amandeep Sodhi (Brampton Centre, Lib.): Thank you, Mr. Chair.

Thank you to our ministers for attending today.

Minister Anandasangaree, in Brampton, we have seen a concerning rise in crime of any and all types, from car thefts to robbery, breaking and entering, murders and shootings in broad daylight. I'm worried about the safety of my constituents and all residents of Brampton, and they are as well. Our mayor, Patrick Brown, and Peel Regional Police chiefs have been calling for legislation like Bill C-22 and have welcomed this bill's introduction.

With that local context in mind, can you describe the specific threats this bill is designed to respond to and the real-world operational gaps facing law enforcement and CSIS today that Bill C-22 would close?

• (1715)

Hon. Gary Anandasangaree: Let me acknowledge the work of Peel Regional Police in informing us on the development of this bill. It's been quite critical. I've had conversations with Chief Nishan Duraipappan on a number of occasions.

This is the number one priority as indicated by police leaders, not just in Peel, but across Canada at every level, whether it is Commissioner Carrique in Ontario with the OPP or Commissioner Duheme at the RCMP, as well as regional police services. This is of critical importance.

In a granular sense, the technology we have today is inadequate to deal with the types of issues we're dealing with. Primarily, telephones, the Internet, emails and electronic devices are used on a day-to-day basis for the execution of crime. Extortion, for example, is oftentimes done by way of a phone call or a text, or sometimes by email. Over the years, all of this has meant a great deal of delay for law enforcement to be able to get production orders. Oftentimes, they have to wait weeks, sometimes months, to get the information that will enable them to go to the next step.

Essentially, what we're doing here.... I'll use the example of a phone directory or Bower's reverse lookup, which can be found at a local library. If you have a phone number, you can go to the Bower's directory, put the phone number in and get the address of the individual who owns the phone number. Right now, these are often anonymous, which means that we need to go to the service provider. If it is a telco, we need to go to the telco and ask if this particular telephone number is associated with their service. It takes weeks, sometimes months, to get that information.

Bill C-22 would, as a starting point, enable law enforcement to get what's called confirmation of service. That will say whether this phone number is attached to the service the telco provides. Once that information is obtained.... It's a yes-or-no answer. If it's a no, the matter stops there. If it's a yes, then a production order, a warrant, will need to be prepared, seeking subscriber information on the individual whose phone number may be associated with the telephone company. Based on the warrant, we will get basic subscriber information, which would be their name, email address and so on.

Beyond that, any additional information that is required will go back to what we do right now, which is go back to court, all under judicial authorization, to be able to get the type of information that's required for that investigation to continue. Essentially, an investigation that takes months could take weeks, based on the additional provisions that are provided within this bill.

Amandeep Sodhi: Minister, you said that you discussed it heavily with Chief Nish from Peel Regional Police. Do you find there is consensus? Do police jurisdictions from all over Canada want Bill C-22?

Hon. Gary Anandasangaree: I would say that we've had a number of engagements. The Honourable Murray Rankin engaged in some mediation sessions and advised us on near consensus. I wouldn't say there was consensus, but there were civil liberties organizations and industry representatives present. We had law enforcement, as well as community advocates in different conversations.

What we have here is an area where I think there is a great deal of understanding and acceptance. It is not perfect. Not everyone is 100% behind this. There are concerns that people continue to express, but, by and large, this reflects.... Even with law enforcement, we have had to curtail.... You will see some significant changes in Bill C-22 from Bill C-2, for example narrowing and defining certain aspects of what is included.

We have done an enormous amount of work to build what we think is as close to a consensus as we can get. We won't get full consensus. I think the work we need to do is make sure that all the safeguards are in place. We are fully confident that both privacy and charter rights concerns are addressed in this bill. Some would like us to go further. Some would like us not to have a bill whatsoever, but that is not an option for us.

• (1720)

The Chair: Thank you very much for that, MP Sodhi.

[Translation]

Mrs. DeBellefeuille, you have the floor for six minutes.

Claude DeBellefeuille: Thank you, Mr. Chair.

Thank you very much, ministers.

Mr. Fraser, I don't really have any questions for you, but I honestly want to congratulate you on your French, which has greatly improved.

Mr. Anandasangaree, the Support for Authorized Access to Information Act, enacted by part 2 of the bill, provides for a limited role for the National Security and Intelligence Review Agency, the NSIRA. However, we've noticed that there are comparable legal access mechanisms among our Five Eyes partners that come with a more formal independent oversight role. Australia is an example, where the Telecommunications and Other Legislation Amendment (Assistance and Access) Act of 2018 mandates the NSIRA's counterpart be notified of the issuance of technical assistance orders within a specified period of time.

According to Bill C-22, a year later, you have to provide the agency with an unredacted report, and, if I'm not mistaken, you have 90 days to do so. This means you're handing this report to the review agency about a year and a half after the fact or after the decisions were issued.

You've drawn inspiration from the Five Eyes for your bill, so why don't you want to give the agency a role as important as the one given by Australia to their oversight body?

Hon. Gary Anandasangaree: Thank you for the question.

[English]

I would say that there are a number of safeguards that have been built into Bill C-22. For example, on ministerial orders, there's a requirement to get acceptance from the intelligence commissioner before an order can be issued. There are provisions for judicial review in certain circumstances. There's also a reference to NSIRA *post facto*, and this is the ordinary review process—

[Translation]

Claude DeBellefeuille: I'm sorry to interrupt, but I've already read that. I came prepared.

I find the Canadian agency is somewhat sidelined and I'd like to understand why. I know the intelligence commissioner has a role, but why isn't the agency notified in real time? It's hard to conduct an investigation into whether the agencies involved, such as the RCMP or the Canadian Security Intelligence Service, are complying with the law when you get the facts almost a year and a half later.

I'm letting you know I'll be proposing an amendment so the review agency is notified in real time, similar to the Australian model, because I think that's our guarantee. It's a bit like entrusting the government by ensuring the review agency, whose primary mission is to conduct oversight, is notified in real time, like the intelligence commissioner.

I was also surprised to learn from your team that the various consultation groups organized to study Bill C-22 didn't consult Ms. Deschamps, the current agency chair. That doesn't make sense to me, honestly. We look to our Five Eyes partners for best practices, yet we fail to include an important role for the agency in Bill C-22. Would you be willing to discuss the idea of notifying the agency in real time?

[English]

Hon. Gary Anandasangaree: I would say, in part, that in order to move forward on a ministerial order, the timeline for it to go through the NSIRA review process could be quite significant, so

this is a safeguard that's built in. The role of the intelligence commissioner, as you're aware, involves a lot more real-time responses and the ability of the intelligence commissioner to give that feedback. That safeguard is there so that the intelligence commissioner could approve or not approve a proposed order—

[Translation]

Claude DeBellefeuille: What prevents you from notifying the National Security and Intelligence Review Agency? That's what I don't understand. I don't understand why you're excluding it. Its primary mission is to monitor and you're setting it aside. It's only informed a year after the fact.

I'll repeat my question. I'll propose my amendment. I know you said in the House of Commons that you'd be open to amendments. If you're going to notify the commissioner, I don't understand why it's complicated to also notify the office of the agency's chair. I think it would make sense, and that's more or less what Australia's doing. However, you don't seem open to the idea. Do you have any arguments to convince me I'm wrong to ask you for this amendment?

• (1725)

[English]

Hon. Gary Anandasangaree: First of all, I did meet with the intelligence commissioner, the Privacy Commissioner and the chair of NSIRA. I have done a number of engagements on a personal level, on top of the engagements undertaken by our departments.

We don't believe NSIRA can provide, in a timely manner, the required acceptance or rejection of a particular ministerial order, just given the urgency of the matter in some cases. This is why the intelligence commissioner is being utilized in this regard. The role of NSIRA is always as a review, as a *post facto* review agency. This legislation is in line with the way NSIRA is currently operational, which is to review matters and to report back on potential errors, potential omissions—

[Translation]

Claude DeBellefeuille: I'm going to interrupt you, Minister.

You know the agency chair disagrees with your interpretation. She told us she thinks she should be notified. She might not need to give her authorization, but she should at least be informed when there are ministerial orders, just like the commissioner. They may not have the same role, but she could at least be informed. In that sense, I think it's important for the agency to have a more important role so it can earn the public's trust. That's my opinion.

The Chair: Thank you very much, Mrs. DeBellefeuille.

Ms. Kirkland, the floor is yours for five minutes.

[English]

Rhonda Kirkland (Oshawa, CPC): Thank you, Chair.

Ministers, I appreciate your being here.

I appreciate what you say about supporting our frontline officers. Lawful access has been called for over many years. I do think, though, that we have to be careful not to rush something through. We need to get it right. We need to balance, as parliamentarians, our duty of care that we are protecting the privacy of Canadians. My questions will be based on that. I think we have to be careful not to race to royal assent. We have to do this right.

More than a decade ago—I don't know if you're aware of this—your party warned against a bill very similar to this. It was a lawful access bill. They said it risked turning Canada into a surveillance state. Today you are advancing similar powers, but actually in a more expansive form, with Bill C-22. In fact, Mr. Francis Scarpaleggia, our current Speaker of the House, was at the time the Liberal public safety critic. He warned that similar lawful access legislation, in his words, risked “creating an Orwellian service state”.

My question for you is this: Was he wrong?

Hon. Gary Anandasangaree: I will say that successive governments have failed to advance lawful access as a very important tool and framework that is required—

Rhonda Kirkland: Yes. I'm aware that it has failed to continue. My question is, has the Liberal government changed their position from what they had over a decade ago, or do you believe Mr. Scarpaleggia was incorrect at that time?

Hon. Gary Anandasangaree: I mean, this is not about Mr. Scarpaleggia, Ms. Kirkland. This is about the safety and security of Canadians. As you're aware, Canada's new government, under Prime Minister Mark Carney, undertook to ensure, as Minister Fraser aptly outlined, the three pillars. This is a very important part of that pillar.

Maybe Sean could add to this.

Rhonda Kirkland: I'm going to move on. I'll get to questions for Mr. Fraser momentarily.

Minister Anandasangaree, can you give any assurances that this legislation, as it is written, will not be used in ways that go beyond its original intent? I've heard department officials say that the bill is not intended to do X, Y and Z. However, if the bill allows the government to do those things, what is to prevent a future government, which maybe has an approach to privacy and civil liberties that's different from yours, from abusing that power?

Hon. Gary Anandasangaree: I will say that a lot of thought has been put into ensuring that the safeguards are in place, both from a privacy perspective and to ensure that it is charter-compliant. We are very confident that the bill as presented does have those safeguards.

Rhonda Kirkland: At the time, over a decade ago, when we tried this, there were warnings that rushing complex surveillance laws without properly gauging Canadians' views could lead to failure. You mentioned that you were very confident that privacy and safety are addressed in the bill as it is currently.

Your government relied on consultations led by Murray Rankin to inform Bill C-22, yet you have not released that report. Will you release Mr. Rankin's report and share it with this committee?

• (1730)

Hon. Gary Anandasangaree: I would say that Mr. Rankin's report—and I'm grateful for the work he has done—was prepared.... He is a lawyer. We are both colleagues. It was presented to me—and Mr. Fraser has used it through me—to inform our decisions.

The bill right now is not about Mr. Rankin's report. What I would say is—

Rhonda Kirkland: Sir, I just wanted to ask, is that a no, then, that you will not release the report to the committee, or yes, you will?

Hon. Gary Anandasangaree: I'm seeking privilege on that matter. I don't believe that will be released, no.

Rhonda Kirkland: Over a decade ago, the Liberal government warned that government rhetoric shut down meaningful debate on that iteration, Bill C-30's lawful access provisions, yet today this committee is being asked to study similar powers without access to the consultation report that informed how to proceed with lawful access reform in Bill C-22. That report is essential to any meaningful scrutiny and Parliament's ability to do its basic legislative function. By withholding it, your government is effectively asking MPs to approve legislation without full disclosure of the evidence behind it.

Why, sir, are you refusing to release this report, while insisting that we move forward with these powers?

Hon. Gary Anandasangaree: I would say—

Rhonda Kirkland: Why are you insisting?

Hon. Gary Anandasangaree: If I may answer, Ms. Kirkland—

Rhonda Kirkland: Thank you. I want you to just answer that question, though.

Hon. Gary Anandasangaree: You had a preamble. I should be able to give you a wholesome response.

If I may, what I would say is that, in the normal course of bringing a bill forward, there are a number of different pieces of information that a department relies on to develop the legislation and get the requisite authorities in order to bring forward legislation. The vast majority of the time, none of this information is disclosed. That is part of the decision-making of the government.

You're welcome, Ms. Kirkland—

Rhonda Kirkland: The difference between the Five Eyes and our country is that we have a charter—

The Chair: I'm sorry to interrupt both of you.

We now need to turn to MP Casey for five minutes, please.

Sean Casey (Charlottetown, Lib.): Thank you very much, Mr. Chair.

I was in Parliament the day Francis Scarpaleggia went after Vic Toews with respect to the lawful access legislation at the time, and I distinctly remember Minister Toews saying that either you're with the government or you're with the child pornographers. I remember the proliferation of the hashtag "TellVicEverything", because there was a widespread perception at the time that the legislation was an overreach. Right across the country, there were people who were providing Minister Toews with information about spilling soup on their tie, because they felt that perhaps Vic was interested in everything, with the measures he was taking to trample privacy and the over-the-top rhetoric that was being used at the time to support it.

I'd like to bring Minister Fraser into the conversation.

Minister, in your opening remarks, you talked about the protection of privacy and compliance with the charter in that regard. Can you talk a bit more about the protection of privacy and the compliance with the charter and the efforts that have been made in this legislation on the two?

Hon. Sean Fraser: Look, to help us get there, I want to provide a bit of context.

Ms. Kirkland, when she led her questions, talked about this debate going on for a few years. It hasn't been going on for just a few years; it's been going on for 30 years.

I invite everybody to watch the video of Commissioner Carrique's summary of the importance of this bill upon the legislation being tabled. You can hear the frustration coming out of law enforcement. I think there is consensus among law enforcement to move forward, because they are very tired of the criminal organizations responsible for human trafficking, auto thefts and drug trafficking. They know this activity is going on, and they are trying to do their jobs with one hand tied behind their backs. When they receive tips from foreign governments, in particular, on something as sensitive as child sexual exploitation, they want to move. They do not want to invade people's privacy along the way.

Thankfully, there have been several evolutions in Canada and around the world that demonstrate how we can better protect privacy. There's been some discussion at this committee about the differences between the approaches of our Five Eyes partners and Canada's. Of our Five Eyes partners—or France, Germany, Finland or Spain, for that matter—none require judicial authorization to get subscriber information. We're talking about information that used to be in the phone book. We would still require that a court approve access to that information. This would streamline access without compromising privacy in any significant way.

If you want to go beyond that, even in exigent circumstances.... The one exception would be when an emergency is playing out and the crime can be stopped, or if evidence is going to be destroyed. There would even be opportunity on the back end to.... The test would still have to be met, but the harm could be undone, so to speak, by a court excluding evidence, should they need to—if, in fact, there was a privacy breach committed.

We've improved this, by the way, through a consultation process with different MPs from different parties, and with experts who said, "You know, you might want to ring-fence what subscriber information you're looking for", so we excluded medical information

and legal advice. This is about finding out who is behind a phone number or an IP address when we suspect they are tied to a criminal activity of one kind or another.

At every step of the way, we've tried to give law enforcement the tools they need to combat modern crime. At every step of the way, we've said, "How are we going to do this in a manner that respects the reasonable expectation of privacy protected by the Canadian Charter of Rights and Freedoms?" I'm convinced that we found the right balance, after many years of debate and many months of discussion among parliamentarians of different parties. This strikes a balance that will allow us to defend the interests of Canadians, keep our communities safe and respect the privacy rights of Canadians at the same time.

● (1735)

Sean Casey: Minister Anandasangaree, do you have anything you'd like to build on, based on the answer you just heard?

Hon. Gary Anandasangaree: I think Minister Fraser has captured the work we've done, and the urgency.

What I want to underscore is this. As technology develops and emerges—we know we're already 30 years behind in this work—in terms of AI and other tools at a scale and speed that I don't think our world is quite ready for, the need for a lawful access framework in Canada is essential, at the very minimum, to keep us up to date and evolving.

The Chair: Thank you very much for that.

[Translation]

Mrs. DeBellefeuille, you have the floor for two and a half minutes.

Claude DeBellefeuille: Thank you very much, Mr. Chair.

Minister, you told Mr. Caputo the intent behind Bill C-22 isn't to create back doors in encryption systems, now or in the future. You've confirmed that.

The possible weakening of encryption was also a concern for us when we studied Bill C-8. At the time, Minister Joly told us that even if the bill expressed a certain intention, she would agree to add a clause clearly stating that encryption will not be weakened.

Honestly, the weakening of encryption is really a widespread fear. Perhaps you could reassure the public by making it clear in the bill that you will not undermine encryption systems.

Do you think there's room in the bill to further clarify your intention, since you told the previous speaker it wasn't your intention to weaken encryption?

[English]

Hon. Gary Anandasangaree: As I indicated, we will look at every amendment. There is an amendment-making process. Once you complete the work, there will be recommendations coming forward from the committee. The undertaking I can give you is that we will look at every single one of those proposals and give you feedback. As always, I will engage with you, Mr. Caputo and others who want to advance on this issue.

That's the commitment I can make to you today.

[Translation]

Claude DeBellefeuille: Minister, when Minister Joly appeared before the committee, she committed to having the government table an amendment to Bill C-8 to add that there would be no weakening of encryption. She said so publicly during the study on Bill C-8.

I'll ask you the same question, then. To reassure the public, are you prepared to ask your team to state in the bill that there will be no breaches of encryption systems?

• (1740)

[English]

Hon. Gary Anandasangaree: I have worked with you very closely now for almost a year, and I think you generally know the approach that I have taken in collaboration. I am certainly willing to meet with you and look at the proposal you have.

We would be more than glad to entertain anything to strengthen the bill.

[Translation]

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Lloyd, you have the floor for five minutes.

[English]

Dane Lloyd: Thank you, Mr. Chair.

Thank you to the ministers for being here.

Minister, you've refused to waive privilege on the report provided by Murray Rankin, on the consultative process in this report. I've been told that this report has been widely shared with people who have participated in the consultation. I'm assuming that those people who have not shared the report have done so because they signed a non-disclosure agreement.

Can you confirm if the members of the consultation had to sign a non-disclosure agreement in order to get access to the report?

Hon. Gary Anandasangaree: Mr. Lloyd, I'm not sure if they did or not.

The conversation today is not about Mr. Rankin's report; it is about the bill that is in front of the House. There is no precedent for governments to be sharing information that was gathered and discussions that took place with a committee. I think we're sidestepping the core issue we're here to discuss, which is the bill itself.

Dane Lloyd: Thank you. I've given you enough time on that, Minister.

This report was critical in your government's coming up with the report. It would be very helpful for us, as members of Parliament, to have access to this report. I think it's critical that governments try to build trust with Canadians. I have to admit that what you're doing here, Minister, does not look accountable or transparent, especially when we're dealing with very contentious legislation that deals with the privacy rights of Canadians.

What are you hiding, Minister? Why are you refusing to share this report?

Hon. Gary Anandasangaree: You're welcome to call Mr. Rankin to the committee, and he will be able to provide information.

What is happening right now is a bit of a distraction from the core issue, which is discussion on the bill itself.

Dane Lloyd: Minister, you're making it a distraction by refusing to reveal the report. The fact that we're talking about it today.... Even people who received the report—people who support Bill C-22 and people who are against it—are baffled as to why this report hasn't been revealed.

It's becoming a distraction because you're making it a distraction, Minister. Why not just reveal the report?

Hon. Gary Anandasangaree: The matter is not about the report, Mr. Lloyd. You know this. This is about the bill itself, as presented by me and Mr. Fraser. If you have specific questions about the bill, I will be more than willing to answer them, but I'm not willing to answer you on privileged information that I believe I sought from Mr. Rankin, which informed our decisions.

There are also a number of other individuals with whom Mr. Fraser and I met. We consult a range of people on developing a bill—

Dane Lloyd: Minister, I've given you plenty of time to respond.

Why should the stakeholders who participated, such as the Canadian Civil Liberties Association and other stakeholders, have more of a right to see what is in this report than members of Parliament, who are being asked to vote on this legislation?

Hon. Gary Anandasangaree: If you would like to invite Mr. Rankin to testify, you're more than welcome to do so.

Dane Lloyd: I'm going to move on, Minister.

I was talking to your officials before. There seems to be a contradiction. The legislation says it's not intended to weaken encryption or create systemic vulnerabilities, yet there are other parts of the legislation that say a ministerial order is intended to create the very technical capabilities needed to get through this encryption.

If one of the outcomes desired by this legislation, that being lawful access, cannot be accessed without creating systemic vulnerabilities, will your government still order telecoms and other ESPs to create these encryption capabilities?

Hon. Gary Anandasangaree: As I said initially, this bill is encryption-neutral. It does not envision or anticipate the breaking of encryption in any way. The ministerial orders, as contemplated, will require the intelligence commissioner to approve them, which is part of the safeguards that are in place right now.

Dane Lloyd: In response to my question during debate regarding compensation for providers, you were pretty blunt. You said that as a condition of CRTC licensing, you expect companies to comply without compensation.

Is that an accurate depiction of what you said in the House?

Hon. Gary Anandasangaree: What I will say is—

• (1745)

Dane Lloyd: Was it accurate, yes or no?

Hon. Gary Anandasangaree: Mr. Lloyd, I don't recall.

Dane Lloyd: Okay.

Hon. Gary Anandasangaree: I have commented on this, so I can—

Dane Lloyd: You're saying no to compensation. Is that correct? Just be clear.

Hon. Gary Anandasangaree: What I will say is that this bill... There is a world in which compensation is possible—

Dane Lloyd: Oh, okay.

Hon. Gary Anandasangaree: —but my view is that companies that are operating in Canada are good corporate citizens. Five Eyes countries do not necessarily pay—

Dane Lloyd: That's very different from the answer you gave in the House.

In what situations do you think compensation could be provided?

Hon. Gary Anandasangaree: At this point, I don't anticipate any particular situation. If there were extenuating circumstances where a company's financial position may be limiting, that would be a one-off consideration, but by and large, we do not anticipate compensation will be provided.

The Chair: Thank you, MP Lloyd.

Next is MP Acan for five minutes, please.

Sima Acan: Thank you, Mr. Chair.

I want to share some technical considerations regarding metadata for my colleagues to consider before proposing amendments that could significantly impact the effectiveness of this bill.

Modern criminal investigations, especially those involving child exploitation, human trafficking, extortion, organized crime and cybercrime, rely heavily on digital metadata to reconstruct events, identify suspects and map complex networks. These cases are often reported long after they occur, making historical data essential for establishing timelines and connections that are not immediately obvious.

It is therefore potentially risky to narrow the types of data retained. Different metadata types serve different investigative and IT functions: attribution, communication mapping and cross-platform activity reconstruction. If key categories are excluded, it can break

the chain of evidence and limit the ability to link activity across systems and jurisdictions. From an investigative and digital forensic perspective, missing metadata reduces the ability to conduct pattern and network analysis, which is central to modern intelligence-led policing and cyber investigations. It can also weaken evidentiary completeness in court. Many serious crimes are reported long after they occur. If certain metadata categories were never stored in the first place, they cannot be recovered later, even with a warrant or a court order.

Mr. Chair, I ask my colleagues to please refer to this transcript of my remarks when considering any amendments related to narrowing the types of metadata or limiting the retention periods, as these changes could significantly weaken the effectiveness of lawful access.

My colleague Mr. Caputo raised concerns regarding not only the types of metadata but also the 12-month data retention framework outlined in part 2.

During my meetings with law enforcement officials, they clarified the general parameters. There remains a practical challenge when it comes to complex investigations. Many serious cases, such as child exploitation, human trafficking, organized crime and extortion, are inherently time-intensive and often extend well beyond six or even nine months due to their cross-jurisdictional and digital nature.

Could CSIS or the RCMP elaborate on the operational importance of data retention in supporting these types of complex investigations? Also, significantly, how does the availability and duration of retained data impact the ability of law enforcement to conduct timely and effective investigations in the digital context?

Thank you.

Nicole Giles (Deputy Director, Canadian Security Intelligence Service): The ministers are gesturing to me, so I'll take that as my cue.

I can give two examples, perhaps. One example could be that CSIS is trying to determine the movements of a terrorist group, and we've received a warrant to track a person of interest's cellphone. The electronic service provider did not have the necessary capabilities to track the device, so we're out of luck if there are not the capabilities to track the device. That is one of the key capabilities that would be provided under part 2, because it would require ESPs to develop and maintain location tracking capabilities, which are, quite frankly, standard in Five Eyes and European countries.

Another example could be that we receive information from a foreign partner who is carrying out an investigation outside of Canada where a few of the subjects of the investigation are associated with a Canadian phone number, and the foreign partner has further highlighted that the threat looks like it's about to move into Canada. We're able to confirm that the phone numbers were obtained through a reseller, but the reseller, quite frequently, neither maintains records of its sales nor tracks its clients' activities. Part 2 would bring that into play by having the resellers brought into the process, which would allow us to respond to those types of requests.

• (1750)

Sima Acan: Do I still have time?

The Chair: You have 30 seconds.

Sima Acan: Okay.

Bill C-22 makes an important legislative change clarifying that....

Actually, it's not going to be enough, Mr. Chair. I'm okay with that.

Hon. Sean Fraser: Mr. Chair, if there are 20 seconds left—

Sima Acan: Minister, do you want to add something?

Hon. Sean Fraser: If I can just add, these are not fictional crimes. If you actually talk to law enforcement officials, particularly on the second example.... A lot of people don't appreciate this, but law enforcement in Canada is receiving an ungodly number of tips about potential threats, including child sexual exploitation. The application of the law is inconsistent between provinces, because it's unclear about the regime of how we actually use digital evidence to investigate and prevent crime.

These are real threats to—

The Chair: I'm sorry to have to cut off a ministerial colleague, but it's over, unfortunately.

[*Translation*]

Thank you to the ministers for taking the time to prepare and travel to join us today.

Thank you to all the officials for doing the needed work.

We will now adjourn, and we'll see you on Thursday for other business.

1400

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>

Tab B

1404



THE CANADIAN
BAR ASSOCIATION
L'ASSOCIATION DU
BARREAU CANADIEN

Bill C-22 (*Lawful Access Act, 2026*)

**CANADIAN BAR ASSOCIATION
CRIMINAL JUSTICE, PRIVACY AND ACCESS TO INFORMATION LAW SECTIONS AND
ANTI-CORRUPTION TEAM**

May 2026

PREFACE

The Canadian Bar Association is a national association representing 40,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Criminal Justice, Privacy and Access to Information Law Sections and Anti-Corruption Team, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Policy Committee and approved as a public statement of the CBA Criminal Justice, Privacy and Access to Information Law Sections and Anti-Corruption Team.

TABLE OF CONTENTS

Bill C-22 (*Lawful Access Act, 2026*)

I. EXECUTIVE SUMMARY 1

II. GENERAL CONCERNS.....2

III. LAWFUL ACCESS OVERVIEW 2

 A. Absence of evidence of necessity 2

 B. Expanding the scope of lawful access powers..... 3

 C. Lack of safeguards..... 3

 D. *Charter* compliance 3

IV. PART 1 - TIMELY ACCESS TO DATA AND INFORMATION 4

 A. New Confirmation of Service Demand 4

 Insufficient Minimum Timeframe to Comply with Confirmation of Service Demand 4

 Timeframe for Non-Disclosure 4

 Revocation or Variation of Demand 4

 B. New Production Order for “Subscriber Information” 4

 C. New Judicial Authorization for Requests of Transmission Data or Subscriber Information from a Foreign Entity 5

 D. Insufficient timeframes to seek review of orders 6

 E. Voluntary disclosure and immunity 6

 F. “Public” Information 7

 G. Exigent Circumstances 7

 H. Examination of Computer Data: Retention and Destruction 7

 I. Amendments to the Canadian Security Intelligence Service Act 8

V.	PART 2 – SUPPORTING AUTHORIZED ACCESS TO INFORMATION ACT	8
A.	General	8
B.	Definitions and scope (s.2)	9
C.	Core Providers and Ministerial Orders (ss.5-13).....	9
	s. 5(2)(a) – Capabilities	10
	s. 5(2)(c) – Notices to the Minister or other persons	10
	s. 5(2)(d) – Retention of categories of metadata	10
D.	Ministerial orders	11
E.	Systemic Vulnerability (ss. 5(3) and 7(4))	11
F.	Government should accept the risk that it is proposing to create	12
G.	Obligation to Assist	13
H.	Judicial Review	13
I.	Mandatory confidentiality	13
J.	Inspection powers	14
K.	Audits (s.21)	14
VI.	PRIOR CBA RECOMMENDATIONS	14
A.	Codify Purpose Limitation and Data Minimization Principles	14
B.	Ensure Cross-Statute Consistency with Privacy Laws.....	15
C.	Mandate Independent Oversight and Reporting	15
D.	Require Transparent Regulation-Making Process	15
VII.	CONCLUSION.....	15

Bill C-22 (*Lawful Access Act, 2026*)

I. EXECUTIVE SUMMARY

The Canadian Bar Association (CBA) Sections appreciate the opportunity to comment on Bill C-22 (*Lawful Access Act, 2026*). We also appreciate the good faith shown by the Ministers who shelved the previous iteration (part 14 and Part 15 of Bill C-2, the *Strong Borders Act*), for further stakeholders' consultations. The process improved the Bill, but the CBA has significant concerns.

The Bill creates new law enforcement and national security authorities in Part 1 and requires electronic service providers to create new capabilities in Part 2. Part 1 was authored by the Department of Justice and Part 2 was authored by the Department of Public Safety. While both are under the banner of "lawful access", they are distinct enough that separate bills would improve debate and discussion.

With respect to Part 1, "Timely Access to Data and Information", we are concerned about the balance between the threshold for obtaining subscriber information in light of the scope of data that is included in the definition (services and devices).. With respect to Part 2, which creates a new "Supporting Authorized Access to Information Act", our concerns are manifold.

The Government claims Canada is the only "Five Eyes" country without a "lawful access" law, which is only partly true. With respect to Part 1 of the Bill, Canada has long had modern tools for law enforcement and Canadian Security Intelligence Service to intercept communications, search premises and computers, and compel customer information from service providers. Canada lacks a comprehensive framework requiring service providers to be "intercept ready". Other countries' actions, especially those intrusive into personal privacy, are insufficient justification. Three of the Five Eyes countries do not have constitutionally protected rights to privacy or freedom from unreasonable search and seizure. The United Kingdom, Australia and New Zealand lack constitutional guardrails, allowing more latitude to enact intrusive surveillance laws. For Canada, s. 8 of the *Charter* must be front of mind.

II. GENERAL CONCERNS

The CBA opposes legislative practices that diminish debate and stakeholder engagement. In Resolutions 13-04-M¹ and 25-03-A², it urged limiting omnibus legislation to minor technical amendments. Bill C-22 instead enacts two different regimes under “lawful access”: Part 1’s changes to the *Criminal Code*³ [hereinafter “the *Code*”] and Canadian Security Intelligence Service Act [hereinafter “the *CSIS Act*”]⁴ and Part 2’s broad new framework. These should be separated to allow proper attention from the public and Parliamentarians.

The government must avoid deferring core definitions and obligations to future regulations. Legislation expanding government powers must be clear to ensure legal predictability and prevent function creep.

III. LAWFUL ACCESS OVERVIEW

Bill C-22 proposes to amend existing lawful access powers in the *Code* and the *CSIS Act*, requiring service providers to enable lawful access requests. Before discussing specific provisions, the CBA Sections will highlight overarching concerns.

A. Absence of evidence of necessity

Bill C-22 expands lawful access powers while reducing judicial oversight, materially impacting individual rights and freedoms and imposing costs on the private sector. Such changes require strong evidence of necessity and a proportionate impact on rights. The government has not provided evidence that these changes are necessary.

In briefings on Bill C-2 and Bill C-22, officials cited the elapsed time, technological advances, the expansion of digital service providers, the outdated Solicitor General’s Enforcement Standards for Lawful Interception of Telecommunications, and Canada’s lack of enhanced lawful access legislation compared with other Five Eyes countries. The government has not cited investigations that are actually hindered by current provisions or technical limits that prevent service providers from satisfying lawful access orders. Both the *CSIS Act*⁵ and the *Code*⁶ provide for “assistance

¹ CBA Resolution 13-04-M, Omnibus Bills, [online](#).

² CBA Resolution 25-03-A, Debate and Consultation in Multipart Legislation, [online](#).

³ Criminal Code, RSC 1985, c C-46 [the *Code*].

⁴ *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*].

⁵ *CSIS Canadian Security Intelligence Service Act*, RSC 1985, c C-23, s 22.3;

⁶ Criminal Code, RSC 1985, c C-46, s 487.02.

orders”, with judicial oversight for technical capabilities. Without evidence of necessity, these changes should not be implemented.

B. Expanding the scope of lawful access powers

Bill C-22 significantly expands lawful access: more parties could demand access, more information could be compelled, technical capacity requirements are broadened, and more entities would be subject to them, while judicial discretion is reduced. This expansion lacks adequate consultation with key stakeholders on its impact, feasibility and proportionality. We note that the consultations between Bill C-2 and Bill C-22 focused on “fixing” Bill C-2 rather than on necessity and proportionality.

C. Lack of safeguards

Part 1 of Bill C-22 reduces judicial oversight. Confirmation of Service Demand powers do not require prior judicial authorization, and officers may impose a non-disclosure for up to a year. Where judicial oversight exists, the threshold is low (i.e., reasonable grounds to suspect). Part 2 requires service providers to support state surveillance with minimal safeguards, no effective proportionality test, limited appeal, and non-disclosure, and allows orders without compensation, shifting costs from Law Enforcement Agencies (LEAs) to the private sector, effectively deputizing businesses as state agents.

Involving the Intelligence Commissioner in the approval of Ministerial Orders in Part 2 is an improvement over Bill C-2, but the combination of expanded powers, limited transparency, and limited safeguards creates serious risks to individual rights and freedoms.

D. Charter compliance

The CBA Sections believe Parts 1 and 2 of Bill C-22 risk violating the s. 8 *Charter* protection against unreasonable search and seizure. In particular, the scope of “subscriber information” may include information that s. 8 of the *Charter* would require a showing of more than reasonable suspicion. In addition, the provisions in Part 1 related to voluntary disclosures appear misaligned with the Supreme Court rulings in *R. v. Spencer* and *R. v. Bykovets*.⁷

⁷ *R. v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212; *R. v. Bykovets*, 2024 SCC 6

IV. PART 1 - TIMELY ACCESS TO DATA AND INFORMATION

A. New Confirmation of Service Demand

Part 1 introduces s. 487.0121 of the *Code*, allowing a “peace officer or public officer”, without judicial authorization, to demand that a telecommunications service provider confirm “whether or not they provide or have provided telecommunication services to any subscriber or client, or to any account or identifier, specified in the demand.”

Insufficient Minimum Timeframe to Comply with Confirmation of Service Demand

The new section 487.0121(5) mandates a 24-hour time response time. The CBA suggests increasing this to 48 or 72 hours, except where there are “exigent circumstances”, as 24 hours might be unrealistic for smaller providers.

Timeframe for Non-Disclosure

The new section 487.0121(5) also permits officers to prohibit disclosure of the demand for a period of up to a year.⁸ The CBA is of the view that this is excessive and recommends reducing it to 90 days, with a court approval required for extensions. Because confirmation of service can precede the production order, the non-disclosure powers related to it should also be tightly time-limited.

Revocation or Variation of Demand

Bill C-22 introduces s. 487.0121(11) of the *Code*, allowing a judge to revoke or vary a demand. The CBA Sections submit that a judge should be able to revoke a demand if, in the totality of the circumstances, the demand is an unreasonable invasion of the privacy of the person(s) involved, where the issuing officer cannot meet the threshold, or where compliance would cause non-Canadian residents to violate foreign law.

B. New Production Order for “Subscriber Information”

Part 1 of the Bill creates a “production order for subscriber information,” requiring judicial authorization based on mere suspicion that (a) an offence has been or will be committed under the *Code* or any other Act of Parliament; and (b) the subscriber information is in the person’s possession or control and will assist in the investigation of the offence. “Reasonable grounds to suspect” is the lowest threshold in our legal system.

⁸ Section 158 of the Bill

Unlike General Production Orders, which specify data being sought, this order compels “all the subscriber information” in the recipient’s possession. The definition “subscriber information” in Bill C-2 goes beyond general production orders connecting an identifier with a suspect, touching the “biographical core” protected by s. 8 of the *Charter*,⁹ revealing “intimate details of the lifestyle and personal choices of the individual”.¹⁰

The definition of “subscriber information”, as presently worded in the proposed amendment to s. 487.011 of the *Code*, raises concerns that the information captured under this definition may go to the “biographical core”. Orders may target any type of service provider such as hotels, health clinics, where the “types of services provided” and devices used (e.g. medical devices, networking equipment) can reveal highly personal and sensitive information.

The CBA Sections submit the definition of “subscriber information”, as set out in s. 4 of the Bill, should be limited to information that identifies the subscriber or the client. If “devices” remain in the definition, it should be limited to devices that primarily facilitate communication. Any information beyond that, based on mere suspicion, risks violating s. 8 of the *Charter*.

C. New Judicial Authorization for Requests of Transmission Data or Subscriber Information from a Foreign Entity

Proposed new s. 487.0181 of the *Code* authorizes a “request” (not an order) directed at a “foreign entity that provides telecommunications service to the public.” The request is approved by a judge on an application by a peace officer or a public officer. The threshold for issuing such a request mirrors the low threshold for the new subscriber production order (reasonable suspicion).

Subject to the same concerns expressed with respect to the new production order for subscriber information (threshold and scope), we are of the view that this section creatively attempts to address the uncertainty of serving Canadian production orders on entities domiciled wholly outside of Canada, relying on the voluntary cooperation of foreign entities, but it raises similar concerns about a low threshold and privacy.

⁹ *R. v. Plant*, 1993 CanLII 70 (SCC), at pg. 293: “to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state”.

¹⁰ *R. v. Bykovets*, *supra*, 2024 SCC 6, at para. 51, citing *R. v. Plant*, 1993 CanLII 70 (SCC), at pg. 293; *R. v. Spencer*, *supra*, at para. 27

D. Insufficient timeframes to seek review of orders

Bill C-22 shortens the window of opportunity for recipients of a production order or information demand to apply to the Court to have it varied or revoked. The amended s. 487.0193 of the *Code* applies to all production orders and reduces the review timeframe to ten business days after receiving the order (from previously generally 30). This timeframe is too short, particularly because decisions to challenge a production order require internal escalation, and many service providers may lack on-call legal counsel. It also limits engagement with the issuing officer or prosecutor to avoid a court application. This change should be removed from the Bill. The ability of a recipient to seek review of a production order should only expire with the deadline imposed by the judge to produce the materials. If advance notice to the officer is retained, email notice should suffice and pause the timeframe to allow time for filing application materials.

E. Voluntary disclosure and immunity

A significant concern of the CBA Sections is that no information demand is necessary for a peace officer or public officer to “ask” for information if the person is lawfully in possession of the information. The proposed legislation then goes on to provide that: “no production order or warrant, or information demand made under s. 487.0121, is necessary for a peace officer or public officer to receive any information from a person who is lawfully in possession of it and to act on the information if the person provides it voluntarily or is required by law, including a law of a foreign state, to provide it.”¹¹

While the CBA Sections appreciate that the stated intent of the proposed new s. 487.0195(3) may be to clarify that police may act on passive, unsolicited receipt of “tips” (e.g. from the National Center for Missing and Exploited Children or Crime Stoppers), it also creates a framework for routine, informal voluntary requests that may reach the “biographical core”. The purported grant of immunity effectively destroys the privacy interests inherent in the requested information. It is also unclear how voluntary provision of information may be requested, and it may be easy for a company to confuse a “demand” with a “request” for voluntary provision of the material, which creates a muddy framework. Essentially, this bypasses judicial control in circumstances where a compelling privacy interest may exist.

This section should be narrowed to provide that police may collect and use information that is (a) provided to law enforcement or government on a person’s or an organization’s own initiative,

¹¹ Section 164 of the Bill: the new s. 487.0195(3) of the *Code*

without being asked, or (b) information that is reported to the police or other authority pursuant to a legal obligation (such as mandatory reporting of child sexual abuse and exploitation material).

F. “Public” Information

The new s. 487.0195(4) of the *Code* suggests that police or public officers may use information that is “available to the public”, assuming no privacy expectation. Law enforcement in the U.S. have bypassed the Bill of Rights by purchasing geolocation information from data brokers and participants in the online advertising ecosystem. One might characterize this information as being “available to the public”, and police should not be able bypass the *Charter* by using data brokers.¹² In addition, the dark web is replete with “leak sites” where hackers disclose and sell information that has been unlawfully purloined from third parties. This illegally sourced information would be “available to the public.” This section should be limited to information that is already lawfully available to the public and for which an individual no longer has any reasonable expectation of privacy.

G. Exigent Circumstances

Clause 167 of the Bill would replace s. 487.11 of the *Code*, allowing law enforcement to seize subscriber information or transmission and tracking data without an order where conditions for obtaining such information and data exist under the proposed applicable provisions, but by reason of exigent circumstances would be impracticable. Any such demand should include enough information for the service provider to be satisfied that exigent circumstances exist, especially where foreign laws related to emergency requests may apply.

H. Examination of Computer Data: Retention and Destruction

Section 156 of the Bill modernizes the language of s. 487 of the *Code* to incorporate the examination of computer data. Sections 170 & 171 would exempt “computer data” from sections 489.1 (“Restitution of thing or report”) and 490.81 (“Management order”) of the *Code*, raising concerns that law enforcement could retain it indefinitely. The CBA Sections recommend a provision mandating the destruction of seized data after a set time (e.g. one year), unless an extension is authorized by the court. Alternatively, the CBA Sections suggest amending warrant conditions¹³ to data retention timeframes, after which data must be destroyed unless extended.

¹² Wolfie Christl, Astrid Perry, Luis Fernando Garcia, Siena Anstis, and Ron Deibert. “Uncovering Webloc: An Analysis of Penlink’s Ad-based Geolocation Surveillance Tech,” Citizen Lab Report No. 191, University of Toronto, April 9, 2026, [online](#). and Lena Cohen, Hudson Hongo. “The Government Uses Targeted Advertising to Track Your Location. Here’s What We Need to Do.” (Electronic Frontier Foundation, March 5, 2026) [online](#).

¹³ Section 156(3) of the Bill: the proposed new s. 487(2.4) of the *Code*.

While prolonged examination may be helpful to complex and long-term investigations (e.g. ongoing criminal organization offences, homicides, sexual assault “cold cases”, etc.), indefinite retention and open-ended use is unacceptable. The CBA Sections note that the *Code* already includes destruction provisions of computer data in the context of “preservation demands” (see s. 487.0194 of the *Code*).

I. Amendments to the Canadian Security Intelligence Service Act

The same concerns raised about the proposed amendments to the *Code* apply, more acutely, to the complementary amendments to the *CSIS Act*.¹⁴ In criminal law proceedings, once a person is charged, they have the ability to have a judge scrutinize the state action in the context of a trial. *Charter* remedies are available at trial when officers fail to perform their obligations with respect to intrusive state powers. By contrast, activities undertaken by the Canadian Security Intelligence Service usually remain unknown to affected individuals and rarely face ex post facto judicial oversight. Any increase in CSIS lawful access should always be subject to judicial oversight and judicial control.

V. PART 2 – SUPPORTING AUTHORIZED ACCESS TO INFORMATION ACT

A. General

The CBA Sections are concerned that Part 2 of Bill C-22, creating the *Supporting Authorized Access to Information Act* (SAAIA), has not been justified by the government as being necessary or proportional. It mandates “electronic service providers” to build backdoors for law enforcement access to data, which may attract hackers, undermining public safety.

Part 2 of Bill C-8, the *Critical Cyber Systems Protection Act* (CCSPA), allows regulators to order “designated operators” of critical systems to take “any [necessary] measure”,¹⁵ potentially including backdoor vulnerabilities, confusing compliance obligations with lawful access and cyber systems regimes.

Obligations on “core providers” and the contents of Minister Orders should be limited so that they cannot dictate (i) any changes to products or services that an ESP provides in the ordinary course of business, (ii) the collection and retention of any data beyond what the ESP requires for its own

¹⁴ *CSIS Act*, RSC 1985, c C-23.

¹⁵ Part 2, s. 36(1)(b) of the *Critical Cyber Systems Protection Act*.

purposes, and (iii) any changes that would affect the functionality (including ordering additional functionality) for any products or services offered by the ESP.

B. Definitions and scope (s.2)

The scope of application of Bill C-2, Part 2 is based on the definition of “electronic service” and “electronic service provider”. The power to require lawful access technical capacity applies to electronic service providers (ESP). The broad definitions of “Electronic Service” and “Electronic Service Provider” could include a much wider range of entities that have digital operations, including retail operations, academic institutions, health care facilities, lawyers’ offices and media outlets. It would be almost impossible to find a business in Canada that does not create, store or transmit information in electronic form.

The CBA Sections are concerned that the government could impose lawful access technical capacities for all aspects of digital life. The definition of electronic service provider should be strictly limited to those who principally provide communication services to the public.

C. Core Providers and Ministerial Orders (ss.5-13)

These sections empower the government to require ESPs to develop, test, implement, operate and monitor lawful access technical capabilities to provide access to information in relation to their electronic services. Section 5 empowers the Governor-in-Council (GiC) to make regulations establishing lawful access technical capabilities for “core providers” a subset of ESP that is defined by the GiC in subsequent regulations. The CBA Sections are concerned by the absence of procedural safeguards for this new and far-reaching power. Section 5 has no obligation to consult or a proportionality test. While section 5(3) lists factors to consider, transparency about their consideration is not required.

An ESP can apply for a temporary exemption, but otherwise, there is no oversight or review process other than judicial review. Any power to impose lawful access technical capabilities should be accompanied by proportionate procedural safeguards.

Section 5 also lacks a process to compensate for costs arising from imposing lawful access technical capabilities. If an ESP lacks a particular capability, it is typically because it has no legitimate business need for it. As a result, lawful access technical capabilities required under s. 5 are capabilities and costs that will generally only be incurred to facilitate lawful access to information. This represents a transfer of investigative costs that traditionally rest with LEAs to

ESPs in the private sector. The CBA Sections are concerned about the impact on ESPs and increased lawful access activity if LEAs ignore costs of their activities.

s. 5(2)(a) – Capabilities

By requiring providers to build and maintain interceptions or data production capabilities, the Bill mandates the existence of a privileged access point within otherwise secure systems. The term broadness creates ambiguity in required technical architecture: compliance uncertainty for smaller providers, excessive regulatory discretion and complex compliance assessment.

While the government has said that Bill C-22 does not permit backdoors, a plain reading of s. 5(2)(a) and the lack of guardrails says otherwise.

s. 5(2)(b) – Devices and equipment

SAAIA should not permit the government, via regulation or Ministerial Order, to require the installation of specific equipment or devices on providers' systems. Diligent companies must have full awareness and control of any equipment or devices associated with its infrastructure. An open-ended obligation to install equipment for surveillance is unreasonable and introduces significant cybersecurity risks for ESPs.

s. 5(2)(c) – Notices to the Minister or other persons

GiC regulations and Ministerial Orders may require ESPs to give notice to the Minister or other person about capabilities and any device, equipment or other thing. The CBA is concerned that this mirrors the powers contained in the UK's lawful access law (the *Investigatory Powers Act 2016* (IPA), significantly expanded by the *Investigatory Powers (Amendment) Act 2024*.

It is entirely lawful, and should remain so, for a company to make changes to its systems that both (a) increase the security of its users' information, and (b) reduce the ability of the company to provide access to user information. Many of the most popular messaging apps in the world have introduced "end to end encryption", which increases the security of user data and means that law enforcement no longer has access to text messages from the service provider.

s. 5(2)(d) – Retention of categories of metadata

Bill C-22, unlike C-2, allows core providers and ESPs subject to ministerial orders to retain metadata for up to one year. Section 5(4) limits data retained, but metadata includes very sensitive information, such as location data. This is a dramatic expansion from Bill C-2.

In Europe, mandatory metadata retention was deemed a privacy rights intrusion when the European Court of Justice struck down the EU *Data Retention Directive* in 2014,¹⁶ holding that the general and indiscriminate retention of all users' telecommunications metadata was a disproportionate interference with privacy and data protection rights. The Directive required member states to mandate retention for between six and twenty-four months. In the years since, the CJEU has progressively clarified that while targeted retention linked to specific threats or geographic areas can be lawful, blanket retention of all users' data remains incompatible with EU fundamental rights. This will likely be challenged as a violation of s. 8 of the *Charter*.

D. Ministerial orders

Section 7 empowers the Minister of Public Safety and Emergency Preparedness to issue Ministerial Orders imposing obligations on ESPs, similar to the GiC regulations, with some procedural safeguards. These include considering the impact on justice administration, the feasibility for ESPs, and the impact on service users. Intelligence Commissioner approval is required, but affected ESPs have no right to make representations, and there is no transparency about the factors considered. This lack of criteria and meaningful and proportionate procedural safeguards is a significant concern for the CBA Sections.

Currently, the police and CSIS can apply to a judge for an "assistance order" requiring service provider assistance for a warrant, potentially with a non-disclosure order. These orders are tailored to the particular warrant, the provider and the nature of the assistance required. The judge would consider the impact of the *Charter* in the issuance of the assistance order. A judge under both the *Code* and the *CSIS Act* is able to have an amicus appointed to consider the impact of the order on third parties. Assistance orders are, by definition, subject to judicial supervision and control. This is effectively being replaced by Ministerial Orders with no judicial oversight.

The CBA notes that there is no evidence that assistance orders under the *Code* or *CSIS Act* are inadequate and recommends that Ministerial Orders should be removed from the Bill.

E. Systemic Vulnerability (ss. 5(3) and 7(4))

Both GiC regulations and Ministerial Orders state a provider can bypass a provision if complying would "introduce a systemic vulnerability in electronic protections related to that service or prevent the provider from rectifying such a vulnerability." Despite government claims not to undermine encryption, similar laws in other jurisdictions have been used to undermine

¹⁶ EU Data Retention Directive, [online](#).

encryption, as reportedly occurred with Apple under the UK regime.¹⁷ This should not be permitted in Canada.

The definition of systemic vulnerability in the Bill is insufficient to meaningfully constrain risk. The current definition only addresses unauthorized third-party access, not data integrity, availability, or limits vulnerabilities related to a device, software or operating system. "Systemic vulnerabilities" should make it clear that an obligation to undermine or circumvent encryption is prohibited, and it should be clear that vulnerabilities are not just related to unauthorized access, and not just related to "services". Specifically, the CBA proposes the following definition of "systemic vulnerability":

systemic vulnerability means a vulnerability in electronic protections that creates a substantial risk to the confidentiality, integrity, or availability of information, services or systems.

And amend paragraphs 5(5) and 7(5) to clearly carve out encryption:

(5) A [core provider/ electronic service provider] is not required to comply with a provision of [a regulation made under subsection (2)/an order], with respect to an electronic service, if compliance with that provision would require the provider to introduce a systemic vulnerability related to that service, or prevent the provider from rectifying such a vulnerability, or require the provider to remove, circumvent or undermine the encryption of information.

F. Government should accept the risk that it is proposing to create

By mandating backdoors and expanded data retention, SAAIA would create valuable targets for malicious actors. The *Communications Assistance to Law Enforcement Act* in the U.S. required similar backdoors, exploited by foreign hackers to obtain U.S. data.¹⁸ Canada faces the same risk if it imposes similar requirements.

Retaining metadata conflicts Canadian privacy laws, which limits retention to necessary and reasonable business purposes. Metadata under SAAIA lacks business purpose, risking privacy laws and best practices violations and attracting cyber criminals.

Overall, the regime should specify the factors, eligible costs, and guidance for calculating compensation. Many ESP capital expenditures under Part 2 will serve no business purpose and will be solely for lawful access. If these costs benefit society, they should be covered by

¹⁷ The Guardian, UK government resumes row with Apple by demanding access to British users' data, (1 October 2025) [online](#).

¹⁸ Wall Street Journal, "U.S. Wiretap Systems Targeted in China-Linked Hack: AT&T and Verizon are among the broadband providers that were breached" (5 October 2024) [online](#).

government revenues rather than imposed on certain ESPs. In addition, SAAIA should compensate to ESPs and affected individuals for losses associated to compliance, including data breaches from government-mandated backdoors.

G. Obligation to Assist

Section 14 grants numerous national security individuals the authority to request information from ESPs. Allowing anyone – civilian or otherwise – within agencies such as the RCMP and CSIS to request information under Part 2 is excessive. The scope and the types of information that can be requested under such a disclosure obligation should be narrowed.

H. Judicial Review

Sections 16 and 17 lack accountability and rule of law. Section 16 minimizes ESPs' right to challenge orders by imposing a 15-day advance notice of application for judicial review to be attached to a formal letter to the Minister. Section 16 lacks a clear right to challenge the government.

I. Mandatory confidentiality

The confidentiality outlined in s. 15 of SAAIA are overbroad and unjustified. Every ESP under a Ministerial Order is prohibited from disclosing to anyone order's existence. Companies should be transparent about their products, unless there is a clear law enforcement or national security imperative.

Experience in the UK shows a similar law to secretly require Apple to remove encryption on certain of its core/key products. US companies should be able to seek the US government's assistance in resolving problematic orders. The Minister should justify, on a per-order basis, the need for secrecy associated with these orders, and any confidentiality requirements should sunset. These orders should be subject to judicial review, where the Minister would have the onus of satisfying the court that the secrecy order is reasonably necessary in order to protect public safety or national security. Non-Canadian companies, particularly from a "Five Eyes" country, should disclose orders to their home jurisdiction counterpart.

Section 18 suggests further confidentiality rules that could limit information sharing, potentially affecting ESP's security clearance programs. The anticipated government overreach in these sections is unreasonable and suggests excessive regulatory control. Judicial review should not be so blocked and advance notice along with section 17, which adds ambiguity to limit disclosure of access requests, should be removed.

J. Inspection powers

Sections 19-21 echo the intrusive investigative powers of the CCSPA (Bill C-8) affording Minister and designated persons with powers of entry - from “examining anything” on-site to removing “any document, record or cyber system, or a portion of it” for the purpose of reviewing or copying it.¹⁹

These powers – and sections – enable warrantless investigations for ESPs, allowing examination and copying of documents, with an obligation to assist. A threshold of reasonable and probable grounds should be required before entry, balancing the broad powers and lack of liability during investigations. Inspections should (a) require notice to the ESPs, (b) be carried out during ordinary business hours, (c) inspectors should have to satisfy the ESP’s reasonable security and operational requirements and (d) they should be carried out in a manner designed to minimize impacts on the ESP’s operations.

K. Audits (s.21)

To verify SAAIA compliance, designated person may order internal audit by ESPs. The ESP must comply without independent review or oversight and no assurance of confidentiality for the resulting report, including any personal information it contains. The CBA Sections believe that further procedural safeguards are required for this audit power, including an independent review of the Audit order and handling of information.

VI. PRIOR CBA RECOMMENDATIONS

A. Codify Purpose Limitation and Data Minimization Principles

The CBA Sections recommend any use of information collected by law enforcement or national security authorities be limited to specific, statutorily defined purposes connected with the purposes for which was collected, with explicit prohibitions on secondary use beyond the initial authorization. For example, computer data retained by the government pursuant to Part 1 of the Bill should not be used for any other purpose except to advance the investigation for which the data was initially seized. Data collection and retention must be proportional and necessary to a legitimate governmental objective²⁰.

¹⁹ See, for example, CCSPA, ss. 49-50.

²⁰ Reference: OBA Submission on Privacy Guidance on facial Recognition for Police Agencies (15 October 2021)

B. Ensure Cross-Statute Consistency with Privacy Laws

The new Act should not override privacy rights or accountability mechanisms in other statutes. The CBA Sections recommend legislative language affirming that existing privacy protections under federal and provincial legislation remain fully applicable²¹.

C. Mandate Independent Oversight and Reporting

The CBA supports annual public reporting obligations to Parliament and an oversight mechanism such as the Privacy Commissioner, the National Security and Intelligence Review agency, or another designated tribunal, to audit compliance, review complaints, and investigate overreach or misuse.

D. Require Transparent Regulation-Making Process

The Act delegates significant authority to future regulations; therefore, the CBA Sections recommend public and stakeholder consultation, particularly from privacy, legal, and civil liberties organizations.

VII. CONCLUSION

Bill C-22 has significant implications that affect Canadians' privacy, safety and cybersecurity interests. The recommendations put forward by the CBA are intended to be a good faith contribution to Parliament's important deliberations in crafting laws that are effective, understandable and consistent with the *Charter*.

²¹ CBA Resolution 15-04-M: Independent Oversight of Canada Border Services Agency (February 21-22, 2015); CBA Submission on Security of Canada Information Sharing Act (SCISA) (January 2017)

Tab C

First Session, Forty-fifth Parliament,
3-4 Charles III, 2025-2026

Première session, quarante-cinquième législature,
3-4 Charles III, 2025-2026

HOUSE OF COMMONS OF CANADA

CHAMBRE DES COMMUNES DU CANADA

BILL C-22

PROJET DE LOI C-22

An Act respecting lawful access

Loi concernant l'accès légal

FIRST READING, MARCH 12, 2026

PREMIÈRE LECTURE LE 12 MARS 2026

MINISTER OF PUBLIC SAFETY

MINISTRE DE LA SÉCURITÉ PUBLIQUE

RECOMMENDATION

Her Excellency the Governor General recommends to the House of Commons the appropriation of public revenue under the circumstances, in the manner and for the purposes set out in a measure entitled “*An Act respecting lawful access*”.

SUMMARY

Part 1 amends various Acts to modernize certain provisions respecting the timely gathering and production of data and information during an investigation. It, among other things,

- (a) amends the *Criminal Code* to, among other things,
 - (i) facilitate access to basic information that will assist in the investigation of federal offences through confirmation of service demands given to telecommunications service providers or judicial production orders for the production of subscriber information,
 - (ii) expedite the response to production orders by shortening the review process and clarify the ability of peace officers and public officers to receive and act on certain information that is voluntarily provided to them and to obtain and act on information that is publicly available,
 - (iii) specify certain circumstances in which peace officers and public officers may obtain evidence, including subscriber information, in exigent circumstances,
 - (iv) allow a justice or judge to authorize, in a warrant, a peace officer or public officer to obtain tracking data or transmission data that relates to any thing that is similar to a thing in relation to which data is authorized to be obtained under the warrant and that is unknown at the time the warrant is issued,
 - (v) provide and clarify authorities by which computer data may be examined, and
 - (vi) allow a justice or judge to authorize a peace officer or public officer to make a request to a foreign entity that provides telecommunications services — or that provides services by a means of telecommunication — to the public to produce transmission data or subscriber information that is in its possession or control;
- (b) makes a consequential amendment to the *Foreign Publishers Advertising Services Act*;
- (c) amends the *Mutual Legal Assistance in Criminal Matters Act* to allow the Minister of Justice to authorize a competent authority to make arrangements for the enforcement of a decision made by an authority of a state or entity that is empowered to compel the production of transmission data or subscriber information that is in the possession or control of a person in Canada;
- (d) amends the *Canadian Security Intelligence Service Act* to, among other things,

Available on the House of Commons website at the following address:
www.ourcommons.ca

RECOMMANDATION

Son Excellence la gouverneure générale recommande à la Chambre des communes l'affectation de deniers publics dans les circonstances, de la manière et aux fins prévues dans une mesure intitulée « *Loi concernant l'accès légal* ».

SOMMAIRE

La partie 1 modifie diverses lois afin de moderniser certaines dispositions relatives à la collecte et à la communication de données et de renseignements en temps opportun lors d'une enquête. Notamment, elle :

- a) modifie le *Code criminel* pour, notamment :
 - (i) faciliter l'accès aux renseignements de base qui seront utiles à l'enquête relative à des infractions fédérales au moyen d'ordres de confirmer la fourniture de services donnés à des fournisseurs de services de télécommunication ou d'ordonnances de communication de renseignements relatifs à l'abonné,
 - (ii) réduire le temps de réponse aux ordonnances de communication en réduisant la période pour en demander la révision et clarifier la possibilité pour l'agent de la paix et le fonctionnaire public de recevoir certains renseignements qui leur sont fournis volontairement ou qui sont accessibles au public et d'y donner suite,
 - (iii) préciser dans quelles circonstances les agents de la paix et les fonctionnaires publics peuvent recueillir des éléments de preuve en cas d'urgence, notamment des renseignements relatifs à l'abonné,
 - (iv) permettre à un juge de paix ou à un juge d'autoriser, dans le mandat, un agent de la paix ou un fonctionnaire public à obtenir des données de localisation ou des données de transmission qui concernent des choses similaires à celle en lien avec laquelle des données sont autorisées à être obtenues en vertu du mandat et qui sont inconnues au moment où le mandat est délivré,
 - (v) conférer et clarifier des pouvoirs d'examen de données informatiques,
 - (vi) permettre à un juge de paix ou à un juge d'autoriser un agent de la paix ou un fonctionnaire public à demander à une entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication de communiquer les données de transmission ou les renseignements relatifs à l'abonné qui sont en sa possession ou à sa disposition;
- b) apporte une modification corrélative à la *Loi sur les services publicitaires fournis par des éditeurs étrangers*;
- c) modifie la *Loi sur l'entraide juridique en matière criminelle* afin de permettre au ministre de la Justice d'autoriser une autorité compétente à prendre des mesures d'exécution d'une décision rendue par une autorité d'un État ou d'une entité ha-

Disponible sur le site Web de la Chambre des communes à l'adresse suivante :
www.noscommunes.ca

(i) facilitate access to basic information that will assist the Canadian Security Intelligence Service in the performance of its duties and functions under section 12 or 16 of that Act through confirmation of service demands given to telecommunications service providers and judicial orders against those providers, and

(ii) clarify the response time for production orders; and

(e) amends the *Controlled Drugs and Substances Act* and the *Cannabis Act* to provide and clarify authorities by which computer data may be examined.

Part 2 enacts the *Supporting Authorized Access to Information Act*. That Act establishes a framework for ensuring that electronic service providers can facilitate the exercise, by authorized persons, of authorities to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act*. It also makes related and consequential amendments to the *Intelligence Commissioner Act*.

Part 3 provides for the parliamentary review of Parts 1 and 2.

bilitée à ordonner la communication de données de transmission ou de renseignements relatifs à l'abonné qui sont en la possession ou à la disposition d'une personne au Canada;

d) modifie la *Loi sur le Service canadien du renseignement de sécurité* pour, notamment :

(i) faciliter l'accès à des renseignements de base qui aideront le Service canadien du renseignement de sécurité dans l'exercice des fonctions qui lui sont conférées en vertu des articles 12 ou 16 de cette loi au moyen d'ordres de confirmer la fourniture de services donnés à des fournisseurs de services de télécommunication et d'ordonnances rendues contre de tels fournisseurs,

(ii) préciser le temps de réponse aux ordonnances de communication;

e) modifie la *Loi réglementant certaines drogues et autres substances* et la *Loi sur le cannabis* pour conférer et clarifier des pouvoirs d'examen de données informatiques.

La partie 2 édicte la *Loi sur le soutien en matière d'accès autorisé à de l'information*. Cette loi établit un cadre qui a pour but de faire en sorte que les fournisseurs de services électroniques puissent faciliter l'exercice efficace, par des personnes autorisées, de pouvoirs en matière d'accès à de l'information qui sont conférés à ces personnes sous le régime du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité*. Elle apporte aussi des modifications connexes et corrélatives à la *Loi sur le commissaire au renseignement*.

La partie 3 prévoit l'examen parlementaire des parties 1 et 2.

TABLE OF PROVISIONS

An Act respecting lawful access

Alternative Title

1 *Lawful Access Act, 2026*

PART 1

Timely Access to Data and Information

2

PART 2

Supporting Authorized Access to Information Act

41 Enactment of Act

An Act respecting the obligations of electronic service providers in relation to authorized access to information

Short Title

1 *Supporting Authorized Access to Information Act*

Interpretation

2 Definitions

Purpose

3 Purpose

His Majesty

4 Binding on His Majesty

Core Providers

5 Core providers — classes

6 Temporary exemption

Ministerial Orders

7 Order

8 Representations

9 Intelligence Commissioner

10 Duration

TABLE ANALYTIQUE

Loi concernant l'accès légal

Titre subsidiaire

1 *Loi de 2026 sur l'accès légal*

PARTIE 1

Accès aux données et aux renseignements en temps opportun

2

PARTIE 2

Loi sur le soutien en matière d'accès autorisé à de l'information

41 Édition de la loi

Loi concernant les obligations des fournisseurs de services électroniques en matière d'accès autorisé à de l'information

Titre abrégé

1 *Loi sur le soutien en matière d'accès autorisé à de l'information*

Définitions et interprétation

2 Définitions

Objet

3 Objet

Sa Majesté

4 Obligation de Sa Majesté

Fournisseurs principaux

5 Fournisseurs principaux : catégories

6 Exemption temporaire

Arrêtés ministériels

7 Arrêté

8 Observations

9 Commissaire au renseignement

10 Période de validité

11	Review	11	Examen
12	Compliance with order	12	Obligation de conformité
13	Order prevails	13	Incompatibilité
	Obligation to Assist		Obligation de prêter assistance
14	Obligation to assist	14	Obligation de prêter assistance
	Confidentiality		Confidentialité
15	Prohibition on disclosure	15	Communication interdite
16	Confidential information	16	Information confidentielle
17	Judicial review — notice to Minister	17	Contrôle judiciaire : préavis
18	Regulations — confidentiality and security	18	Règlements : confidentialité et sécurité
	Administration and Enforcement		Exécution et contrôle d'application
	Designation		Désignation
19	Designation	19	Désignation
	Inspections		Inspections
20	Authority to enter place	20	Accès au lieu
21	Dwelling-house	21	Maison d'habitation
	Internal Audit		Vérification interne
22	Audit order	22	Ordre
23	Compliance with order	23	Obligation de conformité
	Compliance Order		Ordre de conformité
24	Power to order termination of contravention	24	Pouvoir d'ordonner : cessation de la contravention
25	Compliance with order	25	Obligation de conformité
26	Request for review	26	Demande de révision
27	Decision on completion of review	27	Issue de la révision
	Administrative Monetary Penalties		Sanctions administratives pécuniaires
	Violations		Violations
28	Purpose of penalty	28	But de la sanction
29	Commission of violations	29	Violation
30	Proof of violation	30	Preuve de la violation
31	Violation by corporate officers, etc.	31	Participants à la violation
	Proceedings		Ouverture de la procédure
32	Issuance of notice of violation	32	Verbalisation
33	Limitation or prescription period	33	Prescription
34	How act or omission may be proceeded with	34	Cumul interdit
	Payment of Penalties and Alternatives to Payment		Paiement de la sanction et options
35	Effect of payment	35	Paiement

Compliance Agreements

- 36 Compliance agreements
37 Refusal to enter into compliance agreement

Review by the Minister

- 38 Review — facts

Recovery of Debts

- 39 Debt to His Majesty
40 Certificate

Offences

- 41 Offences — general
42 Proof of offence
43 Offence by corporate officers, etc.
44 Obstruction
45 False or misleading statements
46 Punishment

Regulations

- 47 Regulations
48 Distinguishing

Report

- 49 Annual report

PART 3
Parliamentary Review

48

SCHEDULE**Transactions**

- 36 Conclusion d'une transaction
37 Refus de transiger

Contestation devant le ministre

- 38 Contestation relative aux faits reprochés

Recouvrement des créances

- 39 Créance de Sa Majesté
40 Certificat de non-paiement

Infractions

- 41 Infractions générales
42 Preuve de l'infraction
43 Participants à l'infraction
44 Entrave
45 Déclaration fausse ou trompeuse
46 Peine

Règlements

- 47 Règlements
48 Précision

Rapport

- 49 Rapport annuel

PARTIE 3
Examen parlementaire

48

ANNEXE

1st Session, 45th Parliament,
3-4 Charles III, 2025-2026

HOUSE OF COMMONS OF CANADA

BILL C-22

An Act respecting lawful access

His Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

Alternative Title

Alternative title

1 This Act may be cited as the *Lawful Access Act, 2026*.

PART 1

Timely Access to Data and Information

R.S., c. C-46

Criminal Code

Amendments to the Act

2 Subsection 462.32(3) of the *Criminal Code* is replaced by the following:

Other provisions to apply

(3) Subsections 487(2.1) to (2.3) and (2.5) to (3) and section 488 apply, with any modifications that the circumstances require, to a warrant issued under this section.

3 (1) The portion of subsection 487(1) of the Act before paragraph (a) is replaced by the following:

Information for search warrant

487 (1) A judge or justice who is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that there is in a building, receptacle or place

1^{re} session, 45^e législature,
3-4 Charles III, 2025-2026

CHAMBRE DES COMMUNES DU CANADA

PROJET DE LOI C-22

Loi concernant l'accès légal

Sa Majesté, sur l'avis et avec le consentement du Sénat et de la Chambre des communes du Canada, édicte :

Titre subsidiaire

Titre subsidiaire

1 *Loi de 2026 sur l'accès légal.*

PARTIE 1

Accès aux données et aux renseignements en temps opportun

L.R., ch. C-46

Code criminel

Modification de la loi

2 Le paragraphe 462.32(3) du *Code criminel* est remplacé par ce qui suit :

Autres dispositions applicables

(3) Les paragraphes 487(2.1) à (2.3) et (2.5) à (3) et l'article 488 s'appliquent aux mandats décernés en vertu du présent article avec les adaptations nécessaires.

3 (1) Le passage du paragraphe 487(1) de la même loi précédant l'alinéa a) est remplacé par ce qui suit :

Dénonciation pour mandat de perquisition

487 (1) Le juge ou le juge de paix qui est convaincu, à la suite d'une dénonciation faite sous serment selon la formule 1, qu'il existe des motifs raisonnables de croire que,

(2) Subsection 487(1) of the Act is amended by replacing “a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant” with “a public officer”.

(3) Subsections 487(2) to (2.2) of the Act are replaced by the following:

Execution in Canada

(2) A warrant issued under subsection (1) may be executed at any place in Canada. A peace officer or public officer who executes the warrant must have authority to act in that capacity in the place where the warrant is executed.

Operation of computer system and copying equipment

(2.1) A person authorized under a warrant issued under subsection (1) to search a computer system in a building or place for computer data may

- (a)** use or cause to be used any computer system at the building or place to search any computer data contained in or available to the computer system; and
- (b)** seize any computer data for examination.

Duty of person in possession or control

(2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under a warrant issued under subsection (1) shall, on presentation of the warrant, permit the person carrying out the search to perform any of the acts referred to in subsection (2.1).

Examination of computer data

(2.3) The judge or justice may, in a warrant issued under subsection (1), authorize the examination of any computer data seized under the warrant or contained in or available to a computer system seized under the warrant, if the judge or justice is satisfied that there are reasonable grounds to believe that the computer data will afford evidence with respect to the commission of the offence set out in the information.

dans un bâtiment, contenant ou lieu, se trouve, selon le cas :

(2) Au paragraphe 487(1) de la même loi, « , dans le cas d'un fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé » est remplacé par « un fonctionnaire public ».

(3) Les paragraphes 487(2) à (2.2) de la même loi sont remplacés par ce qui suit :

Exécution au Canada

(2) Le mandat décerné en vertu du paragraphe (1) peut être exécuté en tout lieu au Canada. L'agent de la paix ou le fonctionnaire public qui exécute le mandat doit être habilité à agir à ce titre dans le lieu où celui-ci est exécuté.

Usage d'un système informatique

(2.1) La personne autorisée au titre du mandat décerné en vertu du paragraphe (1) à perquisitionner des données informatiques contenues dans un ordinateur se trouvant dans un lieu ou un bâtiment peut :

- a)** utiliser ou faire utiliser tout ordinateur s'y trouvant pour vérifier les données informatiques que celui-ci contient ou auxquelles il donne accès;
- b)** saisir des données informatiques pour examen.

Obligation du responsable du lieu

(2.2) Sur présentation du mandat décerné en vertu du paragraphe (1), le responsable du lieu qui fait l'objet de la perquisition doit faire en sorte que la personne qui procède à celle-ci puisse procéder aux opérations mentionnées au paragraphe (2.1).

Examen de données informatiques

(2.3) Dans le mandat décerné en vertu du paragraphe (1), le juge ou le juge de paix peut autoriser l'examen des données informatiques qui sont contenues dans tout ordinateur saisi en vertu du mandat ou auxquelles il donne accès, ou des données informatiques saisies en vertu du mandat, s'il est convaincu qu'il existe des motifs raisonnables de croire que ces données informatiques fourniront une preuve concernant la perpétration de l'infraction précisée dans la dénonciation.

Warrant — examination of computer data

(2.4) A judge or justice may at any time issue a warrant authorizing the examination of computer data contained in or available to a computer system that is specified in the warrant and that is in the possession of a peace officer or public officer if the judge or justice is satisfied by information on oath in Form 1 that there are reasonable grounds to believe that

- (a) an offence has been or will be committed under this Act or any other Act of Parliament; and
- (b) the computer data will afford evidence with respect to the commission of the offence.

Conditions

(2.5) The examination of computer data under a warrant issued under this section may be made subject to any conditions that the judge or justice considers advisable to ensure that the examination is reasonable in the circumstances.

Copy of warrant relating to computer data

(2.6) As soon as feasible after a warrant authorizing the examination of computer data is issued under this section, the person who applied for it shall give a copy of it to the following persons:

- (a) any person, if known, who is the lawful owner of the computer system that contains the computer data or through which the computer data is available or who is lawfully entitled to the possession of that computer system; and
- (b) any person who is referred to in the information, who is under investigation for the commission of the offence set out in the warrant and whose computer data is authorized to be examined under the warrant.

Exception

(2.7) However, a copy of the warrant is not required to be given to a person under subsection (2.6) if

- (a) the person has already received a copy under section 487.093; or
- (b) the judge or justice who issues the warrant sets aside the requirement in respect of the person, on being satisfied that doing so is justified in the circumstances.

Mandat : examen de données informatiques

(2.4) Le juge ou le juge de paix peut à tout moment décerner un mandat autorisant l'examen des données informatiques qui sont contenues dans l'ordinateur qui y est précisé et qui est en la possession d'un agent de la paix ou d'un fonctionnaire public, ou des données informatiques auxquelles cet ordinateur donne accès, s'il est convaincu, à la suite d'une dénonciation faite sous serment selon la formule 1, qu'il existe des motifs raisonnables de croire, à la fois :

- a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;
- b) que les données informatiques fourniront une preuve concernant la perpétration de l'infraction.

Conditions

(2.5) L'examen de données informatiques effectué au titre d'un mandat décerné en vertu du présent article peut être assorti des conditions que le juge ou le juge de paix estime indiquées pour que l'examen soit raisonnable dans les circonstances.

Remise d'une copie du mandat

(2.6) Dans les meilleurs délais après qu'est décerné un mandat autorisant l'examen de données informatiques en vertu du présent article, la personne qui a demandé le mandat en remet une copie aux personnes ci-après :

- a) si elle est connue, la personne qui est le propriétaire légitime ou celle qui a droit à la possession légitime de l'ordinateur contenant les données informatiques ou auxquelles celui-ci donne accès;
- b) la personne qui est visée dans la dénonciation, qui fait l'objet de l'enquête relative à l'infraction et dont les données informatiques sont autorisées à être examinées en vertu du mandat.

Exception

(2.7) Il n'est pas nécessaire de remettre une copie du mandat à une personne en application du paragraphe (2.6) dans les cas suivants :

- a) la personne en a déjà reçu une en application de l'article 487.093;
- b) le juge ou le juge de paix qui décerne le mandat accorde une dispense de cette obligation à l'égard de la personne, s'il est convaincu que les circonstances le justifient.

Extension

(2.8) If the judge or justice who issues a warrant under this section authorizing the examination of computer data or any other judge or justice having jurisdiction to issue such a warrant is satisfied, on the basis of an affidavit submitted in support of an application to extend the period within which a copy of the warrant shall be given under subsection (2.6), that the interests of justice warrant the granting of the application, the judge or justice may grant an extension, or a subsequent extension, of the period, but no extension may exceed three years.

Examination — time and place

(2.9) An examination of computer data authorized under a warrant issued under this section may take place at any time and at any place in Canada and, for the purposes of the examination, a person may copy computer data at any time and at any place in Canada.

(4) Section 487 of the Act is amended by adding the following after subsection (3):

Definitions

(4) The following definitions apply in this section.

computer data has the same meaning as in subsection 342.1(2). (*données informatiques*)

computer system has the same meaning as in subsection 342.1(2). (*ordinateur*)

judge means a judge of a superior court of criminal jurisdiction or a judge of the Court of Quebec. (*juge*)

public officer means a public officer who is appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament. (*fonctionnaire public*)

4 (1) The portion of section 487.011 of the Act before the first definition is replaced by the following:

Definitions

487.011 The following definitions apply in this section and in sections 487.012 to 487.0199, 487.11, 492.1 and 492.2.

(2) Section 487.011 of the Act is amended by adding the following in alphabetical order:

Prolongation

(2.8) Le juge ou juge de paix qui décerne un mandat autorisant l'examen de données informatiques en vertu du présent article ou un juge ou juge de paix compétent pour décerner un tel mandat peut accorder une prolongation — initiale ou ultérieure — du délai visé au paragraphe (2.6), d'une durée maximale de trois ans, s'il est convaincu par l'affidavit appuyant la demande de prolongation que les intérêts de la justice justifient la prolongation.

Examen — temps et lieu

(2.9) L'examen de données informatiques autorisé au titre d'un mandat décerné en vertu du présent article peut être effectué en tout temps et en tout lieu au Canada et, pour les besoins de cet examen, toute personne peut copier les données informatiques en tout temps et en tout lieu au Canada.

(4) L'article 487 de la même loi est modifié par adjonction, après le paragraphe (3), de ce qui suit :

Définitions

(4) Les définitions qui suivent s'appliquent au présent article.

données informatiques S'entend au sens du paragraphe 342.1(2). (*computer data*)

fonctionnaire public Fonctionnaire public nommé ou désigné pour l'exécution ou le contrôle d'application d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale. (*public officer*)

juge Juge de la cour supérieure de juridiction criminelle ou juge de la Cour du Québec. (*judge*)

ordinateur S'entend au sens du paragraphe 342.1(2). (*computer system*)

4 (1) Le passage de l'article 487.011 de la même loi précédant la première définition est remplacé par ce qui suit :

Définitions

487.011 Les définitions qui suivent s'appliquent au présent article et aux articles 487.012 à 487.0199, 487.11, 492.1 et 492.2.

(2) L'article 487.011 de la même loi est modifié par adjonction, selon l'ordre alphabétique, de ce qui suit :

subscriber information, in relation to any client of a person who provides services to the public or any subscriber to the services of such a person, means

- (a) information that may be used to identify the subscriber or client, including their name, pseudonym, address, telephone number and email address;
- (b) identifiers assigned to the subscriber or client by the person, including account numbers; and
- (c) information relating to the services provided to the subscriber or client, including
 - (i) the types of services provided,
 - (ii) the period during which the services were provided, and
 - (iii) information that identifies the devices, equipment or things used by the subscriber or client in relation to the services. (*renseignements relatifs à l'abonné*)

5 The Act is amended by adding the following after section 487.012:

Confirmation of service demand

487.0121 (1) A peace officer or public officer may make a demand in Form 5.0011 to a telecommunications service provider requiring them to confirm, within the time and in the manner specified in the demand, whether or not they provide or have provided telecommunication services to any subscriber or client, or to any account or identifier, specified in the demand.

Conditions for making demand

- (2) The peace officer or public officer may make the demand only if they have reasonable grounds to suspect that
 - (a) an offence has been or will be committed under this Act or any other Act of Parliament; and
 - (b) the confirmation that is demanded will assist in the investigation of the offence.

Medical and privileged information

(3) For greater certainty, a demand must not be made if the confirmation would disclose medical information or information that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries.

renseignements relatifs à l'abonné S'agissant d'un client d'une personne fournissant des services au public ou d'un abonné aux services fournis par une telle personne, les renseignements suivants :

- a) les renseignements permettant d'identifier l'abonné ou le client, notamment ses nom, pseudonyme, adresse, numéro de téléphone et adresse de courriel;
- b) l'identifiant que la personne a attribué à l'abonné ou au client, notamment des numéros de compte;
- c) les renseignements relatifs aux services fournis à l'abonné ou au client, notamment :
 - (i) les types de services fournis,
 - (ii) la période pendant laquelle les services ont été fournis,
 - (iii) les renseignements qui identifient les dispositifs, équipements ou choses utilisés par l'abonné ou le client en lien avec les services. (*subscriber information*)

5 La même loi est modifiée par adjonction, après l'article 487.012, de ce qui suit :

Ordre de confirmer la fourniture de services

487.0121 (1) L'agent de la paix ou le fonctionnaire public peut, selon la formule 5.0011, ordonner à tout fournisseur de services de télécommunication de confirmer, dans le délai et selon les modalités prévus dans l'ordre, si, oui ou non, il fournit ou a fourni des services de télécommunication à tout abonné ou client ou à tout compte ou identifiant, précisés dans l'ordre.

Conditions préalables à l'ordre

- (2) L'agent de la paix ou le fonctionnaire public ne donne l'ordre que s'il a des motifs raisonnables de soupçonner, à la fois :
 - a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;
 - b) que la confirmation visée par l'ordre sera utile à l'enquête relative à l'infraction.

Renseignements médicaux et protégés

(3) Il est entendu que l'ordre ne peut être donné dans le cas où la confirmation révélerait des renseignements médicaux ou des renseignements protégés par le secret professionnel de l'avocat ou du notaire.

Limitation

(4) A demand must not be made to a telecommunications service provider that is under investigation for the offence referred to in subsection (2).

Time

(5) The time specified in the demand is to be not less than 24 hours.

Non-disclosure

(6) The peace officer or public officer who makes the demand may impose conditions in the demand prohibiting the disclosure of its existence or some or all of its contents for a period not greater than one year after the day on which the demand is made. The peace officer or public officer may impose the conditions only if they have reasonable grounds to believe that the disclosure during that period would jeopardize the conduct of the investigation of the offence to which the demand relates.

Revocation

(7) A peace officer or public officer may, at any time, revoke the demand or a condition by notice given to the telecommunications service provider.

Application for review

(8) The telecommunications service provider may, within five business days after the day on which they receive the demand, apply in writing, to a judge in the judicial district where the demand was received, to revoke or vary the demand.

Notice to apply for review

(9) The telecommunications service provider may make an application under subsection (8) only if, before the confirmation is required to be provided, they give notice to the peace officer or public officer who made the demand of the telecommunications service provider's intention to make the application.

No obligation to provide confirmation

(10) The telecommunications service provider is not required to provide the confirmation until a final decision is made with respect to the application.

Revocation or variation of demand

(11) The judge in the judicial district where the demand was received may revoke or vary the demand if satisfied that

(a) it is unreasonable in the circumstances to require the applicant to provide the confirmation; or

Limite

(4) L'ordre ne peut être donné à un fournisseur de services de télécommunication faisant l'objet d'une enquête relative à l'infraction visée au paragraphe (2).

Délai

(5) Le délai prévu dans l'ordre est d'au moins vingt-quatre heures.

Interdiction de divulgation

(6) L'agent de la paix ou le fonctionnaire public qui donne l'ordre peut l'assortir de conditions pour interdire la divulgation de son existence ou de tout ou partie de son contenu pour une période d'au plus un an après la date à laquelle l'ordre est donné. Il ne peut assortir l'ordre de conditions que s'il a des motifs raisonnables de croire que la divulgation, pendant la période visée, compromettrait le déroulement de l'enquête relative à l'infraction visée dans l'ordre.

Annulation

(7) Tout agent de la paix ou tout fonctionnaire public peut, à tout moment, annuler l'ordre ou toute condition par avis remis à l'intéressé.

Demande de révision

(8) Le fournisseur de services de télécommunication peut, dans les cinq jours ouvrables suivant la date à laquelle il reçoit l'ordre, demander par écrit à un juge du district judiciaire où l'ordre a été reçu de révoquer ou de modifier l'ordre.

Préavis de demande de révision

(9) Le fournisseur de services de télécommunication peut présenter une demande en vertu du paragraphe (8) à la condition d'avoir donné, avant qu'il ne soit tenu de fournir la confirmation, un préavis de son intention de le faire à l'agent de la paix ou au fonctionnaire public qui a donné l'ordre.

Aucune obligation de fournir la confirmation

(10) Le fournisseur de services de télécommunication n'a pas à fournir la confirmation tant qu'il n'a pas été statué en dernier ressort sur sa demande.

Révocation ou modification de l'ordre

(11) Le juge du district judiciaire où l'ordre a été reçu peut révoquer l'ordre ou le modifier s'il est convaincu, selon le cas :

a) qu'il est déraisonnable, dans les circonstances, d'obliger l'intéressé à fournir la confirmation;

(b) provision of the confirmation would disclose information that is privileged or otherwise protected from disclosure by law.

Request for confirmation

(12) Despite subsection (1), no demand under that subsection is necessary for a peace officer or public officer to ask a telecommunications service provider to voluntarily provide the confirmation referred to in that subsection if the telecommunications service provider is not prohibited by law from providing it. A telecommunications service provider that provides a confirmation in those circumstances does not incur any criminal or civil liability for doing so.

Definition of *telecommunications service provider*

(13) In this section, **telecommunications service provider** has the same meaning as in subsection 2(1) of the *Telecommunications Act*.

6 The Act is amended by adding the following after section 487.0141:

Production order — subscriber information

487.0142 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may order a person who provides services to the public to prepare and produce a document containing all the subscriber information that relates to any information, including transmission data, that is specified in the order and that is in their possession or control when they receive the order.

Conditions for making order

(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that

(a) an offence has been or will be committed under this Act or any other Act of Parliament; and

(b) the subscriber information is in the person's possession or control and will assist in the investigation of the offence.

Form

(3) The order is to be in Form 5.0052.

b) que la fourniture de la confirmation révélerait des renseignements protégés par le droit applicable en matière de divulgation ou de privilèges.

Demande de confirmation

(12) Malgré le paragraphe (1), aucun ordre en vertu de ce paragraphe n'est nécessaire pour que l'agent de la paix ou le fonctionnaire public puisse demander à un fournisseur de services de télécommunication de fournir volontairement la confirmation visée à ce paragraphe si aucune règle de droit n'interdit à celui-ci de la fournir. Le fournisseur de services de télécommunication qui fournit la confirmation dans ces circonstances bénéficie de l'immunité en matière civile ou pénale pour cet acte.

Définition de *fournisseur de services de télécommunication*

(13) Pour l'application du présent article, **fournisseur de services de télécommunication** s'entend au sens du paragraphe 2(1) de la *Loi sur les télécommunications*.

6 La même loi est modifiée par adjonction, après l'article 487.0141, de ce qui suit :

Ordonnance de communication : renseignements relatifs à l'abonné

487.0142 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, ordonner à une personne fournissant des services au public d'établir et de communiquer un document comportant tous les renseignements relatifs à l'abonné qui ont trait à tous renseignements précisés dans l'ordonnance, notamment des données de transmission, et qui, au moment où il reçoit l'ordonnance, sont en sa possession ou à sa disposition.

Conditions préalables à l'ordonnance

(2) Il ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.004, qu'il existe des motifs raisonnables de soupçonner, à la fois :

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

b) que les renseignements relatifs à l'abonné sont en la possession ou à la disposition de la personne et seront utiles à l'enquête relative à l'infraction.

Formule

(3) L'ordonnance est rendue selon la formule 5.0052.

Limitation

(4) A person who is under investigation for the offence referred to in subsection (2) is not to be made subject to an order.

7 The Act is amended by adding the following after section 487.018:

Application — transmission data or subscriber information

487.0181 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may authorize a peace officer or public officer to make a request to a foreign entity that provides telecommunications services — or that provides services by a means of telecommunication — to the public to prepare and produce a document containing transmission data or subscriber information that is in the foreign entity's possession or control when it receives the request.

Conditions for authorization

(2) The justice or judge may authorize a peace officer or public officer to make the production request only if the justice or judge is satisfied by information on oath in Form 5.00801 that there are reasonable grounds to suspect that

(a) an offence has been or will be committed under this or any other Act of Parliament; and

(b) the transmission data or the subscriber information is in the foreign entity's possession or control and will assist in the investigation of the offence.

Authorization

(3) The authorization is to be in Form 5.00802 and must specify that a peace officer or public officer must not send a production request more than 30 days after the day on which the authorization is granted.

Form

(4) The production request is to be in Form 5.00803 and may include any information that is required by the foreign entity, by the foreign state in which the foreign entity is located or under an international agreement or arrangement to which Canada and the foreign state are parties.

8 Subsection 487.0191(1) of the Act is replaced by the following:

Limite

(4) La personne faisant l'objet d'une enquête relative à l'infraction visée au paragraphe (2) ne peut être assujettie à l'ordonnance.

7 La même loi est modifiée par adjonction, après l'article 487.018, de ce qui suit :

Demande : données de transmission ou renseignements relatifs à l'abonné

487.0181 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, autoriser tout agent de la paix ou fonctionnaire public à demander à une entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication d'établir et de communiquer un document comportant les données de transmission ou les renseignements relatifs à l'abonné qui sont en sa possession ou à sa disposition au moment où elle reçoit la demande.

Conditions préalables

(2) Il n'autorise l'agent de la paix ou le fonctionnaire public à faire la demande de communication que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.00801, qu'il existe des motifs raisonnables de soupçonner, à la fois :

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

b) que les données de transmission ou les renseignements relatifs à l'abonné sont en la possession de l'entité étrangère ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Autorisation

(3) L'autorisation est rédigée selon la formule 5.00802 et précise que l'agent de la paix ou le fonctionnaire public ne peut expédier la demande de communication plus de trente jours après la date à laquelle l'autorisation est accordée.

Formule

(4) La demande de communication est rédigée selon la formule 5.00803 et peut inclure tout renseignement requis par l'entité étrangère, par l'État étranger où se situe l'entité étrangère ou par toute entente internationale ou tout accord international auquel le Canada et l'État étranger sont parties.

8 Le paragraphe 487.0191(1) de la même loi est remplacé par ce qui suit :

Order prohibiting disclosure

487.0191 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may make an order prohibiting a person from disclosing the existence or some or all of the contents of a preservation demand made under section 487.012, a confirmation of service demand made under section 487.0121 or an order made under any of sections 487.013 to 487.018 during the period set out in the order.

9 Subsection 487.0192(1) of the Act is replaced by the following:

Particulars — production orders

487.0192 (1) An order made under any of sections 487.014, 487.0141, 487.0142 and 487.016 to 487.018 must require a person, financial institution or entity to produce the document to a peace officer or public officer named in the order within the time, at the place and in the form specified in the order.

10 Subsections 487.0193(1) and (2) of the Act are replaced by the following:

Application for review of production order

487.0193 (1) A person, financial institution or entity required by an order made under any of sections 487.014 to 487.018 to produce a document may, before the person, institution or entity is required to produce the document but not later than 10 business days after the day on which the order was received, apply in writing to the justice or judge who made the order — or to a judge in the judicial district where the order was received — to revoke or vary the order.

Notice required

(2) The person, institution or entity may make the application only if, before the application is made, the person, institution or entity gives notice of their intention to make the application to a peace officer or public officer named in the order.

11 Section 487.0195 of the Act is replaced by the following:

For greater certainty

487.0195 (1) For greater certainty, no preservation demand, preservation order, keep account open or active order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from pre-

Ordonnance de non-divulgence

487.0191 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, rendre une ordonnance interdisant à toute personne de divulguer l'existence ou tout ou partie du contenu d'un ordre de préservation donné en vertu de l'article 487.012, d'un ordre de confirmer la fourniture de services donné en vertu de l'article 487.0121 ou d'une ordonnance rendue en vertu de l'un des articles 487.013 à 487.018 pendant la période indiquée dans l'ordonnance.

9 Le paragraphe 487.0192(1) de la même loi est remplacé par ce qui suit :

Précisions concernant des ordonnances de communication

487.0192 (1) L'ordonnance rendue en vertu de l'un des articles 487.014, 487.0141, 487.0142 et 487.016 à 487.018 précise à la personne, à l'institution financière ou à l'entité le lieu et la forme de la communication du document, le délai dans lequel elle doit être faite ainsi que le nom de l'agent de la paix ou du fonctionnaire public à qui elle doit l'être.

10 Les paragraphes 487.0193(1) et (2) de la même loi sont remplacés par ce qui suit :

Demande de révision de l'ordonnance de communication

487.0193 (1) La personne, l'institution financière ou l'entité, avant qu'elle soit tenue de communiquer un document au titre d'une ordonnance rendue en vertu de l'un des articles 487.014 à 487.018 et au plus tard dix jours ouvrables après la date à laquelle l'ordonnance a été reçue, peut demander, par écrit au juge de paix ou au juge qui l'a rendue — ou à tout autre juge du district judiciaire où elle a été reçue — de la révoquer ou de la modifier.

Préavis obligatoire

(2) Elle peut présenter la demande à la condition d'avoir donné un préavis de son intention à l'agent de la paix ou au fonctionnaire public nommé dans celle-ci.

11 L'article 487.0195 de la même loi est remplacé par ce qui suit :

Précision

487.0195 (1) Il est entendu qu'aucun ordre de préservation ni aucune ordonnance visant à ce qu'un compte soit maintenu ouvert ou actif ou ordonnance de préservation ou de communication n'est nécessaire pour que l'agent de la paix ou le fonctionnaire public demande à

serving, to voluntarily keep an account open or active that the person is not prohibited by law from keeping open or active or to voluntarily provide a document or information to the officer that the person is not prohibited by law from disclosing.

No civil or criminal liability

(2) A person who preserves data, keeps an account open or active or provides a document or information in those circumstances does not incur any criminal or civil liability for doing so.

Unsolicited provision of information

(3) For greater certainty, no production order or warrant, or confirmation of service demand made under section 487.0121, is necessary for a peace officer or public officer to receive any information from a person or a telecommunications service provider, as the case may be, who is lawfully in possession of it, and to act on the information, if the person, without being asked for it, provides it voluntarily or is required by law, including a law of a foreign state, to provide it.

Publicly available information

(4) For greater certainty, no production order or warrant, or confirmation of service demand made under section 487.0121, is necessary for a peace officer or public officer to receive, obtain and act on any information that is available to the public.

12 Section 487.0197 of the Act is replaced by the following:

Offence — preservation or confirmation of service demand

487.0197 A person who contravenes a preservation demand made under section 487.012 or a confirmation of service demand made under section 487.0121 without lawful excuse is guilty of an offence punishable on summary conviction and is liable to a fine of not more than \$5,000.

13 (1) Subsection 487.1(1) of the Act is amended by adding the following after paragraph (l):

(l.1) a warrant under subsection 487(2.4);

(l.2) an extension under subsection 487(2.8);

une personne de maintenir volontairement ouvert ou actif un compte qu'aucune règle de droit n'interdit à celle-ci de maintenir ouvert ou actif ou de préserver volontairement des données, de lui communiquer volontairement un document ou de lui fournir volontairement des renseignements qu'aucune règle de droit n'interdit à celle-ci de préserver ou de communiquer.

Immunité

(2) La personne qui maintient un compte ouvert ou actif, préserve des données, communique un document ou fournit des renseignements dans de telles circonstances bénéficie de l'immunité en matière civile ou pénale pour les actes ainsi accomplis.

Fourniture non sollicitée de renseignements

(3) Il est entendu qu'aucun ordre de confirmer la fourniture de services donné en vertu de l'article 487.0121, qu'aucune ordonnance de communication ou qu'aucun mandat n'est nécessaire pour que l'agent de la paix ou le fonctionnaire public puisse recevoir des renseignements dont une personne ou un fournisseur de services de télécommunication, selon le cas, a la possession légitime et y donner suite, si celle-ci les fournit volontairement sans qu'on lui ait demandé ou est légalement tenue de les fournir, notamment par une loi d'un État étranger.

Renseignements accessibles au public

(4) Il est entendu qu'aucun ordre de confirmer la fourniture de services donné en vertu de l'article 487.0121, qu'aucune ordonnance de communication ou qu'aucun mandat n'est nécessaire pour que l'agent de la paix ou le fonctionnaire public puisse recevoir ou obtenir des renseignements accessibles au public et y donner suite.

12 L'article 487.0197 de la même loi est remplacé par ce qui suit :

Infraction : ordres

487.0197 Quiconque, sans excuse légitime, contrevient à l'ordre de préservation donné en vertu de l'article 487.012 ou à l'ordre de confirmer la fourniture de services donné en vertu de l'article 487.0121 commet une infraction et encourt, sur déclaration de culpabilité par procédure sommaire, une amende maximale de 5 000 \$.

13 (1) Le paragraphe 487.1(1) de la même loi est modifié par adjonction, après l'alinéa l), de ce qui suit :

(l.1) le mandat prévu au paragraphe 487(2.4);

(l.2) la prolongation prévue au paragraphe 487(2.8);

(2) Subsection 487.1(1) of the Act is amended by adding the following after paragraph (o):

| **(o.1)** an authorization under subsection 487.0181(1);

14 Section 487.11 of the Act is replaced by the following:

Exigent circumstances

487.11 A peace officer or public officer may, in the course of their duties,

(a) exercise any of the powers described in section 487, 492.1 or 492.2 without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant; or

(b) seize any subscriber information that may be the subject of an order made under subsection 487.0142(1) or any data that may be the subject of an order made under subsection 487.016(1) or 487.017(1) if the conditions for obtaining an order exist but by reason of exigent circumstances it would be impracticable to obtain an order.

15 The portion of section 487.2 of the Act before paragraph (a) is replaced by the following:

Restriction on publication

487.2 If a search warrant is issued under subsection 487(1) or a search is made under such a warrant, everyone who publishes in any document, or broadcasts or transmits in any way, any information with respect to

16 (1) The portion of section 488 of the Act before paragraph (b) is replaced by the following:

Warrant search by day

488 A search of a building, receptacle or place under a warrant issued under subsection 487(1) shall be carried out during the day, unless

(a) the judge or justice is satisfied that there are reasonable grounds for the search to be carried out at night;

(2) Le paragraphe 487.1(1) de la même loi est modifié par adjonction, après l'alinéa o), de ce qui suit :

| **o.1)** l'autorisation prévue au paragraphe 487.0181(1);

14 L'article 487.11 de la même loi est remplacé par ce qui suit :

Urgence de la situation

487.11 L'agent de la paix ou le fonctionnaire public peut, pour l'accomplissement de ses fonctions, selon le cas :

a) sans mandat, exercer tous les pouvoirs prévus aux articles 487, 492.1 ou 492.2 lorsque l'urgence de la situation rend difficilement réalisable l'obtention du mandat, sous réserve que les conditions de délivrance de celui-ci soient réunies;

b) saisir les renseignements relatifs à l'abonné qui peuvent faire l'objet d'une ordonnance rendue en vertu du paragraphe 487.0142(1) ou les données qui peuvent faire l'objet d'une ordonnance rendue en vertu des paragraphes 487.016(1) ou 487.017(1) lorsque l'urgence de la situation rend difficilement réalisable l'obtention de l'ordonnance, sous réserve que les conditions afin que celle-ci soit rendue soient réunies.

15 Le passage de l'article 487.2 de la même loi précédant l'alinéa a) est remplacé par ce qui suit :

Non-publication

487.2 Dans le cas où un mandat de perquisition est décerné en vertu du paragraphe 487(1), ou une perquisition est effectuée en vertu d'un tel mandat, est coupable d'une infraction punissable sur déclaration de culpabilité par procédure sommaire, à moins qu'une accusation n'ait été portée à l'égard d'une infraction visée par le mandat, quiconque publie ou diffuse de quelque façon que ce soit, sans la permission de chaque personne visée à l'alinéa b), des renseignements concernant :

16 (1) Le passage de l'article 488 de la même loi précédant l'alinéa b) est remplacé par ce qui suit :

Perquisition de jour

488 La perquisition dans un bâtiment, un contenant ou un lieu autorisée au titre du mandat décerné en vertu du paragraphe 487(1) est faite de jour, à moins que les conditions suivantes ne soient réunies :

a) le juge ou le juge de paix est convaincu qu'il existe des motifs raisonnables de faire la perquisition la nuit;

(2) Paragraph 488(c) of the Act is replaced by the following:

(c) the warrant authorizes that the search be carried out at night.

17 Section 489.1 of the Act is amended by adding the following after subsection (3):

Exception — computer data

(4) This section does not apply with respect to *computer data*, as defined in subsection 342.1(2), other than virtual currency or other digital assets.

18 Subsection 492(1) of the Act is replaced by the following:

Seizure of explosives

492 (1) Every person who executes a warrant issued under subsection 487(1) may seize any explosive substance that they suspect is intended to be used for an unlawful purpose, and shall, as soon as possible, remove to a place of safety anything that they seize under this section and detain it until they are ordered by a judge of a superior court to deliver it to some other person or an order is made under subsection (2).

19 (1) Subsection 492.1(3) of the Act is replaced by the following:

Tracking similar things

(2.1) A justice or judge who authorizes a peace officer or public officer to obtain tracking data that relates to the location of a thing that a person uses, carries or wears may, in the warrant, authorize the peace officer or public officer to obtain tracking data that relates to the location of any similar thing that is unknown at the time the warrant is issued if the justice or judge is satisfied that there are reasonable grounds to suspect that the person will use, carry or wear that similar thing.

Scope of warrant

(3) The warrant authorizes the peace officer or public officer, or a person acting under their direction, to install, activate, use, maintain, monitor and remove the tracking device, including covertly. The warrant also authorizes a person acting under the direction of the peace officer or public officer to obtain the tracking data that is authorized to be obtained under the warrant.

(2) L'alinéa 488c) de la même loi est remplacé par ce qui suit :

c) le libellé du mandat autorise la perquisition la nuit.

17 L'article 489.1 de la même loi est modifié par adjonction, après le paragraphe (3), de ce qui suit :

Exception : données informatiques

(4) Le présent article ne s'applique pas aux *données informatiques*, au sens du paragraphe 342.1(2), autres que la monnaie virtuelle ou les autres actifs numériques.

18 Le paragraphe 492(1) de la même loi est remplacé par ce qui suit :

Saisie d'explosifs

492 (1) Toute personne qui exécute un mandat décerné en vertu du paragraphe 487(1) peut saisir une substance explosive qu'elle soupçonne d'être destinée à servir à une fin illégale et elle doit, dès que possible, transporter dans un endroit sûr tout ce qu'elle saisit en vertu du présent article et le détenir jusqu'à ce qu'elle reçoive, d'un juge d'une cour supérieure, l'ordre de le livrer à une autre personne ou un ordre rendu en conformité avec le paragraphe (2).

19 (1) Le paragraphe 492.1(3) de la même loi est remplacé par ce qui suit :

Localisation de choses similaires

(2.1) Le juge de paix ou le juge qui autorise l'agent de la paix ou le fonctionnaire public à obtenir les données de localisation qui concernent le lieu d'une chose qu'une personne utilise, porte ou transporte peut, dans le mandat, autoriser cet agent de la paix ou ce fonctionnaire public à obtenir les données de localisation qui concernent le lieu d'une chose similaire qui est inconnue au moment où le mandat est délivré s'il est convaincu qu'il existe des motifs raisonnables de soupçonner que la personne utilisera, portera ou transportera la chose similaire.

Portée du mandat

(3) Le mandat autorise l'agent de la paix ou le fonctionnaire public, ou toute personne qui agit sous sa direction, à installer, activer, employer, entretenir, surveiller et enlever le dispositif, notamment d'une manière secrète. Il autorise également toute personne qui agit sous la direction de l'agent de la paix ou du fonctionnaire public à obtenir les données de localisation dont le mandat autorise l'obtention.

(2) Subsection 492.1(8) of the Act is replaced by the following:

Definition of *tracking device*

(8) In this section, ***tracking device*** means a device, including a *computer program as defined in* subsection 342.1(2), that may be used to obtain or record tracking data or to transmit it by a means of telecommunication.

20 (1) Subsection 492.2(2) of the Act is replaced by the following:

Transmission data — means of telecommunication

(1.1) A justice or judge who authorizes a peace officer or public officer to obtain transmission data that relates to any means of telecommunication used by a person may, in the warrant, authorize the peace officer or public officer to obtain transmission data that relates to any means of telecommunication that is unknown at the time the warrant is issued but that is of a similar type to the means of telecommunication described in the warrant if the justice or judge is satisfied that there are reasonable grounds to suspect that the person will use that other means of telecommunication.

Scope of warrant

(2) The warrant authorizes the peace officer or public officer, or a person acting under their direction, to install, activate, use, maintain, monitor and remove the transmission data recorder, including covertly. The warrant also authorizes a person acting under the direction of the peace officer or public officer to obtain the transmission data that is authorized to be obtained under the warrant.

Conditions

(2.1) A warrant may contain any conditions that the justice or judge considers appropriate, including conditions to protect a person's interests.

(2) Subsection 492.2(6) of the Act is replaced by the following:

Subscriber information related to transmission data

(5.2) The justice or judge may, in the warrant, authorize a peace officer or public officer to obtain from a person who provides services to the public any information referred to in paragraph (a) of the definition *subscriber information* in section 487.011 that relates to the transmission data that is authorized to be obtained under the warrant and that is in the person's possession or control.

(2) Le paragraphe 492.1(8) de la même loi est remplacé par ce qui suit :

Définition de *dispositif de localisation*

(8) Au présent article, ***dispositif de localisation*** s'entend de tout dispositif, notamment un *programme d'ordinateur* au sens du paragraphe 342.1(2), pouvant servir à obtenir ou à enregistrer des données de localisation ou à les transmettre par un moyen de télécommunication.

20 (1) Le paragraphe 492.2(2) de la même loi est remplacé par ce qui suit :

Données de transmission : moyens de télécommunication

(1.1) Le juge de paix ou le juge qui autorise l'agent de la paix ou le fonctionnaire public à obtenir les données de transmission qui concernent un moyen de télécommunication utilisé par une personne peut, dans le mandat, autoriser cet agent de la paix ou ce fonctionnaire public à obtenir les données de transmission qui concernent un moyen de télécommunication qui est inconnu au moment où le mandat est délivré et qui est d'un type similaire à celui qui y est mentionné, s'il est convaincu qu'il existe des motifs raisonnables de soupçonner que la personne utilisera cet autre moyen de télécommunication.

Portée du mandat

(2) Le mandat autorise l'agent de la paix ou le fonctionnaire public, ou toute personne qui agit sous sa direction, à installer, activer, employer, entretenir, surveiller et enlever l'enregistreur de données de transmission, notamment d'une manière secrète. Il autorise également toute personne qui agit sous la direction de l'agent de la paix ou du fonctionnaire public à obtenir les données de transmission dont le mandat autorise l'obtention.

Conditions

(2.1) Le mandat peut être assorti des conditions que le juge de paix ou le juge estime indiquées, notamment quant à la protection des intérêts de toute personne.

(2) Le paragraphe 492.2(6) de la même loi est remplacé par ce qui suit :

Renseignements relatifs à l'abonné : données de transmission

(5.2) Dans le mandat, le juge de paix ou le juge peut autoriser l'agent de la paix ou le fonctionnaire public à obtenir d'une personne qui fournit des services au public des *renseignements relatifs à l'abonné* visés à l'alinéa a) de la définition de ce terme à l'article 487.011 qui sont en lien avec les données de transmission dont le mandat

Definition of *transmission data recorder*

(6) In this section, **transmission data recorder** means a device, including a *computer program* as defined in subsection 342.1(2), that may be used to obtain or record transmission data or to transmit it by a means of telecommunication.

21 Form 1 of Part XXVIII of the Act is replaced by the following:

FORM 1

(Sections 320.29, 462.32, 462.321 and 487)

Information to Obtain a Search Warrant

Canada,
 Province of ,
 (*territorial division*).

This is the information of A.B., of in the (*territorial division*), (*occupation*), in this information called the informant, taken before me.

The informant says that (*describe things or computer data to be searched for and offence in respect of which search is to be made*), and that they believe on reasonable grounds that those things, or some part of them, (*or that computer data*) are in the (*dwelling-house, etc. or computer system*) of C.D., of , in (*territorial division*). (*Here add the grounds of belief, whatever they may be.*)

The informant therefore requests that a search warrant be granted to search the (*dwelling-house, etc. or computer system*) for those things (*or that computer data*).

(or)

The informant says that they believe on reasonable grounds that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*) and that computer data contained in or available to (*specify computer system in the possession of a peace officer or public officer*) will afford evidence with respect to the commission of the offence. (*Here add the grounds of belief, whatever they may be.*)

The informant therefore requests that a warrant be granted to examine that computer data.

autorise l'obtention et qui sont en sa possession ou à sa disposition.

Définition d'*enregistreur de données de transmission*

(6) Au présent article, **enregistreur de données de transmission** s'entend de tout dispositif, notamment un *programme d'ordinateur* au sens du paragraphe 342.1(2), pouvant servir à obtenir ou à enregistrer des données de transmission ou à les transmettre par un moyen de télécommunication.

21 La formule 1 de la partie XXVIII de la même loi est remplacée par ce qui suit :

FORMULE 1

(articles 320.29, 462.32, 462.321 et 487)

Dénonciation en vue d'obtenir un mandat de perquisition

Canada,
 Province de ,
 (*circonscription territoriale*).

Les présentes constituent la dénonciation de A.B., de , dans (*circonscription territoriale*), (*profession ou occupation*), ci-après appelé(e) le dénonciateur, portée devant moi.

Le dénonciateur déclare que (*décrire les choses ou les données informatiques à rechercher et l'infraction qui donne lieu à la perquisition*), et qu'il a des motifs raisonnables de croire que ces choses ou une partie d'entre elles (*ou ces données informatiques*) se trouvent dans (*l'habitation, etc., ou l'ordinateur*) de C.D., de , dans (*circonscription territoriale*). (*Ajouter ici ces motifs raisonnables, quels qu'ils soient.*)

En conséquence, le dénonciateur demande qu'un mandat de perquisition soit accordé pour perquisitionner dans (*cette habitation, etc., ou cet ordinateur*) en vue de trouver ces choses (*ou ces données informatiques*).

(ou)

Le dénonciateur déclare qu'il existe des motifs raisonnables de croire qu'une infraction prévue à (*préciser la disposition du Code criminel ou de toute autre loi fédérale*) a été ou sera commise et que des données informatiques qui sont contenues dans (*préciser un ordinateur en la possession d'un agent de la paix ou d'un fonctionnaire public*) ou auxquelles celui-ci donne accès fourniront une preuve concernant la

Sworn before me on
 (date), at (Signature of Informant)
 (place).

A (*judge or justice*) in and for

22 Form 5 of Part XXVIII of the Act is replaced by the following:

FORM 5

(Sections 320.29 and 487)

Warrant to Search

Canada,
 Province of ,
 (*territorial division*).

To the peace officers in the (*territorial division*) or to the public officers whose duties include the enforcement of (*specify an Act of Parliament*):

Whereas it appears on the oath of A.B., of that there are reasonable grounds for believing that (*describe things or computer data to be searched for and offence in respect of which search is to be made*) are in at , in this warrant called the premises;

This warrant authorizes and requires you between the hours of (*as the judge or justice may direct*) to enter into the premises and to search for the things referred to in this warrant and to bring them before a justice.

(and, if applicable)

This warrant also authorizes the examination of computer data contained in or available to a computer system seized under this warrant or of computer data seized under this warrant.

(Specify any conditions to which the examination is subject.)

(or)

Whereas it appears on the oath of A.B., of , that they have reasonable grounds to believe that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*) and to believe that computer data contained in or available to (*specify computer system in*

perpétration de l'infraction. (*Ajouter ici ces motifs raisonnables, quels qu'ils soient.*)

En conséquence, le dénonciateur demande qu'un mandat soit accordé pour autoriser l'examen de ces données informatiques.

Assermenté devant moi
 le (date), à (Signature du dénonciateur)
 (lieu).

(*Juge ou juge de paix*) dans et pour

22 La formule 5 de la partie XXVIII de la même loi est remplacée par ce qui suit :

FORMULE 5

(articles 320.29 et 487)

Mandat de perquisition

Canada,
 Province de ,
 (*circonscription territoriale*).

Aux agents de la paix de (*circonscription territoriale*) ou aux fonctionnaires publics chargés, notamment, de faire observer (*préciser la loi fédérale*) :

Attendu qu'il appert de la déposition sous serment de A.B., de , qu'il existe des motifs raisonnables de croire que (*décrire les choses ou les données informatiques à rechercher et l'infraction au sujet de laquelle la perquisition doit être faite*) se trouvent dans , à , ci-après appelé les lieux,

Le présent mandat a pour objet de vous autoriser et obliger à entrer, entre les heures de (*selon que le juge ou le juge de paix l'indique*), dans les lieux et de rechercher ces choses et de les apporter devant un juge de paix.

(et, le cas échéant)

Le présent mandat a également pour objet d'autoriser l'examen des données informatiques qui sont contenues dans tout ordinateur saisi en vertu du mandat ou auxquelles celui-ci donne accès ou des données informatiques saisies en vertu du mandat.

(Préciser toute condition dont l'examen est assorti.)

(ou)

Attendu qu'il appert de la déposition sous serment de A.B., de , qu'il existe des motifs raisonnables de croire qu'une infraction prévue à (*préciser la disposition du Code criminel ou de toute autre loi fédérale*) a été ou sera commise et que des données

the possession of a peace officer or public officer) will afford evidence with respect to the commission of the offence;

This warrant authorizes the examination of that computer data.

(Specify any conditions to which the examination is subject.)

Dated (date) at (place).

A (judge or justice) in and for

23 Part XXVIII of the Act is amended by adding the following after Form 5.001:

FORM 5.0011

(Subsection 487.0121(1))

Confirmation of Service Demand

Canada,

Province of,

(territorial division)

To (name of the telecommunications service provider), of

Because I have reasonable grounds to suspect that an offence has been or will be committed under (specify the provision of the Criminal Code or other Act of Parliament) and that the confirmation specified below will assist in the investigation of that offence, you are required to confirm, as soon as possible but not later than (specify time by which the confirmation is to be provided) whether or not you provide or have provided telecommunication services to (specify subscriber or client, or account or identifier), unless this demand is revoked.

The confirmation must be provided to (name of peace officer or public officer), (specify the form and manner).

This demand is subject to the following conditions: (specify any conditions to which the demand is subject).

You have the right to apply to revoke or vary this demand.

If you contravene this demand without lawful excuse, you may be subject to a fine.

(Signature of peace officer or public officer)

informatiques qui sont contenues dans (préciser un ordinateur en la possession d'un agent de la paix ou d'un fonctionnaire public) ou auxquelles celui-ci donne accès fourniront une preuve concernant la perpétration de l'infraction,

Le présent mandat a pour objet d'autoriser l'examen de ces données informatiques.

(Préciser toute condition dont l'examen est assorti.)

Fait le (date), à (lieu).

(Juge ou juge de paix) dans et pour

23 La partie XXVIII de la même loi est modifiée par adjonction, après la formule 5.001, de ce qui suit :

FORMULE 5.0011

(paragraphe 487.0121(1))

Ordre de confirmer la fourniture de services

Canada,

Province de,

(circonscription territoriale)

À (nom du fournisseur de services de télécommunication), de

Attendu que j'ai des motifs raisonnables de soupçonner qu'une infraction à (préciser la disposition du Code criminel ou de l'autre loi fédérale) a été ou sera commise et que la confirmation précisée ci-dessous sera utile à l'enquête relative à l'infraction. En conséquence, vous êtes tenu(e) de confirmer si, oui ou non, vous fournissez ou avez fourni des services de télécommunication à (préciser l'abonné, le client, le compte ou l'identifiant) dès que possible et au plus tard (indiquer l'échéance) à moins que l'ordre ne soit annulé.

La confirmation doit être fournie à (nom de l'agent de la paix ou du fonctionnaire public) (préciser les modalités).

Le présent ordre est assorti des conditions suivantes : (préciser les conditions, le cas échéant).

Vous avez le droit de demander la révocation ou la modification du présent ordre.

Sachez que toute contravention au présent ordre, sans excuse légitime, peut entraîner une amende.

(Signature de l'agent de la paix ou du fonctionnaire public)

24 Form 5.004 of Part XXVIII of the Act is replaced by the following:

FORM 5.004

(Subsections 487.014(2), 487.0141(2), (5) and (10), 487.0142(2), 487.015(2), 487.016(2), 487.017(2) and 487.018(3))

Information to Obtain a Production Order

Canada,
 Province of
 (territorial division)

This is the information of (*name of peace officer or public officer*), of ("the informant").

The informant says that they have reasonable grounds to suspect (*or, if the application is for an order under section 487.014 or 487.0141 of the Criminal Code, reasonable grounds to believe*)

(a) that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*); and

(b) (*if the application is for an order under section 487.014 of the Criminal Code*) that (*specify the document or data*) is in the possession or control of (*name of the person*) and will afford evidence respecting the commission of the offence.

(or)

(b) (*if the application is for an order under section 487.0141 of the Criminal Code*) that (*specify the document or data*), if it is in the possession or control of (*name of the person*) on (*specify the dates to be specified in the order*), will afford evidence respecting the commission of the offence (*and if applicable, and that the information contained in all reports made under any of sections 7, 7.1 and 9 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act during the period the order is to be in effect will afford evidence respecting the commission of the offence*).

(or)

(b) (*if the application is for an order under section 487.0142 of the Criminal Code*) that subscriber information is in the possession or control of (*name of the person*) and will assist in the investigation of the offence.

(or)

24 La formule 5.004 de la partie XXVIII de la même loi est remplacée par ce qui suit :

FORMULE 5.004

(paragraphe 487.014(2), 487.0141(2), (5) et (10), 487.0142(2), 487.015(2), 487.016(2), 487.017(2) et 487.018(3))

Dénonciation en vue d'obtenir une ordonnance de communication

Canada,
 Province de
 (circonscription territoriale)

La présente constitue la dénonciation de (*nom de l'agent de la paix ou du fonctionnaire public*), de , ci-après appelé(e) « le dénonciateur ».

Le dénonciateur déclare qu'il a des motifs raisonnables de soupçonner (*ou, si la demande vise à obtenir une ordonnance en vertu des articles 487.014 ou 487.0141 du Code criminel, de croire*) que les conditions suivantes sont réunies :

a) une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise;

b) (*si la demande vise à obtenir une ordonnance en vertu de l'article 487.014 du Code criminel, préciser le document ou les données*) sont en la possession de (*nom de la personne*) ou à sa disposition et fourniront une preuve concernant la perpétration de l'infraction.

(ou)

b) (*si la demande vise à obtenir une ordonnance en vertu de l'article 487.0141 du Code criminel, préciser le document ou les données*), s'ils sont en la possession de (*nom de la personne*) ou à sa disposition en date du (*préciser les dates qui doivent être précisées dans l'ordonnance*), ils fourniront une preuve concernant la perpétration de l'infraction (*et, le cas échéant, et les renseignements contenus dans toutes déclarations qu'elle fait en application de l'un des articles 7, 7.1 ou 9 de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes au cours de la période où l'ordonnance doit être en vigueur fourniront une preuve concernant la perpétration de l'infraction*).

(ou)

(b) (if the application is for an order under section 487.015 of the Criminal Code) that the identification of a device or person involved in the transmission of (specify the communication) will assist in the investigation of the offence and that (specify the transmission data) that is in the possession or control of one or more persons whose identity is unknown will enable that identification.

(or)

(b) (if the application is for an order under section 487.016 of the Criminal Code) that (specify the transmission data) is in the possession or control of (name of the person) and will assist in the investigation of the offence.

(or)

(b) (if the application is for an order under section 487.017 of the Criminal Code) that (specify the tracking data) is in the possession or control of (name of the person) and will assist in the investigation of the offence.

(or)

(b) (if the application is for an order under section 487.018 of the Criminal Code) that (specify the data) is in the possession or control of (name of the financial institution, person or entity) and will assist in the investigation of the offence.

The reasonable grounds are:

The informant therefore requests

(if the application is for an order under section 487.014 of the Criminal Code) that (name of the person) be ordered to produce a document that is a copy of (specify the document) that is in their possession or control when they receive the order (and/or to prepare and produce a document containing (specify the data) that is in their possession or control when they receive the order).

(or)

(if the application is for an order under section 487.0141 of the Criminal Code) that (name of the person) be ordered to produce a document that is a copy of (specify the document) that is in their possession or control on (specify the dates to be specified in the order) (and/or to prepare and produce a document containing (specify the data) that is in their possession or control on (specify the dates to be specified in the order)) (and if applicable, and that the person be ordered to produce a copy of all reports made under any of sections 7, 7.1 and 9 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act during the period the order is to be in effect).

(b) (si la demande vise à obtenir une ordonnance en vertu de l'article 487.0142 du Code criminel) des renseignements relatifs à l'abonné sont en la possession de (nom de la personne) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

(ou)

(b) (si la demande vise à obtenir une ordonnance en vertu de l'article 487.015 du Code criminel) l'identification de tout dispositif ayant servi à la transmission de (préciser la communication) ou de toute personne y ayant participé sera utile à l'enquête relative à l'infraction et (préciser les données de transmission) sont en la possession ou à la disposition d'une ou de plusieurs personnes — dont l'identité n'est pas connue — et permettront cette identification.

(ou)

(b) (si la demande vise à obtenir une ordonnance en vertu de l'article 487.016 du Code criminel, préciser les données de transmission) sont en la possession de (nom de la personne) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

(ou)

(b) (si la demande vise à obtenir une ordonnance en vertu de l'article 487.017 du Code criminel, préciser les données de localisation) sont en la possession de (nom de la personne) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

(ou)

(b) (si la demande vise à obtenir une ordonnance en vertu de l'article 487.018 du Code criminel, préciser les données) sont en la possession de (nom de l'institution financière, de la personne ou de l'entité) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Les motifs raisonnables sont les suivants :

En conséquence, le dénonciateur demande

(si la demande vise à obtenir une ordonnance en vertu de l'article 487.014 du Code criminel) qu'il soit ordonné à (nom de la personne) de communiquer un document qui est la copie de (indiquer le document) qui est en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance (ou d'établir et de communiquer un document comportant (indiquer les données) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance).

(ou)

(or)

(if the application is for an order under section 487.0142 of the Criminal Code) that (name of the person) be ordered to prepare and produce a document containing all the subscriber information that is in their possession or control when they receive the order that relates to (specify information).

(or)

(if the application is for an order under section 487.015 of the Criminal Code) that a person who is served with the order in accordance with subsection 487.015(4) of the Criminal Code be ordered to prepare and produce a document containing (specify the transmission data) that is in their possession or control when they are served with the order.

(or)

(if the application is for an order under section 487.016 of the Criminal Code) that (name of the person) be ordered to prepare and produce a document containing (specify the transmission data) that is in their possession or control when they receive the order.

(or)

(if the application is for an order under section 487.017 of the Criminal Code) that (name of the person) be ordered to prepare and produce a document containing (specify the tracking data) that is in their possession or control when they receive the order.

(or)

(if the application is for an order under section 487.018 of the Criminal Code) that (name of the financial institution, person or entity) be ordered to prepare and produce a document setting out (specify the data) that is in their possession or control when they receive the order.

Sworn before me on (date), at (place).

(Signature of informant)

(Signature of justice or judge)

(si la demande vise à obtenir une ordonnance en vertu de l'article 487.0141 du Code criminel) qu'il soit ordonné à (nom de la personne) de communiquer un document qui est la copie de (indiquer le document) qui est en sa possession ou à sa disposition en date du (préciser les dates qui doivent être précisées dans l'ordonnance) (ou d'établir et de communiquer un document comportant (indiquer les données) qui sont en sa possession ou à sa disposition en date du (préciser les dates qui doivent être précisées dans l'ordonnance)) (et, le cas échéant, de communiquer une copie de toutes déclarations qu'elle fait en application de l'un des articles 7, 7.1 et 9 de la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes au cours de la période où l'ordonnance doit être en vigueur).

(ou)

(si la demande vise à obtenir une ordonnance en vertu de l'article 487.0142 du Code criminel) qu'il soit ordonné à (nom de la personne) d'établir et de communiquer un document comportant tous les renseignements relatifs à l'abonné qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance et qui sont relatifs à (préciser les renseignements).

(ou)

(si la demande vise à obtenir une ordonnance en vertu de l'article 487.015 du Code criminel) qu'il soit ordonné à toute personne à qui l'ordonnance est signifiée conformément au paragraphe 487.015(4) du Code criminel d'établir et de communiquer un document comportant (préciser les données de transmission) qui sont en sa possession ou à sa disposition au moment où l'ordonnance lui est signifiée.

(ou)

(si la demande vise à obtenir une ordonnance en vertu de l'article 487.016 du Code criminel) qu'il soit ordonné à (nom de la personne) d'établir et de communiquer un document comportant (préciser les données de transmission) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance.

(ou)

(si la demande vise à obtenir une ordonnance en vertu de l'article 487.017 du Code criminel) qu'il soit ordonné à (nom de la personne) d'établir et de communiquer un document comportant (préciser les données de localisation) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance.

(ou)

(si la demande vise à obtenir une ordonnance en vertu de l'article 487.018 du Code criminel) qu'il soit ordonné à (nom de l'institution financière, de la personne ou de l'entité) d'établir et de communiquer un document énonçant (préciser les données) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance.

Fait sous serment devant moi ce (date), à (lieu).

(Signature du dénonciateur)

10

(Signature du juge de paix ou du juge)

25 Part XXVIII of the Act is amended by adding the following after Form 5.0051:

25 La partie XXVIII de la même loi est modifiée par adjonction, après la formule 5.0051, de ce qui suit :

15

FORM 5.0052

(Subsection 487.0142(3))

Production Order — Subscriber Information

Canada,
 Province of
 (territorial division)

To (name of person), of :

Whereas I am satisfied by information on oath of (name of peace officer or public officer), of , that there are reasonable grounds to suspect that an offence has been or will be committed under (specify the provision of the Criminal Code or other Act of Parliament) and that subscriber information is in your possession or control and will assist in the investigation of the offence;

Therefore, you are ordered to

produce a document that is a copy of (specify the document) that is in your possession or control when you receive this order

(and/or)

prepare and produce a document containing all the subscriber information that is in your possession or control when you receive this order and that relates to (specify information).

FORMULE 5.0052

(paragraphe 487.0142(3))

Ordonnance de communication : renseignements relatifs à l'abonné

Canada,
 Province de.....
 (circonscription territoriale)

À (nom de la personne), de :

Attendu que je suis convaincu(e), en me fondant sur une dénonciation sous serment par (nom de l'agent de la paix ou du fonctionnaire public), de , qu'il existe des motifs raisonnables de soupçonner qu'une infraction prévue à (préciser la disposition du Code criminel ou de l'autre loi fédérale) a été ou sera commise et que des renseignements relatifs à l'abonné sont en votre possession ou à votre disposition et seront utiles à l'enquête relative à l'infraction.

En conséquence, vous êtes tenu(e)

de communiquer un document qui est la copie de (préciser le document) qui est en votre possession ou à votre disposition au moment où vous recevez l'ordonnance,

(et/ou)

d'établir et de communiquer un document comportant tous les renseignements relatifs à l'abonné qui sont en votre possession ou à votre disposition au

The document must be produced to (*name of peace officer or public officer*) within (*time*) at (*place*) in (*form*).

This order is subject to the following conditions: (*specify any conditions to which the demand is subject*). 5

You have the right to apply to revoke or vary this order.

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both. 10

Dated (*date*), at (*place*).

(*Signature of justice or judge*)

moment où vous recevez l'ordonnance (*préciser les renseignements*).

Le document doit être communiqué à (*nom de l'agent de la paix ou du fonctionnaire public*), dans un délai de (*indiquer le délai*), à (*lieu*), et être présenté (*indiquer la forme*). 5

La présente ordonnance est assortie des conditions suivantes : (*préciser les conditions, le cas échéant*).

Vous avez le droit de demander la révocation ou la modification de la présente ordonnance. 10

Sachez que toute contravention à la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Fait le (*date*), à (*lieu*). 15

(*Signature du juge de paix ou du juge*)

26 Part XXVIII of the Act is amended by adding the following after Form 5.008: 15

26 La partie XXVIII de la même loi est modifiée par adjonction, après la formule 5.008, de ce qui suit :

FORM 5.00801

(Subsection 487.0181(2))

Information to Obtain an Authorization

Canada,

Province of

(*territorial division*) 20

This is the information of (*name of peace officer or public officer*), of ("the informant").

The informant says that they have reasonable grounds to suspect

(a) that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*); and 25

(b) that (*specify the transmission data or the subscriber information*) is in the possession or control of (*name of the foreign entity that provides telecommunications services — or that provides services by a means of telecommunication — to the public*) and will assist in the investigation of the offence. 30

The reasonable grounds are: 35

The informant therefore requests

FORMULE 5.00801 20

(paragraphe 487.0181(2))

Dénonciation en vue d'obtenir une autorisation

Canada,

Province de

(*circonscription territoriale*) 20

La présente constitue la dénonciation de (*nom de l'agent de la paix ou du fonctionnaire public*), de , ci-après appelé(e) « le dénonciateur ». 25

Le dénonciateur déclare qu'il a des motifs raisonnables de soupçonner que les conditions suivantes sont réunies : 30

a) une infraction à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise;

b) (*préciser les données de transmission ou les renseignements relatifs à l'abonné*) sont en la possession de (*nom de l'entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication*) ou à sa disposition et seront utiles à l'enquête relative à l'infraction. 35 40

Les motifs raisonnables sont les suivants :

En conséquence, le dénonciateur demande

that a peace officer or public officer be authorized to request that (*name of the foreign entity that provides telecommunications services — or that provides services by a means of telecommunication — to the public*) prepare and produce a document containing (*specify the transmission data or the subscriber information*) that is in its possession or control when it receives the request.

Sworn before me on (*date*), at (*place*).

(*Signature of informant*)

(*Signature of justice or judge*)

FORM 5.00802

(Subsection 487.0181(3))

Authorization to Request Production of Transmission Data or Subscriber Information

Canada,

Province of

(*territorial division*)

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of , that there are reasonable grounds to suspect

(a) that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*); and

(b) that (*specify the transmission data or the subscriber information*) is in the possession or control of (*name of the foreign entity that provides telecommunications services — or that provides services by a means of telecommunication — to the public*) and the data or information will assist in the investigation of the offence.

Therefore, a peace officer or public officer is authorized to request that (*name of the foreign entity that provides telecommunications services — or that provides services by a means of telecommunication — to the public*) prepare and produce a document containing (*specify the transmission data or the subscriber information*) that is in its possession or control when it receives the request.

qu'un agent de la paix ou un fonctionnaire public soit autorisé à demander à (*nom de l'entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication*) d'établir et de communiquer un document comportant (*préciser les données de transmission ou les renseignements relatifs à l'abonné*) qui sont en sa possession ou à sa disposition au moment où elle reçoit la demande.

Fait sous serment devant moi ce (*date*), à (*lieu*).

(*Signature du dénonciateur*)

(*Signature du juge de paix ou du juge*)

FORMULE 5.00802

(paragraphe 487.0181(3))

Autorisation de demander la communication de données de transmission ou de renseignements relatifs à l'abonné

Canada,

Province de

(*circonscription territoriale*)

Attendu que je suis convaincu(e), en me fondant sur une dénonciation sous serment par (*nom de l'agent de la paix ou du fonctionnaire public*), de , qu'il existe des motifs raisonnables de soupçonner, à la fois :

a) qu'une infraction à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise;

b) que (*préciser les données de transmission ou les renseignements relatifs à l'abonné*) sont en la possession de (*nom de l'entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication*) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

En conséquence, un agent de la paix ou un fonctionnaire public est autorisé à demander à (*nom de l'entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication*) d'établir et de communiquer un document comportant (*préciser les données de transmission ou les renseignements rela-*

A peace officer or public officer must not send the production request more than 30 days after the day on which this authorization is granted.

Dated (*date*), at (*place*).

(*Signature of justice or judge*)

5

FORM 5.00803

(Subsection 487.0181(4))

Production Request for Transmission Data or Subscriber Information

Canada,

Province of

To (*name of foreign entity that provides telecommunications services — or that provides services by a means of telecommunication — to the public*), of :

10

This is a production request of (*name of peace officer or public officer*), of

15

Whereas I am authorized to make this request by a justice or judge under section 487.0181 of the *Criminal Code* (*attach authorization*).

Therefore, I request that you prepare and produce a document containing (*specify the transmission data or the subscriber information*) that is in your possession or control when you receive this request.

20

I request that you produce this document to (*recipient*) in (*form*).

(*Specify any information that may be included under subsection 487.0181(4) of the Criminal Code, if applicable.*)

25

Dated (*date*), at (*place*).

(*Signature of peace officer or public officer*)

tifs à l'abonné) qui sont en sa possession ou à sa disposition au moment où elle reçoit la demande.

L'agent de la paix ou le fonctionnaire public ne peut expédier la demande de communication plus de trente jours après la date à laquelle l'autorisation est accordée.

5

Fait le (*date*), à (*lieu*).

(*Signature du juge de paix ou du juge*)

FORMULE 5.00803

(paragraphe 487.0181(4))

10

Demande de communication : données de transmission ou renseignements relatifs à l'abonné

Canada,

Province de

À (*nom de l'entité étrangère qui fournit au public des services de télécommunication ou des services à l'aide d'un moyen de télécommunication*), de :

15

La présente constitue la demande de communication de (*nom de l'agent de la paix ou du fonctionnaire public*), de

Attendu que j'ai été autorisé(e) par un juge de paix ou un juge, au titre de l'article 487.0181 du *Code criminel*, à faire la présente demande (*joindre l'autorisation*).

20

En conséquence, je vous demande d'établir et de communiquer un document comportant (*préciser les données de transmission ou les renseignements relatifs à l'abonné*) qui sont en votre possession ou à votre disposition au moment où vous recevez la présente demande.

25

Je vous demande de communiquer ce document à (*préciser le destinataire*), présenté (*indiquer la forme*).

30

(*Préciser tout renseignement qui peut être inclus au titre du paragraphe 487.0181(4) du Code criminel, s'il y a lieu.*)

35

Fait le (*date*), à (*lieu*).

(*Signature de l'agent de la paix ou du fonctionnaire public*)

27 Forms 5.009 and 5.0091 of Part XXVIII of the Act are replaced by the following:

FORM 5.009

(Subsection 487.0191(2))

Information to Obtain a Non-Disclosure Order

Canada,
 Province of
(territorial division)

This is the information of (*name of peace officer or public officer*), of ("the informant").

The informant says that they have reasonable grounds to believe that the disclosure of the existence (or any of the contents or any of the following portion or portions) of (*identify the preservation demand made under section 487.012 of the Criminal Code, the confirmation of service demand made under section 487.0121 of that Act or the order made under any of sections 487.013 to 487.018 of that Act, as the case may be*) during (*identify the period*) would jeopardize the conduct of the investigation of the offence to which it relates:

(*specify portion or portions*)

The reasonable grounds are:

The informant therefore requests an order prohibiting (*name of the person, financial institution or entity*) from disclosing the existence (or any of the contents or any of the specified portion or portions) of the demand (or the order) during a period of (*identify the period*) after the day on which the order is made.

Sworn before me on (*date*), at (*place*).

(*Signature of informant*)

(*Signature of justice or judge*)

FORM 5.0091

(Subsection 487.0191(3))

Non-Disclosure Order

Canada,
 Province of

27 Les formules 5.009 et 5.0091 de la partie XXVIII de la même loi sont remplacées par ce qui suit :

FORMULE 5.009

(paragraphe 487.0191(2))

Dénonciation en vue d'obtenir une ordonnance de non-divulgation

5 Canada, 5
 Province de
(circonscription territoriale)

La présente constitue la dénonciation de (*nom de l'agent de la paix ou du fonctionnaire public*), de , ci-après appelé(e) « le dénonciateur ». 10

Le dénonciateur déclare qu'il a des motifs raisonnables de croire que la divulgation de l'existence (ou d'une partie quelconque ou d'une partie quelconque du ou des passages précisés ci-dessous) de (*indiquer l'ordre de préservation donné en vertu de l'article 487.012 du Code criminel, l'ordre de confirmer la 15*
fourniture de services donné en vertu de l'article 487.0121 de cette loi ou l'ordonnance rendue en vertu de l'un des articles 487.013 à 487.018 de cette loi, 20
selon le cas) pendant (*indiquer la période*) compromettrait le déroulement de l'enquête relative à l'infraction visée : 20

(*préciser le ou les passages*)

Les motifs raisonnables sont les suivants :

25 En conséquence, le dénonciateur demande qu'il soit 25
 ordonné à (*nom de la personne, de l'institution financière ou de l'entité*) de ne pas divulguer l'existence (ou une partie quelconque ou une partie quelconque du ou des passages précisés) de l'ordre (ou de l'ordonnance) pendant (*indiquer la période*) après la 30
 date à laquelle l'ordonnance est rendue. 30

Fait sous serment devant moi ce (*date*), à (*lieu*).

(*Signature du dénonciateur*)

(*Signature du juge de paix ou du juge*)

FORMULE 5.0091

(paragraphe 487.0191(3))

Ordonnance de non-divulgation

35 Canada,
 35 Province de

(territorial division)

To (name of person, financial institution or entity), of :

Whereas I am satisfied by information on oath of (name of peace officer or public officer), of 5
 , that there are reasonable grounds to believe that the disclosure of the existence (or any of the contents or any of the portion or portions, specified in the information,) of (identify the preservation demand made under section 487.012 of the Criminal Code, the confirmation of service demand made under section 487.0121 of that Act or the order made under any of sections 487.013 to 487.018 of that Act, as the case may be) during (identify the period) would jeopardize the conduct of the investigation of the offence to which it relates; 10 15

Therefore, you are prohibited from disclosing the existence (or any of the contents or any of the following portion or portions) of the demand (or the order) during a period of (identify the period) after the day on which this order is made. 20

(specify portion or portions)

You have the right to apply to revoke or vary this order.

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both. 25

Dated (date), at (place).

(Signature of justice or judge)

1999, c. 23

Consequential Amendment to the Foreign Publishers Advertising Services Act

28 Subsection 5(1) of the Foreign Publishers Advertising Services Act is amended by replacing “section 487” with “subsection 487(1)”. 30

(circonscription territoriale)

À (nom de la personne, de l'institution financière, ou de l'entité), de :

Attendu que je suis convaincu(e), en me fondant sur une dénonciation sous serment par (nom de l'agent de la paix ou du fonctionnaire public), de , qu'il existe des motifs raisonnables de croire que la divulgation de l'existence (ou d'une partie quelconque ou d'une partie quelconque du ou des passages — précisés dans la dénonciation —) de (indiquer l'ordre de préservation donné en vertu de l'article 487.012 du Code criminel, l'ordre de confirmer la fourniture de services donné en vertu de l'article 487.0121 de cette loi ou l'ordonnance rendue en vertu de l'un des articles 487.013 à 487.018 de cette loi, selon le cas) pendant (indiquer la période) compromettrait le déroulement de l'enquête relative à l'infraction visée, 5 10 15

En conséquence, vous êtes tenu(e) de ne pas divulguer l'existence (ou une partie quelconque ou une partie quelconque du ou des passages précisés ci-dessous) de l'ordre (ou de l'ordonnance) pendant (indiquer la période) après la date à laquelle la présente ordonnance est rendue : 20

(préciser le ou les passages) 25

Vous avez le droit de demander la révocation ou la modification de la présente ordonnance.

Sachez que la contravention de la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines. 30

Fait le (date), à (lieu).

(Signature du juge de paix ou du juge)

1999, ch. 23

Modification corrélative à la Loi sur les services publicitaires fournis par des éditeurs étrangers

28 Au paragraphe 5(1) de la Loi sur les services publicitaires fournis par des éditeurs étrangers, « de l'article 487 » est remplacé par « du paragraphe 487(1) ». 35

R.S., c. 30 (4th Supp.)

Mutual Legal Assistance in Criminal Matters Act

29 The *Mutual Legal Assistance in Criminal Matters Act* is amended by adding the following after section 22.06:

Enforcement of Foreign Decisions for Production

Request to Minister

22.07 (1) When a written request is presented to the Minister by a state or entity for the enforcement in Canada of a decision made by an authority of that state or entity that is empowered to compel the production of transmission data or subscriber information that is in the possession or control of a person in Canada, the Minister may authorize a competent authority to make arrangements for the enforcement of the decision.

Application for enforcement

(2) The competent authority must apply *ex parte* for the enforcement of the decision to a *justice*, as defined in section 2 of the *Criminal Code*, a judge of a *superior court of criminal jurisdiction*, as defined in that section, or a judge of the Court of Quebec.

Enforcement

(3) The justice or judge to whom the application is made may make the decision enforceable if they are satisfied that

(a) in the case of transmission data, the conditions set out in subsection 487.016(2) of the *Criminal Code*, with any necessary modifications, are met; or

(b) in the case of subscriber information, the conditions set out in subsection 487.0142(2) of the *Criminal Code*, with any necessary modifications, are met.

A decision that is made enforceable is deemed to be a judgment of the court to which the judge or justice belongs and may be executed anywhere in Canada.

Designated person

(4) The justice or judge who makes the decision enforceable under subsection (3) must designate a person to whom a record containing the transmission data or the subscriber information must be produced by the person in Canada referred to in the decision.

L.R., ch. 30 (4^e suppl.)

Loi sur l'entraide juridique en matière criminelle

29 La Loi sur l'entraide juridique en matière criminelle est modifiée par adjonction, après l'article 22.06, de ce qui suit :

Exécution de décisions étrangères de communication

Demande au ministre

22.07 (1) Lorsqu'une demande est présentée par écrit au ministre par un État ou une entité en vue de l'exécution au Canada d'une décision rendue par une autorité de l'État ou de l'entité habilitée à ordonner la communication de données de transmission ou de renseignements relatifs à l'abonné qui sont en la possession ou à la disposition d'une personne au Canada, le ministre peut autoriser une autorité compétente à prendre les mesures d'exécution de la décision.

Requête en vue de l'exécution

(2) L'autorité compétente présente une requête *ex parte*, en vue de l'exécution de la décision, à un *juge de paix* au sens de l'article 2 du *Code criminel*, à un juge de la *cour supérieure de juridiction criminelle* au sens de cet article ou à un juge de la Cour du Québec.

Exécution

(3) Le juge de paix ou le juge saisi de la requête peut rendre exécutoire la décision, s'il est convaincu que :

a) s'agissant de données de transmission, les conditions énoncées au paragraphe 487.016(2) du *Code criminel*, avec les adaptations nécessaires, sont réunies;

b) s'agissant de renseignements relatifs à l'abonné, les conditions énoncées au paragraphe 487.0142(2) du *Code criminel*, avec les adaptations nécessaires, sont réunies.

La décision rendue exécutoire vaut jugement du tribunal auquel le juge de paix ou le juge appartient et peut être exécutée partout au Canada.

Personne désignée

(4) Le juge de paix ou le juge qui rend la décision exécutoire au titre du paragraphe (3) désigne la personne à qui un document comportant les données de transmission ou les renseignements relatifs à l'abonné doit être communiqué par la personne au Canada visée par la décision.

Timing

(5) The justice or judge must order that the person in Canada referred to in the decision produce the record containing the transmission data or the subscriber information to the designated person

(a) no later than 45 days after the day on which the decision is served, in the case of transmission data; or

(b) no later than 20 days after the day on which the decision is served, in the case of subscriber information.

Order prohibiting disclosure

(6) Section 487.0191 of the *Criminal Code* applies, with any necessary modifications, in respect of a decision made enforceable under subsection (3) and an order made under subsection (5).

Sending abroad

(7) The justice or judge must also order

(a) that the designated person send the record containing the transmission data or the subscriber information directly to the state or entity referred to in subsection (1) that made the request; or

(b) that sections 20 and 21 apply to the sending of the record containing the transmission data or the subscriber information, with any necessary modifications.

Report

(8) The designated person must

(a) make a report concerning the execution of the decision to the justice or judge who made it enforceable — or to another justice for the same territorial division or another judge in the judicial district where the decision was made enforceable — accompanied by a general description of the transmission data or the subscriber information contained in the record and, if the justice or judge requires it, the record containing the transmission data or the subscriber information; and

(b) send a copy of the report to the Minister without delay.

Timing of report and sending abroad

(9) If the justice or judge makes an order under paragraph (7)(a), the designated person must make the report to the justice or judge and send the record containing the transmission data or the subscriber information to the

Délais

(5) Le juge de paix ou le juge ordonne que la personne au Canada visée par la décision communique à la personne désignée le document comportant les données de transmission ou les renseignements relatifs à l'abonné :

a) au plus tard quarante-cinq jours après la date de signification de la décision, dans le cas de données de transmission;

b) au plus tard vingt jours après la date de signification de la décision, dans le cas de renseignements relatifs à l'abonné.

Ordonnance de non-divulagation

(6) L'article 487.0191 du *Code criminel* s'applique, avec les adaptations nécessaires, à l'égard de la décision rendue exécutoire au titre du paragraphe (3) et de l'ordonnance rendue au titre du paragraphe (5).

Transmission à l'étranger

(7) Le juge de paix ou le juge ordonne en outre, selon le cas :

a) que la personne désignée transmette directement à l'État ou à l'entité requérant visé au paragraphe (1) le document comportant les données de transmission ou les renseignements relatifs à l'abonné;

b) que les articles 20 et 21 s'appliquent à la transmission du document comportant ces données ou renseignements, avec les adaptations nécessaires.

Rapport

(8) La personne désignée :

a) remet au juge de paix ou au juge qui a rendu exécutoire la décision — ou à un autre juge de paix de la même circonscription territoriale ou à un autre juge du district judiciaire où la décision a été rendue exécutoire — un rapport d'exécution comportant une description générale des données de transmission ou des renseignements relatifs à l'abonné contenus dans le document et, si le juge de paix ou le juge l'exige, le document comportant ces données ou renseignements;

b) envoie sans délai une copie du rapport au ministre.

Délai : rapport et transmission à l'étranger

(9) Dans le cas d'une ordonnance rendue en vertu de l'alinéa (7)a), la personne désignée est tenue de remettre le rapport au juge de paix ou au juge et de transmettre le document comportant les données de transmission ou les

state or entity that made the request no later than five days after the day on which the record was produced under subsection (5).

Offence

(10) Section 487.0198 of the *Criminal Code* applies with respect to an order made under subsection (5).

Definitions

(11) In this section, **transmission data** and **subscriber information** have the same meaning as in section 487.011 of the *Criminal Code*.

R.S., c. C-23

Canadian Security Intelligence Service Act

30 The heading of Part II of the *Canadian Security Intelligence Service Act* is replaced by the following:

Confirmation of Service Demand and Judicial Control

31 The Act is amended by adding the following before section 20.3:

Definition of *telecommunications service provider*

20.21 In sections 20.22 to 20.26 and 20.5, **telecommunications service provider** has the same meaning as in subsection 2(1) of the *Telecommunications Act*.

Confirmation of service demand

20.22 (1) For the purpose of performing its duties and functions under section 12 or 16, the Service may make a demand in Form 0.1 of Schedule 2 to a telecommunications service provider requiring them to confirm, within the time and in the manner specified in the demand, whether or not they provide or have provided services to any subscriber or client, or to any account or identifier, specified in the demand.

Medical and privileged information

(2) For greater certainty, a demand must not be made if the confirmation would disclose medical information or information that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries.

renseignements relatifs à l'abonné à l'État ou à l'entité requérant au plus tard cinq jours après la date à laquelle le document a été communiqué au titre du paragraphe (5).

Infraction

(10) L'article 487.0198 du *Code criminel* s'applique à l'égard de l'ordonnance prévue au paragraphe (5).

Définitions

(11) Au présent article, **données de transmission** et **renseignements relatifs à l'abonné** s'entendent au sens de l'article 487.011 du *Code criminel*.

L.R., ch. C-23

Loi sur le Service canadien du renseignement de sécurité

30 Le titre de la partie II de la *Loi sur le Service canadien du renseignement de sécurité* est remplacé par ce qui suit :

Ordre de confirmer la fourniture de services et contrôle judiciaire

31 La même loi est modifiée par adjonction, avant l'article 20.3, de ce qui suit :

Définition de *fournisseur de services de télécommunication*

20.21 Pour l'application des articles 20.22 à 20.26 et 20.5, **fournisseur de services de télécommunication** s'entend au sens du paragraphe 2(1) de la *Loi sur les télécommunications*.

Ordre de confirmer la fourniture de services

20.22 (1) Dans l'exercice des fonctions qui lui sont conférées en vertu des articles 12 ou 16, le Service peut, selon le formulaire 0.1 de l'annexe 2, ordonner à tout fournisseur de services de télécommunication de confirmer, dans le délai et selon les modalités prévus dans l'ordre, si, oui ou non, il fournit ou a fourni des services à tout abonné ou client ou à tout compte ou identifiant, précisés dans l'ordre.

Informations médicales et protégées

(2) Il est entendu que l'ordre ne peut être donné dans le cas où la confirmation révélerait des informations médicales ou des informations protégées par le secret professionnel de l'avocat ou du notaire.

Time

(3) The time specified in the demand is to be not less than 24 hours.

Non-disclosure

(4) The Service may impose conditions in the demand prohibiting the disclosure of its existence or some or all of its contents.

Obligation to comply

(5) The telecommunications service provider must comply with the demand. Section 126 of the *Criminal Code* does not apply in respect of a contravention of this subsection.

Revocation of demand

(6) The Service may, at any time, revoke the demand or a condition by notice given to the telecommunications service provider.

Revocation or variation of confirmation of service demand

20.23 (1) Before a telecommunications service provider is required to provide the confirmation required by a demand made under section 20.22, but not later than five business days after the day on which they receive the demand, they may apply in writing to a judge to revoke or vary the demand.

Notice required

(2) The telecommunications service provider may make the application only if, before the application is made, they give notice of their intention to do so to an employee in the manner specified in the demand and to a judge in Form 0.2 of Schedule 2.

No obligation to provide confirmation

(3) The telecommunications service provider is not required to provide the confirmation until a final decision is made with respect to the application.

Revocation or variation of demand

(4) The judge may revoke or vary the demand if satisfied that

(a) it is unreasonable in the circumstances to require the applicant to provide the confirmation; or

(b) provision of the confirmation would disclose information that is privileged or otherwise protected from disclosure by law.

Délai

(3) Le délai prévu dans l'ordre est d'au moins vingt-quatre heures.

Interdiction de divulgation

(4) Le Service peut assortir l'ordre de conditions pour interdire la divulgation de son existence ou de tout ou partie de son contenu.

Obligation de se conformer

(5) Le fournisseur de services de télécommunication est tenu de se conformer à l'ordre. Les contraventions au présent paragraphe sont soustraites à l'application de l'article 126 du *Code criminel*.

Annulation de l'ordre

(6) Le Service peut, à tout moment, annuler l'ordre ou une condition de celui-ci par avis remis au fournisseur de services de télécommunication.

Révocation ou modification de l'ordre de confirmer la fourniture de services

20.23 (1) Le fournisseur de services de télécommunication peut, avant qu'il ne soit tenu de fournir la confirmation requise par un ordre donné en vertu de l'article 20.22 et au plus tard cinq jours ouvrables après la date à laquelle il a reçu l'ordre, demander par écrit à un juge de révoquer ou de modifier l'ordre.

Préavis obligatoire

(2) Le fournisseur de services de télécommunication peut présenter la demande à la condition d'avoir donné un préavis de son intention de le faire à un employé, selon les modalités précisées dans l'ordre, et à un juge, selon le formulaire 0.2 de l'annexe 2.

Aucune obligation de fournir la confirmation

(3) Le fournisseur de services de télécommunication n'a pas à fournir la confirmation tant qu'il n'a pas été statué en dernier ressort sur sa demande.

Révocation ou modification de l'ordre

(4) Le juge peut révoquer l'ordre ou le modifier, s'il est convaincu, selon le cas :

a) qu'il est déraisonnable, dans les circonstances, d'obliger le demandeur à fournir la confirmation;

b) que la fourniture de la confirmation révélerait des renseignements protégés par le droit applicable en matière de divulgation ou de privilèges.

Application for order

20.24 (1) If a telecommunications service provider fails to comply with a confirmation of service demand made under section 20.22, the Director or an employee who is designated by the Director for the purpose may make an application to a judge for an order under this section.

5

Making of order

(2) The judge may order the telecommunications service provider to provide, within the time and in the manner specified in the order, the confirmation referred to in subsection 20.22(1) if the judge is satisfied that the confirmation will assist the Service to perform its duties and functions under section 12 or 16.

10

Measures

(3) The judge may include in the order any measure that they consider necessary in the public interest, including to ensure the confidentiality of the order.

Clarification — voluntary provision of confirmation

20.25 (1) For greater certainty, the Service may request that a telecommunications service provider voluntarily provide the confirmation required by a confirmation of service demand made under section 20.22 or by an order made under section 20.24, without such a demand or such an order having been made, so long as the telecommunications service provider is not prohibited by law from providing the confirmation, and the Service may collect it under section 12 or 16.

15

20

Clarification — other collection authorities

(2) For greater certainty, the fact that a confirmation of service demand may be made under section 20.22 or that an order may be made under section 20.24 does not affect the Service's authority to collect any information under any other provision of this Act.

25

No civil or criminal liability

20.26 No criminal or civil proceedings lie against a telecommunications service provider that voluntarily provides a confirmation following a request from the Service made in the circumstances described in subsection 20.25(1) or against a person acting on behalf of a telecommunications service provider that receives such a request.

30

35

32 (1) Subsections 20.5(1) to (3) of the Act are replaced by the following:

Demande d'ordonnance

20.24 (1) Si le fournisseur de services de télécommunication ne se conforme pas à l'ordre donné en vertu de l'article 20.22, le directeur ou un employé désigné à cette fin par le directeur peut demander à un juge de rendre une ordonnance en conformité avec le présent article.

5

Délivrance de l'ordonnance

(2) Le juge peut ordonner au fournisseur de services de télécommunication de fournir, dans le délai et selon les modalités prévus dans l'ordonnance, la confirmation visée au paragraphe 20.22(1) s'il est convaincu que la confirmation aidera le Service à exercer les fonctions qui lui sont conférées en vertu des articles 12 ou 16.

10

Mesures

(3) Le juge peut prévoir dans l'ordonnance toute mesure qu'il estime nécessaire dans l'intérêt public, notamment afin de garantir la confidentialité de l'ordonnance.

Précision — fourniture volontaire de confirmation

20.25 (1) Il est entendu que le Service peut demander à tout fournisseur de services de télécommunication de fournir volontairement la confirmation qui peut être requise par un ordre de confirmer la fourniture de services donné en vertu de l'article 20.22 ou par une ordonnance rendue en vertu de l'article 20.24 — sans qu'il soit nécessaire de donner un tel ordre ou qu'une telle ordonnance soit rendue — si, d'une part, aucune règle de droit n'interdit au fournisseur de services de télécommunication de la fournir, et si, d'autre part, le Service peut la recueillir en vertu des articles 12 ou 16.

15

20

25

Précision — autres pouvoirs de collecte

(2) Il est entendu qu'un ordre de confirmer la fourniture de services pouvant être donné en vertu de l'article 20.22 ou qu'une ordonnance pouvant être rendue en vertu de l'article 20.24 est sans effet sur la capacité du Service de recueillir toute information en vertu d'une autre disposition de la présente loi.

30

Immunité

20.26 Le fournisseur de services de télécommunication qui fournit volontairement toute confirmation à la suite d'une demande faite par le Service dans les circonstances prévues au paragraphe 20.25(1), et la personne qui agit pour le compte d'un fournisseur de services de télécommunication ayant reçu une telle demande, bénéficie de l'immunité en matière civile ou pénale pour les actes ainsi accomplis.

35

32 (1) Les paragraphes 20.5(1) à (3) de la même loi sont remplacés par ce qui suit :

40

Revocation or variation — sections 20.24 and 20.4

20.5 (1) Before a telecommunications service provider is required to provide a confirmation under an order made under section 20.24, or a person or entity is required to produce any information, record or document under an order made under section 20.4, but no later than 10 business days after the day on which they receive the order, the telecommunications service provider or the person or entity, as the case may be, may apply in writing to a judge to revoke or vary the order.

Notice required

(2) The telecommunications service provider, person or entity may make the application only if, before the application is made, they give notice of their intention to do so to a judge and to an employee in Form 5 of Schedule 2.

No obligation to provide or produce

(3) The telecommunications service provider, person or entity is not required to provide the confirmation or to produce the information, record or document, as the case may be, until a final decision is made with respect to the application.

(2) Paragraphs 20.5(4)(a) and (b) of the Act are replaced by the following:

(a) it is unreasonable in the circumstances to require the applicant to provide the confirmation or produce the information, record or document; or

(b) provision of the confirmation or production of the information, record or document would disclose information that is privileged or otherwise protected from disclosure by law.

33 Section 27 of the Act is replaced by the following:

Making and hearing of applications

27 (1) An application for a judicial authorization under section 11.13, an application for an order under section 20.24, an application under section 20.3 for a preservation order, an application under section 20.4 for a production order, an application under section 21, 21.1, 22.21 or 23 for a warrant, an application under section 22 or 22.1 for the renewal of a warrant or an application for an order under section 22.3 shall be made *ex parte* and heard in private in accordance with regulations made under section 28.

Révocation ou modification — articles 20.24 et 20.4

20.5 (1) Le fournisseur de services de télécommunication qui est tenu de fournir une confirmation requise par une ordonnance rendue en vertu de l'article 20.24 ou la personne ou l'entité qui est tenue de communiquer toute information ou tout document aux termes d'une ordonnance rendue en vertu de l'article 20.4 peut, avant que le fournisseur, la personne ou l'entité ne soit tenu de fournir la confirmation ou de communiquer les informations ou documents et au plus tard dix jours ouvrables après la date à laquelle le fournisseur, la personne ou l'entité a reçu l'ordonnance, demander par écrit à un juge de la révoquer ou de la modifier.

Préavis obligatoire

(2) Le fournisseur de services de télécommunication, la personne ou l'entité peut présenter la demande à la condition d'avoir donné un préavis de son intention à un juge et à un employé selon le formulaire 5 de l'annexe 2.

Aucune obligation de fournir ou de communiquer

(3) Le fournisseur de services de télécommunication, la personne ou l'entité n'a pas à fournir la confirmation ou à communiquer les informations ou documents, selon le cas, tant qu'il n'a pas été statué en dernier ressort sur sa demande.

(2) Les alinéas 20.5(4)a) et b) de la même loi sont remplacés par ce qui suit :

a) qu'il est déraisonnable, dans les circonstances, d'obliger le demandeur à fournir la confirmation ou à communiquer les informations ou documents;

b) que la fourniture de la confirmation ou la communication de toute information révélerait des renseignements protégés par le droit applicable en matière de divulgation ou de privilèges.

33 L'article 27 de la même loi est remplacé par ce qui suit :

Présentation et audition des demandes

27 (1) La demande d'autorisation judiciaire présentée en vertu de l'article 11.13, la demande d'ordonnance présentée en vertu de l'article 20.24, la demande d'ordonnance de préservation présentée en vertu de l'article 20.3 ou d'ordonnance de communication présentée en vertu de l'article 20.4, ou la demande de mandat faite en vertu des articles 21, 21.1, 22.21 ou 23, de renouvellement de mandat faite en vertu des articles 22 ou 22.1 ou d'ordonnance présentée au titre de l'article 22.3 est faite *ex parte* et est entendue à huis clos conformément aux règlements d'application pris en vertu de l'article 28.

Making and hearing of applications — sections 20.23 and 20.5

(2) An application under section 20.23 for the revocation or variation of a confirmation of service demand or under section 20.5 for the revocation or variation of an order made under section 20.24 or a production order shall be made and heard in accordance with regulations made under section 28 and may be heard in private in accordance with those regulations.

34 (1) Paragraph 28(b) of the Act is replaced by the following:

(b) governing the practice and procedure of, and security requirements applicable to, hearings of applications for judicial authorization under section 11.13, for warrants that may be issued under section 21, 21.1, 22.21 or 23, for renewals of those warrants and for orders that may be made under section 20.24, 20.3, 20.4 or 22.3;

(2) Paragraph 28(b.2) of the Act is replaced by the following:

(b.2) governing the practice and procedure of, and security requirements applicable to, the making of applications for the revocation or variation of a confirmation of service demand under section 20.22, an order under section 22.24 or a production order under section 20.5 and hearings of such applications; and

35 Schedule 2 to the Act is amended by adding the following before Form 1:

FORM 0.1

(Subsection 20.22(1))

Confirmation of Service Demand

To (name of person or entity), of

You are required under section 20.22 of the *Canadian Security Intelligence Service Act* to confirm, as soon as possible, but not later than (specify time by which the confirmation is to be provided), whether or not you provide or have provided telecommunication services to (specify subscriber or client, or account or identifier), unless this demand is revoked.

The confirmation must be provided (specify the form and manner).

Présentation et audition d'une demande — articles 20.23 et 20.5

(2) La demande de révocation ou de modification d'un ordre de confirmer la fourniture de services présentée en vertu de l'article 20.23 ou d'une ordonnance rendue en vertu de l'article 20.24 ou d'une ordonnance de communication présentée en vertu de l'article 20.5 est présentée et entendue conformément aux règlements d'application pris en vertu de l'article 28 et peut être entendue à huis clos conformément à ces règlements.

34 (1) L'alinéa 28b) de la même loi est remplacé par ce qui suit :

b) régir la pratique et la procédure, ainsi que les conditions de sécurité, applicables à l'audition des demandes de ces autorisations judiciaires, à celle des demandes de ces mandats ou de renouvellement de mandat ou à celle des demandes d'ordonnance présentées au titre des articles 20.24, 20.3, 20.4 ou 22.3;

(2) L'alinéa 28b.2) de la même loi est remplacé par ce qui suit :

b.2) régir la pratique et la procédure, ainsi que les conditions de sécurité, applicables à la présentation et à l'audition des demandes de révocation ou de modification d'un ordre de confirmer la fourniture de services présentées en vertu de l'article 20.22 ou d'une ordonnance rendue en vertu de l'article 20.24 ou d'une ordonnance de communication présentées en vertu de l'article 20.5;

35 L'annexe 2 de la même loi est modifiée par adjonction, avant le formulaire 1, de ce qui suit :

FORMULAIRE 0.1

(paragraphe 20.22(1))

Ordre de confirmer la fourniture de services

À (nom de la personne ou de l'entité), de

Vous êtes tenu(e) aux termes de l'article 20.22 de la *Loi sur le Service canadien du renseignement de sécurité* de confirmer, dès que possible, mais au plus tard (indiquer l'échéance), si, oui ou non, vous fournissez ou avez fourni des services de télécommunication à (préciser l'abonné, le client, le compte ou l'identifiant), à moins que l'ordre ne soit révoqué.

Les informations doivent être fournies (préciser les modalités).

This demand is subject to the following conditions:
(specify conditions, if any)

You have the right to apply to revoke or vary this confirmation of service demand in accordance with section 20.23 of the *Canadian Security Intelligence Service Act*.

FORM 0.2

(Subsection 20.23(2))

Notice — Application for Revocation or Variation of a Confirmation of Service Demand

FEDERAL COURT

IN THE MATTER OF an application by (*Name*) for the revocation or variation of a confirmation of service demand under section 20.23 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23

NOTICE

This is a notice that (*name of telecommunications service provider named in the confirmation of service demand*) ("the applicant") intends to apply to the Federal Court for the revocation or variation of the confirmation of service demand made on (*date*).

Notice of the applicant's intention has been provided to an employee of the Canadian Security Intelligence Service on (*date*).

The applicant intends to file the application for revocation or variation on or before (*date*).

Dated (*date*), at (*place*).

(*Signature of applicant*)

Le présent ordre est assorti des conditions suivantes :
(préciser les conditions, le cas échéant)

Vous avez le droit de demander la révocation ou la modification du présent ordre conformément à l'article 20.23 de la *Loi sur le Service canadien du renseignement de sécurité*.

FORMULAIRE 0.2

(paragraphe 20.23(2))

Préavis — demande de révocation ou de modification d'un ordre de confirmer la fourniture de services

COUR FÉDÉRALE

DANS L'AFFAIRE d'une demande de révocation ou de modification d'un ordre de confirmer la fourniture de services présentée par (*préciser le nom*) en vertu de l'article 20.23 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23

PRÉAVIS

La présente constitue un préavis de l'intention de (*nom du fournisseur de services de télécommunication visé par l'ordre*), ci-après appelé(e) « le demandeur », de demander la révocation ou la modification de l'ordre de confirmer la fourniture de services donné le (*date*).

Un préavis de l'intention du demandeur a été fourni à un employé du Service canadien du renseignement de sécurité le (*date*).

Le demandeur a l'intention de déposer une demande de révocation ou de modification d'ici le (*date*).

Fait le (*date*), à (*lieu*).

(*Signature du demandeur*)

36 Form 5 of Schedule 2 to the Act is replaced by the following:

36 Le formulaire 5 de l'annexe 2 de la même loi est remplacé par ce qui suit :

FORM 5

(Subsection 20.5(2))

Notice — Application for Revocation or Variation of an Order Under Section 20.24 or a Production Order

(Court File No. — to match order under section 20.24 or production order)

FEDERAL COURT

IN THE MATTER OF an application by (Name) for the revocation or variation of an order under section 20.24 or a production order under section 20.5 of the Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23

NOTICE

This is a notice that (*name of telecommunications service provider, person or entity named in the order*) ("the applicant") intends to apply to the Federal Court for the revocation or variation of the (*specify: order under section 20.24 or production order*) made on (*date*) and received by the applicant on (*date*).

A copy of this notice has been provided to an employee of the Canadian Security Intelligence Service on (*date*).

The applicant intends to file the application for revocation or variation on or before (*date*).

Dated (*date*), at (*place*).

(*Signature of applicant*)

1996, c. 19

Controlled Drugs and Substances Act

37 Section 11 of the *Controlled Drugs and Substances Act* is amended by adding the following after subsection (3):

Computer data

(3.1) Subsections 487(2.1) to (2.3) and (2.5) to (2.9) of the *Criminal Code* apply, with any modifications that the cir-

FORMULAIRE 5

(paragraphe 20.5(2))

Préavis — demande de révocation ou de modification d'une ordonnance rendue en vertu de l'article 20.24 ou d'une ordonnance de communication

(N° du dossier de la Cour — correspondant à celui de l'ordonnance rendue en vertu de l'article 20.24 ou de l'ordonnance de communication)

COUR FÉDÉRALE

DANS L'AFFAIRE d'une demande de révocation ou de modification d'une ordonnance rendue en vertu de l'article 20.24 ou de communication présentée par (*préciser le nom*) en vertu de l'article 20.5 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. (1985), ch. C-23

PRÉAVIS

La présente constitue un préavis de l'intention de (*nom du fournisseur de services de télécommunication, de la personne ou de l'entité visé par l'ordonnance*), ci-après appelé(e) « le demandeur », de demander la révocation ou la modification de (*préciser l'ordonnance rendue en vertu de l'article 20.24 ou l'ordonnance de communication*) rendue le (*date*) et reçue par le demandeur le (*date*).

Une copie de ce préavis a été fournie à un employé du Service canadien du renseignement de sécurité le (*date*).

Le demandeur a l'intention de déposer une demande de révocation ou de modification d'ici le (*date*).

Fait le (*date*), à (*lieu*).

(*Signature du demandeur*)

1996, ch. 19

Loi réglementant certaines drogues et autres substances

37 L'article 11 de la *Loi réglementant certaines drogues et autres substances* est modifié par adjonction, après le paragraphe (3), de ce qui suit :

Données informatiques

(3.1) Les paragraphes 487(2.1) à (2.3) et (2.5) à (2.9) du *Code criminel* s'appliquent, avec les adaptations néces-

circumstances require, with respect to a warrant issued under subsection (1).

2018, c. 16

Cannabis Act

38 Section 87 of the *Cannabis Act* is amended by adding the following after subsection (3):

Computer data

(3.1) Subsections 487(2.1) to (2.3) and (2.5) to (2.9) of the *Criminal Code* apply, with any modifications that the circumstances require, with respect to a warrant issued under subsection (1).

Coordinating Amendments

Bill C-16

39 (1) Subsections (2) to (4) apply if Bill C-16, introduced in the 1st session of the 45th Parliament and entitled the *Protecting Victims Act* (in this section referred to as the “other Act”), receives royal assent.

(2) If section 43 of the other Act comes into force before section 17 of this Act, then that section 17 is repealed.

(3) If section 17 of this Act comes into force before section 43 of the other Act, then that section 43 is repealed.

(4) If section 43 of the other Act and section 17 of this Act come into force on the same day, then that section 17 is deemed never to have come into force and is repealed.

Coming into Force

180th day after royal assent

40 This Part, other than section 39, comes into force on the 180th day after the day on which this Act receives royal assent.

saires, à l'égard du mandat délivré en vertu du paragraphe (1).

2018, ch. 16

Loi sur le cannabis

38 L'article 87 de la *Loi sur le cannabis* est modifié par adjonction, après le paragraphe (3), de ce qui suit :

Données informatiques

(3.1) Les paragraphes 487(2.1) à (2.3) et (2.5) à (2.9) du *Code criminel* s'appliquent, avec les adaptations nécessaires, à l'égard du mandat délivré en vertu du paragraphe (1).

Dispositions de coordination

Projet de loi C-16

39 (1) Les paragraphes (2) à (4) s'appliquent en cas de sanction du projet de loi C-16, déposé au cours de la 1^{re} session de la 45^e législature et intitulé *Loi visant à protéger les victimes* (appelé « autre loi » au présent article).

(2) Si l'article 43 de l'autre loi entre en vigueur avant l'article 17 de la présente loi, cet article 17 est abrogé.

(3) Si l'article 17 de la présente loi entre en vigueur avant l'article 43 de l'autre loi, cet article 43 est abrogé.

(4) Si l'entrée en vigueur de l'article 43 de l'autre loi et celle de l'article 17 de la présente loi sont concomitantes, cet article 17 est réputé ne pas être entré en vigueur et est abrogé.

Entrée en vigueur

Cent quatre-vingtième jour suivant la sanction

40 La présente partie, à l'exception de l'article 39, entre en vigueur le cent quatre-vingtième jour suivant la date de la sanction de la présente loi.

PART 2

Supporting Authorized Access to Information Act

Enactment of Act

Enactment

41 The *Supporting Authorized Access to Information Act*, whose text is as follows and whose schedule is set out in the schedule to this Act, is enacted:

An Act respecting the obligations of electronic service providers in relation to authorized access to information

Short Title

Short title

1 This Act may be cited as the *Supporting Authorized Access to Information Act*.

Interpretation

Definitions

2 (1) The following definitions apply in this Act.

access, in relation to information, includes obtaining a document containing information and, with respect to information related to a communication, intercepting the communication within the meaning of section 183 of the *Criminal Code*. (*accès*)

authorized person means a person having authority under the *Criminal Code* or the *Canadian Security Intelligence Service Act* to access information. (*personne autorisée*)

core provider means an electronic service provider belonging to a class of electronic service providers set out in the schedule. (*fournisseur principal*)

electronic protection means authentication, encryption and any other prescribed type of data protection. (*protection électronique*)

electronic service means a service, or a feature of a service, that involves the creation, recording, storage, processing, transmission, reception, emission or making available of information in electronic, digital or any other

PARTIE 2

Loi sur le soutien en matière d'accès autorisé à de l'information

Édiction de la loi

Édiction

41 Est édictée la *Loi sur le soutien en matière d'accès autorisé à de l'information*, dont le texte suit et dont l'annexe figure à l'annexe de la présente loi :

Loi concernant les obligations des fournisseurs de services électroniques en matière d'accès autorisé à de l'information

Titre abrégé

Titre abrégé

1 *Loi sur le soutien en matière d'accès autorisé à de l'information*.

Définitions et interprétation

Définitions

2 (1) Les définitions qui suivent s'appliquent à la présente loi.

accès À l'égard d'information, s'entend notamment de l'obtention de documents contenant de l'information et, s'agissant d'information concernant des communications, de l'interception, au sens de l'article 183 du *Code criminel*, des communications. (*access*)

fournisseur de services électroniques Personne qui, seule ou au titre de son appartenance à un groupe, fournit des services électroniques, notamment en vue de permettre la communication, et qui, selon le cas :

a) fournit ces services à des personnes se trouvant au Canada;

b) exerce tout ou partie de ses activités commerciales au Canada. (*electronic service provider*)

fournisseur principal Fournisseur de services électroniques qui appartient à l'une des catégories de fournisseurs de services électroniques figurant à l'annexe. (*core provider*)

intangible form by an electronic, digital, magnetic, optical, biometric, acoustic or other technological means, or a combination of any such means. (*service électronique*)

electronic service provider means a person that, individually or as part of a group, provides an electronic service, including for the purpose of enabling communications, and that

(a) provides the service to persons in Canada; or

(b) carries on all or part of its business activities in Canada. (*fournisseur de services électroniques*)

information includes any information, intelligence or data to which access may be authorized under the *Criminal Code* or the *Canadian Security Intelligence Service Act*. (*information*)

Minister means the Minister of Public Safety and Emergency Preparedness. (*ministre*)

person includes a corporation, a trust, a partnership, a fund, a joint venture, a government, a government agency, an unincorporated association or organization and any other legal entity. (*personne*)

prescribed means prescribed by the regulations. (*Version anglaise seulement*)

systemic vulnerability means a vulnerability in the electronic protections of an electronic service that creates a substantial risk that secure information could be accessed by a person who does not have any right or authority to do so. (*vulnérabilité systémique*)

Preservation of existing authorities

(2) Nothing in this Act derogates from any authority to access information conferred under the *Criminal Code* or the *Canadian Security Intelligence Service Act* — or from any similar authority conferred under another Act of Parliament — or from any corresponding obligation imposed on an electronic service provider to assist in a person's exercise of such an authority.

Preservation of agreements and arrangements

(3) Nothing in this Act derogates from any agreement or arrangement between an electronic service provider and a national security or law enforcement agency with re-

information S'entend notamment de toute information, de tout renseignement ou de toute donnée auquel l'accès peut être autorisé sous le régime du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité*. (*information*)

ministre Le ministre de la Sécurité publique et de la Protection civile. (*Minister*)

personne S'entend notamment d'une personne morale, d'une fiducie, d'une société de personnes, d'un fonds, d'une coentreprise, d'une administration, d'un organisme public, d'une association ou d'une organisation non dotée de la personnalité morale ou de toute autre entité juridique. (*person*)

personne autorisée Personne qui est autorisée, sous le régime du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité*, à accéder à de l'information. (*authorized person*)

protection électronique Authentification, chiffrement ou tout autre type de protection de données prévu par règlement. (*electronic protection*)

service électronique Tout service — ou fonctionnalité d'un service — qui implique la création, l'enregistrement, le stockage, le traitement, la transmission, la réception, la diffusion ou la mise à disposition d'information sous toute forme immatérielle, notamment électronique ou numérique, par tout moyen technologique — électronique, numérique, magnétique, optique, biométrique, acoustique ou autre — ou par une combinaison de tels moyens. (*electronic service*)

vulnérabilité systémique Toute vulnérabilité dans les protections électroniques d'un service électronique qui crée un risque sérieux qu'une personne puisse accéder à de l'information sécurisée sans en avoir le droit ou l'autorisation. (*systemic vulnerability*)

Maintien des pouvoirs existants

(2) La présente loi n'a pas pour effet de porter atteinte aux pouvoirs d'accéder à de l'information conférés sous le régime du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité* — ou à tout pouvoir similaire conféré sous le régime de toute autre loi fédérale — ni aux obligations correspondantes qui incombent aux fournisseurs de services électroniques de prêter assistance à la personne qui exerce de tels pouvoirs.

Maintien des accords ou ententes

(3) La présente loi n'a pas pour effet de porter atteinte aux accords ou ententes conclus entre un fournisseur de services électroniques et un organisme chargé de la sécu-

spect to assistance to be provided to an authorized person in the exercise of the person's authority to access information, nor prevents entry into such an agreement or arrangement.

Purpose

Purpose

3 The purpose of this Act is to ensure that electronic service providers can facilitate the exercise of authorities to access information that are conferred on authorized persons.

His Majesty

Binding on His Majesty

4 This Act is binding on His Majesty in right of Canada or of a province.

Core Providers

Core providers — classes

5 (1) The Governor in Council may, by regulation, amend the schedule by adding, amending or deleting a class of electronic service providers.

Core providers — obligations

(2) The Governor in Council may make regulations respecting the obligations of core providers, including regulations respecting

(a) the development, implementation, assessment, testing and maintenance of operational and technical capabilities, including capabilities related to extracting and organizing information that is authorized to be accessed and to providing access to such information to authorized persons;

(b) the installation, use, operation, management, assessment, testing and maintenance of any device, equipment or other thing that may enable an authorized person to access information;

(c) notices to be given to the Minister or other persons, including with respect to any capability referred to in paragraph (a) and any device, equipment or other thing referred to in paragraph (b); and

(d) the retention of categories of metadata — including *transmission data*, as defined in section 487.011 of the *Criminal Code* — for reasonable periods of time not exceeding one year.

rité nationale ou du contrôle d'application des lois relativement à l'assistance à prêter à la personne autorisée dans l'exercice de ses pouvoirs d'accéder à de l'information. Elle n'a pas non plus pour effet de prévenir la conclusion de tels accords ou ententes.

Objet

Objet

3 La présente loi a pour objet de faire en sorte que les fournisseurs de services électroniques puissent faciliter l'exercice des pouvoirs d'accès à de l'information qui sont conférés aux personnes autorisées.

Sa Majesté

Obligation de Sa Majesté

4 La présente loi lie Sa Majesté du chef du Canada ou d'une province.

Fournisseurs principaux

Fournisseurs principaux : catégories

5 (1) Le gouverneur en conseil peut, par règlement, modifier l'annexe pour ajouter, modifier ou supprimer une catégorie de fournisseurs de services électroniques.

Fournisseurs principaux : obligations

(2) Le gouverneur en conseil peut prendre des règlements concernant les obligations incombant aux fournisseurs principaux, notamment des règlements concernant :

a) l'élaboration, la mise en œuvre, l'évaluation, la mise à l'essai et le maintien de leurs capacités opérationnelles et techniques, notamment en ce qui touche l'extraction et l'organisation de l'information à laquelle l'accès est autorisé et l'accès à celle-ci par les personnes autorisées;

b) l'installation, l'utilisation, le fonctionnement, la gestion, l'évaluation, la mise à l'essai et l'entretien de tout dispositif ou équipement ou de toute autre chose pouvant permettre à la personne autorisée d'accéder à de l'information;

c) les avis à donner au ministre ou à toute autre personne, notamment en ce qui concerne toute capacité visée à l'alinéa a) et tout dispositif ou équipement ou toute autre chose visé à l'alinéa b);

d) la conservation de catégories de métadonnées — y compris des *données de transmission*, au sens de

l'article 487.011 du *Code criminel* — pour des périodes raisonnables d'au plus un an.

Factors

(3) In making a regulation under subsection (2), the Governor in Council must take into account the following factors:

- (a) the benefits of the regulation to the administration of justice, in particular to investigations under the *Criminal Code*, and to the exercise of powers and the performance of duties and functions under the *Canadian Security Intelligence Service Act*; 5
- (b) the feasibility of compliance with the regulation for the core providers; 10
- (c) the costs to be incurred by the core providers to ensure compliance with the regulation;
- (d) the potential impact of the regulation on the persons to whom the core providers provide services;
- (e) the potential impact of the regulation on privacy protection and cybersecurity; and 15
- (f) any other factor that the Governor in Council considers relevant.

Restrictions

(4) Paragraph (2)(d) does not authorize the making of regulations that require core providers to retain information that would reveal 20

- (a) the content — that is to say the substance, meaning or purpose — of information transmitted in the course of an electronic service;
- (b) a person's web browsing history; or 25
- (c) a person's social media activities.

Systemic vulnerability

(5) A core provider is not required to comply with a provision of a regulation made under subsection (2), with respect to an electronic service, if compliance with that provision would require the provider to introduce a systemic vulnerability related to that service or prevent the provider from rectifying such a vulnerability. 30

Temporary exemption

6 (1) On application by a core provider, the Minister may, by order and on any terms that the Minister considers necessary, exempt the core provider, for a specified 35

Facteurs

(3) Au moment de prendre un règlement en vertu du paragraphe (2), le gouverneur en conseil tient compte des facteurs suivants : 5

- a) les avantages du règlement quant à l'administration de la justice — notamment pour les enquêtes menées sous le régime du *Code criminel* — et l'exercice des attributions conférées sous le régime de la *Loi sur le Service canadien du renseignement de sécurité*; 10
- b) la mesure dans laquelle les fournisseurs principaux peuvent se conformer au règlement;
- c) les frais à engager par les fournisseurs principaux pour se conformer au règlement;
- d) les effets possibles du règlement sur les personnes auxquelles les fournisseurs principaux fournissent des services; 15
- e) les effets possibles du règlement sur la protection de la vie privée et la cybersécurité;
- f) tout autre facteur que le gouverneur en conseil estime pertinent. 20

Restrictions

(4) L'alinéa (2)d) ne permet pas la prise de règlements qui obligent les fournisseurs principaux à conserver de l'information qui révélerait, selon le cas : 25

- a) le contenu — c'est-à-dire la substance, le sens ou l'objet — d'information transmise dans le cadre de services électroniques; 25
- b) l'historique de navigation Web d'une personne;
- c) les activités d'une personne sur les médias sociaux.

Vulnérabilité systémique

(5) Le fournisseur principal n'est pas tenu de se conformer à la disposition d'un règlement pris en vertu du paragraphe (2), à l'égard d'un service électronique, si le fait de s'y conformer l'obligerait à introduire une vulnérabilité systémique liée à ce service ou l'empêcherait de corriger une telle vulnérabilité. 30 35

Exemption temporaire

6 (1) Sur demande du fournisseur principal, le ministre peut, par arrêté, exempter celui-ci, aux conditions qu'il estime nécessaires et pour une période déterminée, de

period, from the application of any provision of a regulation made under subsection 5(2).

Application

(2) The application must be submitted in the form and manner specified by the Minister and must contain

- (a) the provision with respect to which the exemption is sought; 5
- (b) a proposed period for the exemption;
- (c) a rationale explaining why the core provider requires the exemption;
- (d) a plan setting out the measures that the core provider intends to take to comply with the provision within the period referred to in paragraph (b); and 10
- (e) any other information specified by the Minister.

Pending application

(3) The provision with respect to which the exemption is sought does not apply to the core provider pending the determination of the application. 15

Decision

(4) As soon as feasible after the application is submitted, the Minister must make a decision in respect of it and give written notice of the decision to the core provider.

Denial of application

(5) In a decision to deny the application, the Minister may specify the day by which the core provider must comply with the provision with respect to which the application was denied. 20

Statutory Instruments Act

(6) The *Statutory Instruments Act* does not apply to an order made under subsection (1). 25

Ministerial Orders

Order

7 (1) Subject to section 8, the Minister may make an order with respect to an electronic service provider and the order may contain any provision that may be contained in a regulation made under subsection 5(2), whether or not the provider is a core provider. The order must specify the period during which it has effect. 30

l'application de toute disposition des règlements pris en vertu du paragraphe 5(2).

Demande

(2) La demande est présentée selon les modalités que fixe le ministre et contient :

- a) la disposition visée; 5
- b) la période d'exemption proposée;
- c) les motifs à l'appui de la demande;
- d) un plan prévoyant les mesures que le fournisseur principal a l'intention de prendre pour se conformer à la disposition avant l'expiration de la période visée à l'alinéa b); 10
- e) tout autre renseignement précisé par le ministre.

Demande en traitement

(3) La disposition visée ne s'applique pas au fournisseur principal pendant que sa demande est en traitement.

Décision

(4) Dès que possible après la présentation de la demande, le ministre rend sa décision et en donne un avis écrit au fournisseur principal. 15

Demande rejetée

(5) Dans sa décision de rejeter la demande, le ministre peut inclure le délai accordé au fournisseur principal pour se conformer à la disposition en question. 20

Loi sur les textes réglementaires

(6) La *Loi sur les textes réglementaires* ne s'applique pas aux arrêtés pris en vertu du paragraphe (1). 25

Arrêtés ministériels

Arrêté

7 (1) Sous réserve de l'article 8, le ministre peut prendre, à l'égard d'un fournisseur de services électroniques, que celui-ci soit un fournisseur principal ou non, un arrêté pouvant comporter toute disposition que peut contenir un règlement pris en vertu du paragraphe 5(2) et y précise la période de validité de l'arrêté. 25

Approval of Intelligence Commissioner

(2) The order is valid when — if it is approved by the Intelligence Commissioner under paragraph 20(1)(a) of the *Intelligence Commissioner Act* — the Intelligence Commissioner provides the Minister with the written decision approving the order.

5

Factors

(3) In making the order, the Minister must take into account the following factors:

- (a) the benefits of the order to the administration of justice, in particular to investigations under the *Criminal Code*, and to the exercise of powers and the performance of duties and functions under the *Canadian Security Intelligence Service Act*; 10
- (b) the feasibility of compliance with the order for the electronic service provider;
- (c) the costs to be incurred by the electronic service provider to ensure compliance with the order; 15
- (d) the potential impact of the order on the persons to whom the electronic service provider provides services;
- (e) the potential impact of the order on privacy protection and cybersecurity; and 20
- (f) any other factor that the Minister considers relevant.

Discretionary compensation

(4) For the purpose of offsetting all or part of the costs referred to in paragraph (3)(c), in the order, the Minister may provide for compensation to be paid to the electronic service provider in an amount that the Minister considers appropriate and may include provisions with respect to the time and manner of payment. 25

Systemic vulnerability

(5) The electronic service provider is not required to comply with a provision of the order, with respect to an electronic service, if compliance with that provision would require the provider to introduce a systemic vulnerability related to that service or prevent the provider from rectifying such a vulnerability. 30 35

Statutory Instruments Act

(6) The *Statutory Instruments Act* does not apply to an order made under subsection (1).

Approbation du commissaire au renseignement

(2) L'arrêté est valide au moment où, dans le cas où le commissaire au renseignement approuve l'arrêté au titre de l'alinéa 20(1)a) de la *Loi sur le commissaire au renseignement*, il fournit une décision écrite en ce sens au ministre.

5

Facteurs

(3) Au moment de prendre l'arrêté, le ministre tient compte des facteurs suivants :

- a) les avantages de l'arrêté pour l'administration de la justice — notamment pour les enquêtes menées sous le régime du *Code criminel* — et quant à l'exercice des attributions conférées sous le régime de la *Loi sur le Service canadien du renseignement de sécurité*; 10
- b) la mesure dans laquelle le fournisseur de services électroniques peut se conformer à l'arrêté;
- c) les frais à engager par le fournisseur de services électroniques pour se conformer à l'arrêté; 15
- d) les effets possibles de l'arrêté sur les personnes auxquelles le fournisseur de services électroniques fournit des services;
- e) les effets possibles de l'arrêté sur la protection de la vie privée et la cybersécurité; 20
- f) tout autre facteur que le ministre estime pertinent.

Indemnité discrétionnaire

(4) Afin de compenser, en tout ou en partie, les frais visés à l'alinéa (3)c), le ministre peut, dans l'arrêté, prévoir le versement d'une indemnité qu'il estime raisonnable au fournisseur de services électroniques ainsi que toute disposition concernant le délai et les modalités du versement. 25

Vulnérabilité systémique

(5) Le fournisseur de services électroniques n'est pas tenu de se conformer à la disposition de l'arrêté le concernant, à l'égard d'un service électronique, si le fait de s'y conformer l'obligerait à introduire une vulnérabilité systémique liée à ce service électronique ou l'empêcherait de corriger une telle vulnérabilité. 30 35

Loi sur les textes réglementaires

(6) La *Loi sur les textes réglementaires* ne s'applique pas aux arrêtés pris en vertu du paragraphe (1). 35

Representations

8 Before making an order under subsection 7(1), the Minister must provide the electronic service provider with an opportunity to make representations.

Intelligence Commissioner

9 (1) The Minister must provide a copy of any order made under subsection 7(1) to the Intelligence Commissioner for the purposes of the Intelligence Commissioner's review and approval under the *Intelligence Commissioner Act*.

Notice

(2) The copy of the order constitutes notice of the order for the purposes of calculating the time limit referred to in paragraph 20(3)(b) of the *Intelligence Commissioner Act*.

Duration

10 (1) Unless revoked, an order made under subsection 7(1) has effect for the period specified in the order.

Non-application

(2) Subsection 7(2) and sections 8 and 9 do not apply in respect of an order that only revokes another order made under subsection 7(1) or only extends the period specified in another order made under subsection 7(1).

Review

11 (1) Before the order expires, the Minister must review the order to determine whether, taking into account the factors referred to in subsection 7(3), the period specified in it should be extended.

New information

(2) Before the order expires, an electronic service provider subject to it may submit to the Minister any information that is relevant to the review.

Compliance with order

12 An electronic service provider that is subject to an order made under subsection 7(1) must comply with it.

Order prevails

13 An order made under subsection 7(1) prevails over any regulation made under subsection 5(2) to the extent of any inconsistency.

Observations

8 Avant de prendre l'arrêté en vertu du paragraphe 7(1), le ministre donne au fournisseur de services électroniques la possibilité de présenter ses observations.

Commissaire au renseignement

9 (1) Le ministre fournit au commissaire au renseignement une copie de tout arrêté qu'il prend en vertu du paragraphe 7(1) aux fins d'examen et d'approbation par ce dernier en application de la *Loi sur le commissaire au renseignement*.

Avis

(2) La copie de l'arrêté constitue l'avis de l'arrêté aux fins du calcul du délai visé à l'alinéa 20(3)b) de la *Loi sur le commissaire au renseignement*.

Période de validité

10 (1) L'arrêté pris en vertu du paragraphe 7(1) est valide pour la période qui y est précisée, sauf révocation.

Non-application

(2) Le paragraphe 7(2) et les articles 8 et 9 ne s'appliquent pas à l'arrêté qui n'a pour effet que de révoquer un autre arrêté pris en vertu du paragraphe 7(1) ou d'en prolonger la période de validité.

Examen

11 (1) Avant l'expiration de l'arrêté, le ministre examine celui-ci afin de déterminer si, compte tenu des facteurs prévus au paragraphe 7(3), il devrait en prolonger la période de validité.

Nouvelle information

(2) Avant l'expiration de l'arrêté, le fournisseur de services électroniques qui y est visé peut présenter au ministre toute nouvelle information qui est pertinente pour l'examen.

Obligation de conformité

12 Le fournisseur de services électroniques visé par l'arrêté pris en vertu du paragraphe 7(1) est tenu de s'y conformer.

Incompatibilité

13 L'arrêté pris en vertu du paragraphe 7(1) l'emporte sur tout règlement incompatible pris en vertu du paragraphe 5(2).

Obligation to Assist

Obligation to assist

14 (1) On request made by the Minister, an electronic service provider must provide all reasonable assistance to a person or class of persons specified in the request to permit the assessment or testing of any device, equipment or other thing that may enable an authorized person to access information. 5

Persons to be assisted

(2) Only the following persons or classes of persons may receive assistance:

- (a)** the Minister;
- (b)** an employee of the Canadian Security Intelligence Service; 10
- (c)** a person appointed or employed under Part I of the *Royal Canadian Mounted Police Act* or a civilian employee referred to in section 10 of that Act;
- (d)** a civilian employee of another police force; 15
- (e)** a *peace officer*, as defined in section 2 of the *Criminal Code*.

Request

(3) The request must be in writing and set out the purpose of the assessment or testing and any limits and conditions that the Minister considers appropriate. 20

For greater certainty

(4) For greater certainty, the assessment or testing must not have the effect of granting access to personal information.

Confidentiality

Prohibition on disclosure

15 An electronic service provider and any person acting on its behalf must not disclose any of the following information except as permitted under this Act or the *Canada Evidence Act*: 25

- (a)** information contained in an order made under subsection 6(1) or 7(1);
- (b)** information on which the Minister relied in making the order; 30

Obligation de prêter assistance

Obligation de prêter assistance

14 (1) Le fournisseur de services électroniques est tenu, sur demande du ministre, de prêter toute assistance raisonnable à la personne ou catégorie de personnes précisée dans la demande pour permettre l'évaluation ou la mise à l'essai de tout dispositif ou équipement ou de toute autre chose pouvant permettre à la personne autorisée d'accéder à de l'information. 5

Personnes recevant de l'assistance

(2) Seules les personnes ou catégories de personnes ci-après peuvent recevoir de l'assistance :

- a)** le ministre; 10
- b)** tout employé du Service canadien du renseignement de sécurité;
- c)** toute personne nommée ou employée sous le régime de la partie I de la *Loi sur la Gendarmerie royale du Canada* ou tout membre du personnel civil visé à l'article 10 de cette loi; 15
- d)** tout membre du personnel civil d'une autre force policière;
- e)** tout *agent de la paix*, au sens de l'article 2 du *Code criminel*. 20

Demande

(3) La demande est présentée par écrit et précise l'objet de l'évaluation ou de la mise à l'essai ainsi que les restrictions et conditions que le ministre estime indiquées.

Précision

(4) Il est entendu que l'évaluation ou la mise à l'essai ne peut avoir pour effet de permettre l'accès à des renseignements personnels. 25

Confidentialité

Communication interdite

15 Sauf dans la mesure permise sous le régime de la présente loi ou de la *Loi sur la preuve au Canada*, il est interdit au fournisseur de services électroniques et à toute personne agissant en son nom de communiquer : 30

- a)** l'information contenue dans un arrêté pris en vertu des paragraphes 6(1) ou 7(1);
- b)** l'information sur laquelle le ministre s'est fondé pour prendre l'arrêté;

(c) the fact that the electronic service provider is subject to the order;

(d) information provided in the course of representations made under section 8 or in any response given by the Minister and the fact that the Minister has invited the representations; 5

(e) information contained in an application referred to in subsection 6(1) or in a decision made under subsection 6(4);

(f) information submitted under subsection 11(2) and any information received from the Minister in response; 10

(g) any prescribed information.

Confidential information

16 The following information is confidential and must, subject to the regulations, be treated accordingly by a person designated under subsection 19(1): 15

(a) information obtained by the designated person in the course of exercising their powers or performing their duties and functions under sections 20 and 21; and 20

(b) information contained in an audit report referred to in section 23.

Judicial review — notice to Minister

17 (1) An electronic service provider is not to make an application for judicial review in respect of an order or decision made under this Act unless, at least 15 days before making the application, it provides written notice to the Minister, including a copy of the notice of application. 25

For greater certainty

(2) For greater certainty, the Federal Court has exclusive jurisdiction to hear applications for judicial review in respect of any order or decision made under this Act. 30

Regulations — confidentiality and security

18 The Governor in Council may make regulations respecting confidentiality and security requirements with which electronic service providers and persons acting on their behalf must comply, including regulations 35

(a) respecting the disclosure of information referred to in section 15 or 16;

c) le fait que le fournisseur de services électroniques est assujéti à l'arrêté;

d) l'information contenue dans les observations présentées au titre de l'article 8 ou dans toute réponse du ministre à celles-ci et le fait que le ministre a donné la possibilité au fournisseur de les présenter; 5

e) l'information contenue dans une demande visée au paragraphe 6(1) ou dans une décision rendue au titre du paragraphe 6(4);

f) l'information présentée au titre du paragraphe 11(2) et toute information communiquée par le ministre en réponse; 10

g) toute autre information prévue par règlement.

Information confidentielle

16 L'information ci-après est confidentielle et doit être traitée comme telle, sous réserve des règlements, par toute personne désignée en vertu du paragraphe 19(1) : 15

a) celle obtenue par la personne désignée dans l'exercice des attributions qui lui sont conférées par les articles 20 et 21;

b) celle contenue dans le rapport visé à l'article 23. 20

Contrôle judiciaire : préavis

17 (1) Le fournisseur de services électroniques ne peut présenter une demande de contrôle judiciaire à l'égard d'un arrêté pris ou d'une décision rendue sous le régime de la présente loi que si, au moins quinze jours avant la date de la présentation de sa demande, il en avise le ministre par écrit et lui fournit une copie de l'avis de demande. 25

Précision

(2) Il est entendu que la Cour fédérale a compétence exclusive pour connaître des demandes de contrôle judiciaire visant tout arrêté pris ou toute décision rendue sous le régime de la présente loi. 30

Règlements : confidentialité et sécurité

18 Le gouverneur en conseil peut prendre des règlements concernant les exigences en matière de confidentialité et de sécurité auxquelles les fournisseurs de services électroniques et toute personne agissant en leur nom doivent se conformer, notamment des règlements : 35

a) concernant la communication d'information visée aux articles 15 ou 16;

(b) establishing rules of procedure for the protection of information referred to in section 15 or 16 in administrative or judicial proceedings;

(c) respecting requirements related to employees of electronic service providers and other persons whose services may be engaged by electronic service providers — who participate in activities in relation to requests for access to information that is authorized under the *Criminal Code* or the *Canadian Security Intelligence Service Act* or in relation to compliance with this Act — including with respect to their security clearance and location; and

(d) respecting security requirements with respect to the facilities and premises of electronic service providers that are used for storing, processing or transmitting information that is related to — or that may be the subject of — requests for access to information that is authorized under the *Criminal Code* or the *Canadian Security Intelligence Service Act*.

b) établissant des règles de procédures applicables à la protection d'information visée aux articles 15 ou 16 dans le cadre de procédures administratives ou judiciaires;

c) concernant les exigences applicables aux employés des fournisseurs de services électroniques — ainsi qu'à toute autre personne dont les services sont retenus par des fournisseurs de services électroniques — qui participent à des activités liées à une demande d'accès à de l'information autorisé sous le régime du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité* ou au respect de la présente loi, notamment en ce qui concerne leur habilitation de sécurité et de leur emplacement;

d) concernant les exigences en matière de sécurité relatives aux installations et locaux des fournisseurs de services électroniques qui sont utilisés pour le stockage, le traitement ou la transmission d'information faisant l'objet d'une demande d'accès à de l'information autorisé sous le régime du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité*, ou qui s'y rapporte.

Administration and Enforcement

Designation

Designation

19 (1) The Minister may, subject to any restrictions or conditions that the Minister may specify, designate persons or classes of persons for the purposes of the administration and enforcement of this Act.

Certificate

(2) The Minister must provide every designated person with a certificate attesting to their designation.

Inspections

Authority to enter place

20 (1) Subject to subsection 21(1), a designated person may, for the purpose of verifying compliance or preventing non-compliance with this Act, at any reasonable time enter any place if they have reasonable grounds to believe that anything relevant to that purpose, including any document or electronic data, is located in that place or that an activity regulated by this Act is conducted in that place.

Exécution et contrôle d'application

Désignation

Désignation

19 (1) Le ministre peut, sous réserve des restrictions et conditions qu'il précise, désigner toute personne — à titre individuel ou au titre de son appartenance à une catégorie — pour l'exécution et le contrôle d'application de la présente loi.

Certificat

(2) Il fournit à chaque personne désignée un certificat attestant sa qualité.

Inspections

Accès au lieu

20 (1) Sous réserve du paragraphe 21(1), la personne désignée peut, à toute fin liée à la vérification du respect ou à la prévention du non-respect de la présente loi, entrer dans tout lieu, à toute heure convenable, si elle a des motifs raisonnables de croire que s'y trouve une chose, notamment tout document ou toute donnée électronique, pertinente à cette fin ou que s'y déroule une activité régie par la présente loi.

Production of certificate

(2) On entering a place referred to in subsection (1), the designated person must, on request, produce the certificate attesting to their designation to the person in charge of the place.

Powers on entry

(3) The designated person may, for a purpose referred to in subsection (1),

- (a) examine anything found in the place, including any document or electronic data;
- (b) make copies of any document or electronic data that is found in the place or take extracts from the document or electronic data;
- (c) remove any document found in the place for examination or copying;
- (d) use or cause to be used any computer or data processing system at the place to examine or copy electronic data; and
- (e) use or cause to be used any copying equipment at the place to make copies of any document.

Return of items

(4) If the designated person removes a document under paragraph (3)(c), they must return it to its owner or the person in charge of it on completion of the examination or copying.

Duty to assist

(5) Every owner or person in charge of a place that is entered by the designated person and every person found in the place must give all assistance that is reasonably required to enable the designated person to exercise their powers or perform their duties and functions under this section and provide the designated person with any document or electronic data that they may reasonably require.

Persons accompanying

(6) The designated person may be accompanied by any other person that the designated person believes is necessary to help them exercise their powers or perform their duties and functions under this section.

Entering private property

(7) The designated person and any person accompanying them may enter and pass through private property, other than a dwelling-house on that property, to gain entry to a place referred to in subsection (1). For greater certainty, they are not liable for doing so.

Production du certificat

(2) Elle présente, sur demande, le certificat attestant sa qualité au responsable du lieu dans lequel elle entre.

Autres pouvoirs

(3) Elle peut, à toute fin prévue au paragraphe (1) :

- a) examiner toute chose, notamment tout document ou toute donnée électronique, se trouvant dans le lieu;
- b) reproduire, en tout ou en partie, tout document ou toute donnée électronique se trouvant dans le lieu;
- c) emporter, pour examen ou reproduction, tout document se trouvant dans le lieu;
- d) utiliser ou faire utiliser, pour examen ou reproduction de données électroniques, tout ordinateur ou système informatique se trouvant dans le lieu;
- e) utiliser ou faire utiliser, pour reproduction de documents, tout appareil de reproduction se trouvant dans le lieu.

Restitution

(4) Les documents emportés en vertu de l'alinéa (3)c) sont restitués à leur propriétaire ou à la personne qui en est responsable au terme de l'examen ou de la reproduction.

Assistance

(5) Le propriétaire ou le responsable du lieu ainsi que quiconque s'y trouve sont tenus de prêter à la personne désignée toute l'assistance qu'elle peut valablement exiger pour lui permettre d'exercer ses attributions au titre du présent article et de lui fournir tout document ou toute donnée électronique qu'elle peut valablement exiger.

Accompagnement

(6) La personne désignée peut être accompagnée des personnes qu'elle estime nécessaires pour l'aider dans l'exercice de ses attributions au titre du présent article.

Droit de passage sur une propriété privée

(7) La personne désignée et toute personne l'accompagnant peuvent, afin d'accéder au lieu visé au paragraphe (1), pénétrer dans une propriété privée — à l'exclusion de toute maison d'habitation — et y circuler. Il est entendu

Dwelling-house

21 (1) In the case of a dwelling-house, a designated person is not authorized to enter it without the occupant's consent except under the authority of a warrant issued under subsection (2).

Authority to issue warrant

(2) A justice of the peace may, on *ex parte* application, issue a warrant authorizing the designated person named in it to enter a dwelling-house, subject to any conditions specified in the warrant, if the justice of the peace is satisfied by information on oath that

- (a)** the dwelling-house is a place referred to in subsection 20(1);
- (b)** entry to the dwelling-house is necessary for a purpose referred to in subsection 20(1); and
- (c)** entry was refused by the occupant or there are reasonable grounds to believe that entry will be refused by, or that consent to entry cannot be obtained from, the occupant.

Use of force

(3) In executing the warrant, the designated person is not entitled to use force unless the use of force is specifically authorized in the warrant and they are accompanied by a peace officer.

Internal Audit

Audit order

22 (1) Subject to the regulations, a designated person may, for a purpose related to verifying compliance or preventing non-compliance with this Act, make an order in writing requiring an electronic service provider to conduct, within the time and in the manner specified in the order, an internal audit of its practices, documents and electronic data to determine whether it is in compliance with any provision of this Act or the regulations.

Statutory Instruments Act

(2) The *Statutory Instruments Act* does not apply to an order made under subsection (1).

Compliance with order

23 The electronic service provider must comply with the order and provide to the designated person, within the

que ces personnes ne peuvent encourir de poursuites à cet égard.

Maison d'habitation

21 (1) Dans le cas d'une maison d'habitation, la personne désignée ne peut toutefois y entrer sans le consentement de l'occupant que si elle est munie du mandat décerné en vertu du paragraphe (2).

Délivrance du mandat

(2) Sur demande *ex parte*, le juge de paix peut décerner un mandat autorisant, sous réserve des conditions éventuellement fixées, la personne désignée qui y est nommée à entrer dans une maison d'habitation s'il est convaincu, sur la foi d'une dénonciation sous serment, que les conditions suivantes sont réunies :

- a)** la maison d'habitation est un lieu visé au paragraphe 20(1);
- b)** l'entrée est nécessaire à toute fin prévue à ce paragraphe;
- c)** soit l'occupant a refusé l'entrée, soit il y a des motifs raisonnables de croire que tel sera le cas ou qu'il est impossible d'obtenir le consentement de l'occupant.

Usage de la force

(3) La personne désignée ne peut recourir à la force dans l'exécution du mandat que si celui-ci en autorise expressément l'usage et que si elle est accompagnée d'un agent de la paix.

Vérification interne

Ordre

22 (1) Sous réserve des règlements, la personne désignée peut, à toute fin liée à la vérification du respect ou à la prévention du non-respect de la présente loi, ordonner par écrit au fournisseur de services électroniques d'effectuer, dans le délai et selon les modalités précisés dans l'ordre, une vérification interne de ses pratiques, documents et données électroniques afin d'établir s'il se conforme à toute disposition de la présente loi ou des règlements.

Loi sur les textes réglementaires

(2) La *Loi sur les textes réglementaires* ne s'applique pas aux ordres donnés en vertu du paragraphe (1).

Obligation de conformité

23 Le fournisseur de services électroniques est tenu de se conformer à l'ordre et, dans le délai qui y est précisé,

period specified in the order, a report of the results of the audit, including, if the electronic service provider determines that there is non-compliance with a provision of this Act or the regulations, the nature of the non-compliance and any measures that it has taken or will take to comply with the provision or the order. 5

Compliance Order

Power to order termination of contravention

24 (1) If a designated person believes on reasonable grounds that there is or is likely to be a contravention of any provision of this Act or the regulations, they may make an order in writing requiring an electronic service provider to 10

(a) stop doing something that is or is likely to be in contravention of that provision or cause it to be stopped; or

(b) take any measure that is necessary to comply with the requirements of that provision or mitigate the effects of non-compliance. 15

Time and manner for review

(2) The order must specify the time within which and the manner in which the electronic service provider may request a review of the order by the Minister. 20

Statutory Instruments Act

(3) The *Statutory Instruments Act* does not apply to an order made under subsection (1).

Compliance with order

25 (1) An electronic service provider that is subject to an order made under subsection 24(1) must comply with it. 25

Notification of compliance

(2) Once the electronic service provider complies with the order, it must notify the designated person of its compliance without delay.

Request for review

26 (1) An order that is made under subsection 24(1) must be reviewed by the Minister at the written request of the electronic service provider that is subject to the order. 30

de fournir à la personne désignée un rapport sur les résultats de la vérification interne. Il y indique notamment, le cas échéant, la nature de toute non-conformité aux dispositions de la présente loi ou des règlements ainsi que les mesures qu'il a prises ou qu'il prendra pour se conformer aux dispositions en cause ou à l'ordre. 5

Ordre de conformité

Pouvoir d'ordonner : cessation de la contravention

24 (1) Si elle a des motifs raisonnables de croire qu'il y a ou qu'il y aura vraisemblablement contravention à une disposition de la présente loi ou des règlements, la personne désignée peut ordonner par écrit au fournisseur de services électroniques : 10

a) de cesser de faire toute chose en contravention de la disposition — ou toute chose qui donnera vraisemblablement lieu à une contravention de la disposition — ou de la faire cesser; 15

b) de prendre toute mesure nécessaire pour se conformer à la disposition ou pour atténuer les effets découlant de la contravention.

Délai et modalités : révision

(2) L'ordre précise le délai et les modalités selon lesquels le fournisseur de services électroniques peut en demander la révision auprès du ministre. 20

Loi sur les textes réglementaires

(3) La *Loi sur les textes réglementaires* ne s'applique pas aux ordres donnés en vertu du paragraphe (1).

Obligation de conformité

25 (1) Le fournisseur de services électroniques visé par l'ordre donné en vertu du paragraphe 24(1) est tenu de s'y conformer. 25

Avis de conformité

(2) Une fois qu'il s'y est conformé, le fournisseur de services électroniques en avise sans délai la personne désignée.

Demande de révision

26 (1) L'ordre donné en vertu du paragraphe 24(1) est révisé par le ministre sur demande écrite du fournisseur de services électroniques qui y est visé. 30

Time and manner of request

(2) The request must be made within the time and in the manner specified in the order and must state the grounds for review and set out the evidence that supports those grounds.

Order in effect

(3) The order continues to apply during a review unless the Minister decides otherwise. 5

Decision on completion of review

27 (1) On completion of a review, the Minister must confirm, amend, revoke or cancel the order and provide notice of the decision and the reasons for the decision to the electronic service provider. 10

Deemed confirmation

(2) If the Minister does not make a decision in respect of the request within 90 days after the day on which the request is received, or within any further period that is agreed on by the Minister and the electronic service provider, the Minister is deemed to have confirmed the order. 15

Administrative Monetary Penalties

Violations

Purpose of penalty

28 The purpose of an administrative monetary penalty is to promote compliance with this Act and not to punish.

Commission of violations

29 (1) A person who contravenes any of the following provisions commits a violation and is liable to a penalty of an amount that is to be established by a designated person in accordance with the regulations: 20

(a) section 12, subsection 14(1), section 15, subsection 20(5), section 23 or subsection 25(1) or (2);

(b) a provision of the regulations designated by a regulation made under paragraph 47(1)(e). 25

Maximum penalty

(2) The maximum penalty for a violation is \$50,000 in the case of an individual and \$250,000 in the case of any other person.

Délai et modalités : demande

(2) La demande est motivée, énonce les éléments de preuve à son appui et est présentée dans le délai et selon les modalités précisés dans l'ordre.

Absence de suspension

(3) À moins que le ministre n'en décide autrement, la révision n'a pas pour effet de suspendre l'application de l'ordre. 5

Issue de la révision

27 (1) Au terme de la révision, le ministre confirme, modifie, révoque ou annule l'ordre et transmet au fournisseur de services électroniques un avis motivé de la décision. 10

Confirmation réputée

(2) S'il ne rend pas sa décision dans les quatre-vingt-dix jours suivant la date de réception de la demande ou dans tout autre délai supplémentaire convenu entre lui et le demandeur, le ministre est réputé avoir confirmé l'ordre. 10

Sanctions administratives pécuniaires

Violations

But de la sanction

28 La sanction administrative pécuniaire vise non pas à punir, mais à favoriser le respect de la présente loi. 15

Violation

29 (1) Commet une violation et s'expose à une sanction dont le montant est établi par la personne désignée conformément aux règlements quiconque contrevient :

a) à l'article 12, au paragraphe 14(1), à l'article 15, au paragraphe 20(5), à l'article 23 ou aux paragraphes 25(1) ou (2); 20

b) à toute disposition des règlements désignée par les règlements pris en vertu de l'alinéa 47(1)e). 25

Plafond : montant de la sanction

(2) Toute violation expose son auteur à une sanction dont le montant maximal est, dans le cas d'une personne physique, de 50 000 \$ et, dans le cas de toute autre personne, de 250 000 \$. 25

Continuing violation

(3) A violation that is committed or continued on more than one day constitutes a separate violation in respect of each day on which it is committed or continued.

Due diligence defence

(4) A person is not to be found liable for a violation if they establish that they exercised due diligence to prevent its commission. 5

Common law principles

(5) Every rule and principle of the common law that renders any circumstance a justification or excuse in relation to a charge for an offence under this Act applies in respect of a violation to the extent that it is not inconsistent with this Act. 10

Proof of violation

30 In any proceedings under this Act against a person in relation to a violation, it is sufficient proof of the violation to establish that the act or omission that constitutes the violation was committed by an employee or an agent or mandatary of the person, whether or not the employee or agent or mandatary is identified. 15

Violation by corporate officers, etc.

31 If a person other than an individual commits a violation under this Act, any of the person's directors, officers or agents or mandataries who directed, authorized, assented to, acquiesced in or participated in the commission of the violation is a party to and liable for the violation, whether or not the person who actually committed the violation is proceeded against under this Act. 20

Proceedings

Issuance of notice of violation

32 If a designated person believes on reasonable grounds that a person has committed a violation, the designated person may issue, and must serve the person with, a notice of violation. 25

Limitation or prescription period

33 (1) A notice of violation is not to be issued in respect of a violation more than two years after the day on which the Minister becomes aware of the acts or omissions that constitute the alleged violation. 30

Certification by Minister

(2) A document appearing to have been issued by the Minister, certifying the day on which the acts or omissions that constitute the alleged violation became known to the Minister, is admissible in evidence without proof 35

Violation continue

(3) Il est compté une violation distincte pour chacun des jours au cours desquels se commet ou se continue la violation.

Moyen de défense : précautions voulues

(4) Nul ne peut être tenu responsable d'une violation s'il prouve qu'il a pris toutes les précautions voulues pour prévenir sa commission. 5

Principes de la common law

(5) Les règles et principes de la common law qui font d'une circonstance une justification ou une excuse dans le cadre d'une poursuite pour infraction à la présente loi s'appliquent à l'égard d'une violation dans la mesure où ils sont compatibles avec la présente loi. 10

Preuve de la violation

30 Dans les procédures en violation engagées au titre de la présente loi, il suffit, pour prouver la violation, d'établir que l'acte ou l'omission qui la constitue est le fait d'un employé ou d'un mandataire du prétendu auteur de la violation, que l'employé ou le mandataire ait été ou non identifié. 15

Participants à la violation

31 En cas de commission d'une violation par toute personne autre qu'une personne physique, ceux de ses dirigeants, administrateurs ou mandataires qui l'ont ordonnée ou autorisée, ou qui y ont consenti ou participé, sont considérés comme des coauteurs de la violation, que la personne fasse ou non l'objet d'une procédure en violation engagée au titre de la présente loi. 20

Ouverture de la procédure

Verbalisation

32 La personne désignée qui a des motifs raisonnables de croire qu'une violation a été commise peut dresser un procès-verbal qu'elle fait signifier au prétendu auteur de la violation. 25

Prescription

33 (1) Le délai dans lequel le procès-verbal peut être dressé est de deux ans à compter de la date où le ministre prend connaissance des faits reprochés. 30

Attestation du ministre

(2) Tout document apparemment délivré par le ministre et attestant la date où les faits reprochés sont parvenus à sa connaissance fait foi de cette date, sauf preuve

of the signature or official character of the person appearing to have signed the document and, in the absence of evidence to the contrary, is proof that the Minister became aware of the acts or omissions on that day.

How act or omission may be proceeded with

34 If an act or omission may be proceeded with either as a violation or as an offence, proceeding in one manner precludes proceeding in the other. 5

Payment of Penalties and Alternatives to Payment

Effect of payment

35 (1) If a person named in a notice of violation pays, in the prescribed time and manner, the penalty set out in the notice of violation, 10

(a) they are deemed to have committed the violation in respect of which the amount is paid;

(b) the Minister must accept that amount as complete satisfaction of the penalty; and

(c) the proceedings commenced in respect of the violation are ended. 15

Alternatives to payment

(2) Instead of paying the penalty, the person may, in the prescribed time and manner,

(a) request to enter into a compliance agreement with the Minister that ensures the person's compliance with the provision to which the violation relates; or 20

(b) request a review by the Minister of the acts or omissions that constitute the alleged violation or the amount of the penalty.

Failure to act

(3) If the person does not pay the penalty in the prescribed time and manner and does not make one of the requests referred to in subsection (2) in the prescribed time and manner, they are deemed to have committed the violation identified in the notice. 25

Compliance Agreements

Compliance agreements

36 (1) The Minister may, on request, enter into a compliance agreement with a person named in a notice of violation on any conditions that are satisfactory to the Minister. The compliance agreement may provide for the 30

contraire, sans qu'il soit nécessaire de prouver l'authenticité de la signature ni la qualité officielle du signataire.

Cumul interdit

34 S'agissant d'un acte ou d'une omission qualifiable à la fois de violation et d'infraction, la procédure en violation et la procédure pénale s'excluent l'une l'autre. 5

Païement de la sanction et options

Païement

35 (1) Si le prétendu auteur paie, dans le délai et selon les modalités réglementaires, la sanction prévue au procès-verbal, le paiement, que le ministre accepte en règlement, vaut déclaration de responsabilité à l'égard de la violation et met fin à la procédure. 10

Options

(2) S'il ne paie pas la sanction, le prétendu auteur peut, dans le délai et selon les modalités réglementaires :

a) demander au ministre de conclure avec lui une transaction en vue de la bonne observation de la disposition en cause; 15

b) contester devant le ministre les faits reprochés ou le montant de la sanction.

Omission d'agir

(3) L'omission du prétendu auteur de payer la sanction et d'exercer l'une des options prévues au paragraphe (2) dans le délai et selon les modalités réglementaires vaut déclaration de responsabilité à l'égard de la violation. 20

Transactions

Conclusion d'une transaction

36 (1) Sur demande du prétendu auteur, le ministre peut conclure une transaction qui est subordonnée aux conditions qu'il estime indiquées et qui peut prévoir la réduction partielle ou totale du montant de la sanction. 25

reduction, in whole or in part, of the amount of the penalty for the violation.

Effect of entering into agreement

(2) A person who enters into a compliance agreement with the Minister is, on doing so, deemed to have committed the violation in respect of which the compliance agreement was entered into. 5

Notice of compliance

(3) If the Minister is satisfied that a person who has entered into a compliance agreement has complied with it, the Minister must cause a notice to that effect to be provided to the person, at which time the proceedings commenced in respect of the violation are ended. 10

Notice of default

(4) If the Minister is of the opinion that a person who has entered into a compliance agreement has not complied with it, the Minister must cause a notice of default to be provided to the person to the effect that, instead of the penalty set out in the notice of violation in respect of which the compliance agreement was entered into, the person is liable to pay, in the prescribed time and manner, twice the amount of that penalty, and, for greater certainty, subsection 29(2) does not apply in respect of that amount. 15 20

Effect of notice of default

(5) Once provided with the notice of default, the person is not to deduct from the amount set out in the notice any amount that they spent under the compliance agreement and the person is liable to pay the amount set out in the notice. 25

Effect of payment

(6) If the person pays the amount set out in the notice of default, the Minister must accept the amount as complete satisfaction of the amount owing and the proceedings commenced in respect of the violation are ended. 30

Refusal to enter into compliance agreement

37 (1) If the Minister refuses to enter into a compliance agreement with a person named in a notice of violation, the person is liable to pay, in the prescribed time and manner, the penalty set out in the notice of violation.

Effect of payment

(2) If the person pays the penalty, 35
(a) they are deemed to have committed the violation in respect of which the payment is made;

Effet de la conclusion

(2) La conclusion de la transaction vaut déclaration de responsabilité à l'égard de la violation.

Avis d'exécution

(3) La notification au prétendu auteur d'un avis du ministre déclarant que celui-ci estime la transaction exécutée met fin à la procédure. 5

Avis de défaut d'exécution

(4) S'il estime la transaction inexécutée, le ministre fait notifier au prétendu auteur un avis de défaut l'informant qu'il est tenu, dans le délai et selon les modalités réglementaires, de payer, au lieu de la somme correspondant au montant de la sanction infligée initialement et sans qu'il soit tenu compte du plafond fixé au paragraphe 29(2), la somme correspondant au double de ce montant. 10

Effet de l'inexécution

(5) Sur notification de l'avis de défaut, le prétendu auteur perd tout droit de déduire de la somme due les sommes exposées dans le cadre de la transaction. Aux termes de l'avis, il est tenu de payer la somme qui y est prévue. 15

Paiement

(6) Le paiement de la somme prévue dans l'avis de défaut, que le ministre accepte en règlement, met fin à la procédure. 20

Refus de transiger

37 (1) Si le ministre refuse de transiger, le prétendu auteur est tenu, dans le délai et selon les modalités réglementaires, de payer la sanction infligée initialement.

Paiement

(2) Le paiement, que le ministre accepte en règlement, vaut déclaration de responsabilité à l'égard de la violation et met fin à la procédure. 25

(b) the Minister must accept the amount as complete satisfaction of the penalty; and

(c) the proceedings commenced in respect of the violation are ended.

Effect of non-payment

(3) If the person does not pay the penalty in the prescribed time and manner, they are deemed to have committed the violation identified in the notice of violation. 5

Review by the Minister

Review — facts

38 (1) On completion of a review requested under paragraph 35(2)(b) with respect to the acts or omissions that constitute the alleged violation, the Minister must determine, on a balance of probabilities, whether the person named in the notice of violation committed the violation. 10
If the Minister determines that the person committed the violation but that the amount of the penalty was not established by the designated person in accordance with the regulations, the Minister must correct the amount. 15

Violation not committed — effect

(2) If the Minister determines that the person named in the notice of violation did not commit the violation, the proceedings commenced in respect of the violation are ended. 20

Review — with respect to penalty

(3) On completion of a review requested under paragraph 35(2)(b) with respect to the amount of the penalty, the Minister must determine whether the amount of the penalty was established in accordance with the regulations and, if not, the Minister must correct the amount. 25

Notice of decision

(4) The Minister must cause a notice of any decision made under subsection (1) or (3) to be provided to the person named in the notice of violation.

Liability for penalty

(5) The person named in the notice of violation is liable to pay, in the time and manner specified in a decision made under subsection (1) or (3), the amount of the penalty that is confirmed or corrected in the decision. 30

Effect of payment

(6) If the person named in the notice of violation pays the amount referred to in subsection (5), the Minister must accept the amount as complete satisfaction of the 35

Non-paiement

(3) L'omission du prétendu auteur de faire le paiement dans le délai et selon les modalités réglementaires vaut déclaration de responsabilité à l'égard de la violation.

Contestation devant le ministre

Contestation relative aux faits reprochés

38 (1) Saisi au titre de l'alinéa 35(2)b) d'une contestation relative aux faits reprochés, le ministre décide, selon la prépondérance des probabilités, si le prétendu auteur est responsable. S'il conclut que celui-ci a commis la violation, mais juge que la personne désignée n'a pas établi le montant de la sanction en conformité avec les règlements, il y substitue le montant qu'il estime conforme. 10

Effet de la non-responsabilité

(2) La décision du ministre portant que le prétendu auteur n'est pas responsable de la violation met fin à la procédure.

Contestation relative au montant de la sanction

(3) Saisi au titre de l'alinéa 35(2)b) d'une contestation relative au montant de la sanction, le ministre vérifie si celui-ci a été établi en conformité avec les règlements et, si ce n'est pas le cas, y substitue le montant qu'il estime conforme. 15

Notification de la décision

(4) Le ministre fait notifier au prétendu auteur toute décision prise au titre des paragraphes (1) ou (3). 20

Obligation de payer

(5) Le prétendu auteur est tenu, dans le délai et selon les modalités précisés dans la décision, de payer la somme prévue dans celle-ci.

Paiement

(6) Le paiement de la somme prévue dans la décision, que le ministre accepte en règlement, met fin à la procédure. 25

penalty and the proceedings commenced in respect of the violation are ended.

Recovery of Debts

Debt to His Majesty

39 (1) The following amounts constitute debts due to His Majesty in right of Canada that may be recovered in the Federal Court:

- (a) the amount of a penalty, beginning on the day on which the notice of violation setting out the amount of the penalty is served;
- (b) the amount set out in a compliance agreement entered into under subsection 36(1), beginning on the day on which the compliance agreement is entered into;
- (c) the amount set out in a notice of default referred to in subsection 36(4), beginning on the day on which the time the notice is provided; and
- (d) the amount of a penalty as set out in a decision made by the Minister under subsection 38(1) or (3), beginning on the day on which the time the notice of that decision is provided.

Limitation or prescription period

(2) No proceedings to recover such a debt may be commenced later than five years after the debt became payable.

Debt final

(3) The debt is final and not subject to review or to be restrained, prohibited, removed, set aside or otherwise dealt with except to the extent and in the manner provided by sections 35 to 38.

Certificate

40 (1) Any debt referred to in subsection 39(1) in respect of which there is a default of payment, or the part of any such debt that has not been paid, may be certified by the Minister.

Registration

(2) Registration in the Federal Court of the certificate has the same force and effect as a judgment of that court for a debt of the amount specified in the certificate and all related registration costs.

Recouvrement des créances

Créance de Sa Majesté

39 (1) Constituent une créance de Sa Majesté du chef du Canada, dont le recouvrement peut être poursuivi à ce titre devant la Cour fédérale :

- a) toute sanction, à compter de la date de signification du procès-verbal;
- b) toute somme prévue dans une transaction conclue au titre du paragraphe 36(1), à compter de la date de la conclusion;
- c) la somme prévue dans l'avis de défaut notifié au titre du paragraphe 36(4), à compter de la date de la notification;
- d) la somme prévue dans la décision du ministre prise au titre des paragraphes 38(1) ou (3), à compter de la date de la notification.

Prescription

(2) Le recouvrement de la créance se prescrit par cinq ans à compter de la date à laquelle elle est devenue exigible.

Créance définitive

(3) La créance est définitive et n'est susceptible de contestation ou de révision que dans la mesure et selon les modalités prévues aux articles 35 à 38.

Certificat de non-paiement

40 (1) Le ministre peut établir un certificat de non-paiement pour la partie impayée des créances visées au paragraphe 39(1).

Enregistrement à la Cour fédérale

(2) L'enregistrement à la Cour fédérale confère au certificat la valeur d'un jugement de cette juridiction pour la somme visée et les frais afférents à l'enregistrement.

Offences

Offences — general

41 (1) A person who contravenes any of the following provisions commits an offence:

(a) section 12, subsection 14(1), section 15, subsection 20(5), section 23 or subsection 25(1) or (2);

(b) a provision of the regulations designated by a regulation made under paragraph 47(1)(f). 5

Punishment

(2) A person who commits an offence under subsection (1) is liable on summary conviction to a fine of not more than \$100,000 in the case of an individual and not more than \$500,000 in the case of any other person. 10

Continuing offence

(3) If an offence under subsection (1) is committed or continued on more than one day, it constitutes a separate offence for each day on which it is committed or continued.

Due diligence defence

(4) A person is not to be found guilty of an offence under subsection (1) if they establish that they exercised due diligence to prevent its commission. 15

Proof of offence

42 In a prosecution of a person for an offence under subsection 41(1), it is sufficient proof of the offence to establish that the act or omission that constitutes the offence was committed by an employee or an agent or mandatary of the person, whether or not the employee or agent or mandatary is identified. 20

Offence by corporate officers, etc.

43 If a person other than an individual commits an offence under subsection 41(1), any of the person's directors, officers or agents or mandataries who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is a party to the offence and is liable on conviction to the punishment provided for by this Act, whether or not the person who actually committed the offence is prosecuted. 30

Obstruction

44 A person commits an offence if they knowingly obstruct or hinder any of the following persons who are ex-

Infractions

Infractions générales

41 (1) Commet une infraction quiconque contrevient :

a) à l'article 12, au paragraphe 14(1), à l'article 15, au paragraphe 20(5), à l'article 23 ou aux paragraphes 25(1) ou (2);

b) à toute disposition des règlements désignée par les règlements pris en vertu de l'alinéa 47(1)f). 5

Peine

(2) Quiconque commet une infraction prévue au paragraphe (1) encourt, sur déclaration de culpabilité par procédure sommaire, dans le cas d'une personne physique, une amende maximale de 100 000 \$ et, dans le cas de toute autre personne, une amende maximale de 500 000 \$. 10

Infraction continue

(3) Il est compté une infraction distincte pour chacun des jours au cours desquels se commet ou se continue l'infraction prévue au paragraphe (1). 15

Moyen de défense : précautions voulues

(4) Nul ne peut être déclaré coupable d'une infraction prévue au paragraphe (1) s'il prouve qu'il a pris toutes les précautions voulues pour prévenir sa perpétration.

Preuve de l'infraction

42 Dans les poursuites pour une infraction prévue au paragraphe 41(1), il suffit, pour prouver l'infraction, d'établir que l'acte ou l'omission qui la constitue est le fait d'un employé ou d'un mandataire de l'accusé, que l'employé ou le mandataire ait été ou non identifié. 20

Participants à l'infraction

43 En cas de perpétration d'une infraction prévue au paragraphe 41(1) par toute personne autre qu'une personne physique, ceux de ses dirigeants, administrateurs ou mandataires qui l'ont ordonnée ou autorisée, ou qui y ont consenti ou participé, sont considérés comme des coauteurs de l'infraction et encourtent, sur déclaration de culpabilité, la peine prévue, que la personne ait été ou non poursuivie. 30

Entrave

44 Commet une infraction quiconque entrave sciemment l'action de l'une ou l'autre des personnes ci-après

exercising powers or performing duties or functions under this Act:

- (a) a person to whom assistance must be provided under subsection 14(1);
- (b) a person designated under subsection 19(1).

False or misleading statements

45 A person commits an offence if they knowingly make a false or misleading statement, verbally or in writing, to any of the following persons who are exercising powers or performing duties or functions under this Act:

- (a) a person to whom assistance must be provided under subsection 14(1);
- (b) a person designated under subsection 19(1).

Punishment

46 A person who commits an offence under section 44 or 45 is liable on summary conviction

- (a) in the case of an individual, to a fine of not more than \$25,000 for a first offence and of not more than \$50,000 for each subsequent offence; and
- (b) in the case of any other person, to a fine of not more than \$100,000 for a first offence and of not more than \$250,000 for each subsequent offence.

Regulations

Regulations

47 (1) The Governor in Council may make regulations

- (a) respecting any fees payable to electronic service providers for different types of assistance that they provide to persons exercising an authority referred to in subsection 2(2);
- (b) respecting record-keeping and reporting by electronic service providers;
- (c) respecting the meaning of any term or expression for the purposes of this Act;
- (d) respecting orders referred to in section 22 and reports referred to in section 23;
- (e) respecting the administrative monetary penalties scheme, including regulations

agissant dans l'exercice des attributions qui lui sont conférées sous le régime de la présente loi :

- a) la personne à qui doit être prêtée de l'assistance aux termes du paragraphe 14(1);
- b) la personne désignée en vertu du paragraphe 19(1).

Déclaration fausse ou trompeuse

45 Commet une infraction quiconque fait sciemment une déclaration fausse ou trompeuse — oralement ou par écrit — à l'une ou l'autre des personnes ci-après agissant dans l'exercice des attributions qui lui sont conférées sous le régime de la présente loi :

- a) la personne à qui doit être prêtée de l'assistance aux termes du paragraphe 14(1);
- b) la personne désignée en vertu du paragraphe 19(1).

Peine

46 Quiconque commet une infraction prévue aux articles 44 ou 45 encourt, sur déclaration de culpabilité par procédure sommaire :

- a) dans le cas d'une personne physique, une amende maximale de 25 000 \$ pour une première infraction et de 50 000 \$ en cas de récidive;
- b) dans le cas de toute autre personne, une amende maximale de 100 000 \$ pour une première infraction et de 250 000 \$ en cas de récidive.

Règlements

Règlements

47 (1) Le gouverneur en conseil peut prendre des règlements :

- a) concernant les frais payables aux fournisseurs de services électroniques pour différents types d'assistance qu'ils prêtent à des personnes exerçant des pouvoirs visés au paragraphe 2(2);
- b) concernant la tenue de registres et la préparation de rapports par les fournisseurs de services électroniques;
- c) concernant le sens à donner à tout terme ou à toute expression pour l'application de la présente loi;
- d) concernant les ordres visés à l'article 22 et les rapports visés à l'article 23;

(i) designating provisions of the regulations for the purposes of paragraph 29(1)(b),

(ii) respecting the establishment of penalty amounts,

(iii) respecting the content of notices of violation, 5

(iv) respecting reviews by the Minister, and

(v) respecting the service or provision of documents;

(f) designating provisions of the regulations for the purposes of paragraph 41(1)(b); 10

(g) prescribing anything that is required or authorized by this Act to be prescribed;

(h) prescribing the way in which anything that is required or authorized by this Act to be prescribed is to be determined; and 15

(i) generally, for carrying out the purposes and provisions of this Act.

Periodic review

(2) Every five years after the day on which the first regulation is made under paragraph (1)(a), the Minister must review all regulations made under that paragraph. 20

Notice

(3) Before the first regulation under paragraph (1)(a) is made and during every review referred to in subsection (2), the Minister must publish a notice inviting the following persons to make representations within the time and in the form and manner specified in the notice: 25

(a) the Attorney General of Canada;

(b) the attorney general of each province;

(c) core providers; and

(d) electronic service providers that are subject to orders made under subsection 7(1). 30

Distinguishing

48 For greater certainty, regulations made under this Act may establish classes of electronic service providers and distinguish among them, including on the basis of the electronic service provided and on the basis of the

e) concernant le régime de sanctions administratives pécuniaires, notamment des règlements :

(i) désignant les dispositions des règlements pour l'application de l'alinéa 29(1)b),

(ii) concernant l'établissement du montant de la sanction à infliger, 5

(iii) concernant le contenu des procès-verbaux,

(iv) concernant les contestations devant le ministre,

(v) concernant la signification ou la notification des documents; 10

f) désignant les dispositions des règlements pour l'application de l'alinéa 41(1)b);

g) précisant toute mesure d'ordre réglementaire prévue par la présente loi; 15

h) précisant la façon de déterminer ce qui peut ou doit faire l'objet d'une mesure réglementaire;

i) concernant toute autre mesure d'application de la présente loi.

Examen quinquennal

(2) Tous les cinq ans à compter de la date de la prise du premier règlement en vertu de l'alinéa (1)a), le ministre examine tout règlement pris en vertu de cet alinéa. 20

Avis

(3) Avant la prise du premier règlement en vertu de l'alinéa (1)a) et au cours de chaque examen visé au paragraphe (2), le ministre publie un avis invitant les personnes ci-après à lui présenter leurs observations dans le délai et selon les modalités précisés dans l'avis : 25

a) le procureur général du Canada;

b) le procureur général de chaque province;

c) les fournisseurs principaux; 30

d) les fournisseurs de services électroniques visés par un arrêté pris en vertu du paragraphe 7(1).

Précision

48 Il est entendu que les règlements pris en vertu de la présente loi peuvent prévoir des catégories de fournisseurs de services électroniques et les traiter différemment, notamment, selon les services électroniques que les fournisseurs de services électroniques fournissent et 35

number of persons in Canada to whom the electronic service provider provides services.

Report

Annual report

49 (1) Within 90 days after the end of each calendar year, the Minister must prepare a report on the Minister's activities under this Act during that year.

Contents

(2) The report must include

- (a)** the number of orders made under subsection 7(1), as well as information relating to the classes of electronic service providers in respect of which the orders were made and the obligations imposed by the orders in respect of operational and technical capabilities;
- (b)** the number of orders that were not approved by the Intelligence Commissioner, as well as information relating to the electronic service providers in respect of which the orders were made and the obligations that were to be imposed by the orders in respect of operational and technical capabilities;
- (c)** information relating to the compliance orders made and enforcement actions taken under this Act;
- (d)** the number of requests for assistance made under subsection 14(1) and the classes of persons to whom assistance was provided; and
- (e)** any other prescribed information.

Publication

(3) The Minister must make the report available to the public, with any redactions that the Minister considers necessary, within 60 days after the day on which it has been prepared.

Unredacted report

(4) If the report contains any redactions, the Minister must cause the unredacted report to be provided to the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency on any of the first 15 days on which either House of Parliament is sitting after the day on which the report is prepared.

le nombre de personnes qui se trouvent au Canada auxquelles ils fournissent des services.

Rapport

Rapport annuel

49 (1) Dans les quatre-vingt-dix jours suivant la fin de chaque année civile, le ministre établit un rapport des activités qu'il a exercées dans le cadre de la présente loi au cours de l'année précédente.

Contenu

(2) Le rapport contient :

- a)** le nombre d'arrêtés pris en vertu du paragraphe 7(1) ainsi que des renseignements sur les catégories de fournisseurs de services électroniques visées par ces arrêtés et les obligations en matière de capacité opérationnelle et technique qui y sont prévues;
- b)** le nombre d'arrêtés qui n'ont pas été approuvés par le commissaire au renseignement ainsi que des renseignements sur les fournisseurs de services électroniques visés par ces arrêtés et les obligations en matière de capacité opérationnelle et technique qui y sont prévues;
- c)** des renseignements sur les ordres de conformité donnés et les mesures de contrôle d'application de la loi prises en vertu de la présente loi;
- d)** le nombre de demandes d'assistance présentées au titre du paragraphe 14(1) et les catégories de personnes à qui de l'assistance a été prêtée;
- e)** toute autre information prévue par règlement.

Publication

(3) Le ministre met à la disposition du public le rapport — exception faite des passages qu'il estime nécessaire de caviarder — dans les soixante jours suivant la date à laquelle le rapport est établi.

Rapport non caviardé

(4) Si le rapport contient des passages caviardés, le ministre fait transmettre le rapport non caviardé au Comité des parlementaires sur la sécurité nationale et le renseignement et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, et ce, dans les quinze premiers jours de séance de l'une ou l'autre chambre du Parlement suivant la date d'établissement du rapport.

2019, c. 13, s. 50

Related and Consequential Amendments to the Intelligence Commissioner Act

42 Paragraphs 12(a) and (b) of the *Intelligence Commissioner Act* are replaced by the following:

- (a) reviewing the conclusions on the basis of which certain authorizations are issued or amended, and certain determinations are made, under the *Communications Security Establishment Act* and the *Canadian Security Intelligence Service Act* and on the basis of which certain orders are made under the *Supporting Authorized Access to Information Act*; and
- (b) if those conclusions are reasonable, approving those authorizations, amendments, determinations and orders.

43 The Act is amended by adding the following after section 19:

Ministerial orders

19.1 The Commissioner must review whether the conclusions — made under subsection 7(3) of the *Supporting Authorized Access to Information Act* and on the basis of which an order was made under subsection 7(1) of that Act — are reasonable.

44 (1) Subsection 20(1) of the Act is replaced by the following:

Commissioner's decision

20 (1) After conducting a review under any of sections 13 to 16 and 18 to 19.1, the Commissioner, in a written decision,

- (a) must approve the authorization, amendment, determination or order if the Commissioner is satisfied that the conclusions at issue are reasonable, and must set out the Commissioner's reasons for doing so; or
- (b) must not approve the authorization, amendment, determination or order if the Commissioner is not so satisfied, and must set out the Commissioner's reasons for doing so.

(2) Paragraph 20(3)(b) of the Act is replaced by the following:

- (b) within 30 days after the day on which the Commissioner receives notice of the authorization, amend-

2019, ch. 13, art. 50

Modifications connexes et corrélatives à la Loi sur le commissaire au renseignement

42 Les alinéas 12a) et b) de la *Loi sur le commissaire au renseignement* sont remplacés par ce qui suit :

- a) d'examiner les conclusions sur lesquelles reposent certaines autorisations accordées ou modifiées et certaines déterminations effectuées au titre de la *Loi sur le Centre de la sécurité des télécommunications* et de la *Loi sur le Service canadien du renseignement de sécurité* ainsi que celles sur lesquelles reposent certains arrêtés pris en vertu de la *Loi sur le soutien en matière d'accès autorisé à de l'information*;
- b) d'approuver, si ces conclusions sont raisonnables, ces autorisations, modifications, déterminations et arrêtés.

43 La même loi est modifiée par adjonction, après l'article 19, de ce qui suit :

Arrêtés

19.1 Le commissaire examine si les conclusions formulées au titre du paragraphe 7(3) de la *Loi sur le soutien en matière d'accès autorisé à de l'information*, sur la base desquelles un arrêté a été pris en vertu du paragraphe 7(1) de cette loi, sont raisonnables.

44 (1) Le paragraphe 20(1) de la même loi est remplacé par ce qui suit :

Décision du commissaire

20 (1) Après avoir effectué l'examen prévu à l'un des articles 13 à 16 et 18 à 19.1, le commissaire, dans une décision écrite :

- a) approuve l'autorisation, la modification, la détermination ou l'arrêté, s'il est convaincu que les conclusions en cause sont raisonnables, et motive sa décision;
- b) n'approuve pas l'autorisation, la modification, la détermination ou l'arrêté dans le cas contraire et motive sa décision.

(2) L'alinéa 20(3)b) de la même loi est remplacé par ce qui suit :

- b) dans les trente jours suivant la date de réception d'un avis de l'autorisation, de la modification, de la dé-

ment, determination or order, or within any other period that may be agreed on by the Commissioner and the person, in any other case.

45 Subsections 22(1) and (2) of the Act are replaced by the following:

Report to Prime Minister

22 (1) The Commissioner must, each calendar year, submit to the Prime Minister a report with respect to the Commissioner's activities during the previous calendar year. The report must include statistics, that the Commissioner considers appropriate, relating to the authorizations, amendments, determinations and orders that were approved and not approved.

Protection of confidential information

(2) The Commissioner must consult with the Director of the Canadian Security Intelligence Service, the Chief of the Communications Security Establishment and the Minister of Public Safety and Emergency Preparedness in preparing the report in order to ensure that it does not contain information the disclosure of which would be injurious to national security, national defence or international relations or information that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege.

46 Subsection 23(1) of the Act is replaced by the following:

Provision of information to Commissioner

23 (1) Despite any other Act of Parliament and subject to section 26, the person whose conclusions are being reviewed by the Commissioner under any of sections 13 to 19.1 must, for the purposes of the Commissioner's review, provide the Commissioner with all information that was before the person in issuing or amending the authorization or making the determination or order at issue, including information that is subject to any privilege under the law of evidence, solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege.

Coming into Force

Order in council

47 This Part comes into force on a day to be fixed by order of the Governor in Council.

termination ou de l'arrêté en cause ou avant l'expiration de tout autre délai convenu par le commissaire et cette personne, dans tout autre cas.

45 Les paragraphes 22(1) et (2) de la même loi sont remplacés par ce qui suit :

Rapport au premier ministre

22 (1) Chaque année civile, le commissaire présente au premier ministre un rapport portant sur ses activités pour l'année civile précédente. Le rapport comporte les statistiques relatives aux autorisations, modifications, déterminations et arrêtés — approuvés ou non — que le commissaire estime appropriées.

Protection des renseignements confidentiels

(2) Afin d'éviter que le rapport d'activité ne contienne des renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales ou des renseignements protégés par le secret professionnel de l'avocat ou du notaire ou par le privilège relatif au litige, le commissaire consulte le directeur du Service canadien du renseignement de sécurité, le chef du Centre de la sécurité des télécommunications et le ministre de la Sécurité publique et de la Protection civile.

46 Le paragraphe 23(1) de la même loi est remplacé par ce qui suit :

Fourniture de renseignements au commissaire

23 (1) Malgré toute autre loi fédérale et sous réserve de l'article 26, la personne ayant formulé les conclusions examinées par le commissaire au titre de l'un des articles 13 à 19.1 lui fournit, pour les besoins de son examen, les renseignements dont elle disposait pour accorder ou modifier l'autorisation, effectuer la détermination ou prendre l'arrêté en cause, y compris les renseignements protégés par toute immunité reconnue par le droit de la preuve, par le secret professionnel de l'avocat ou du notaire ou par le privilège relatif au litige.

Entrée en vigueur

Décret

47 La présente partie entre en vigueur à la date fixée par décret.

PART 3

Parliamentary Review

Review after three years

48 During the third year after the first day on which all the provisions of this Act are in force, a comprehensive review of the provisions enacted or amended by Parts 1 and 2 as well as their operation is to be undertaken by the standing committee of each House of Parliament that normally considers matters relating to national security. 5

PARTIE 3

Examen parlementaire

Examen après trois ans

48 Au cours de la troisième année qui suit le premier jour où toutes les dispositions de la présente loi sont en vigueur, un examen approfondi des dispositions édictées ou modifiées par les parties 1 et 2 et de leur application est entrepris 5 par le comité permanent de chaque chambre du Parlement habituellement chargé des questions concernant la sécurité nationale.

SCHEDULE

(Section 41)

SCHEDULE

(Subsections 2(1) and 5(1))

Core Providers**ANNEXE**

(article 41)

ANNEXE

(paragraphe 2(1) et 5(1))

Fournisseurs principaux

1495

TAB 42

Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness), 2019 FC 1279 (CanLII)

Source: Federal Court
Date: 2019-10-09
File number: T-1682-18
Citation: Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness), 2019 FC 1279 (CanLII), <<https://canlii.ca/t/j35r2>>, retrieved on 2026-06-27

Date: 20191009

Docket: T-1682-18

Citation: 2019 FC 1279

Ottawa, Ontario, October 9, 2019

PRESENT: Mr. Justice McHaffie

BETWEEN:

**THE INFORMATION COMMISSIONER OF
CANADA**

Applicant

and

**THE MINISTER OF PUBLIC SAFETY AND
EMERGENCY PREPAREDNESS**

Respondent

JUDGMENT AND REASONS**I. Overview**

[1] Information that relates to an object rather than a person, such as the firearm serial numbers at issue in this case, is not by itself generally considered “personal information” since it is not information about an identifiable individual. However, such information may still be personal information exempt from disclosure under the *Access to Information Act*, RSC 1985, c A-1 [*ATIA*] if there is a serious possibility that the information could be used to identify an individual, either on its own or when combined with other available information.

[2] The assessment of whether information could be used to identify an individual is necessarily fact-driven and context-specific. The “other available information” relevant to the inquiry will depend on the nature of the information being considered for release. It will include information that is generally publicly available. Depending on the circumstances, it may also include information available to only a segment of the public. However, it will not typically include information that is only in the hands of government, given the purposes of both the *ATIA* and the personal information exemption.

[3] The evidence in this case does not establish a serious possibility that the release of the firearm serial numbers at issue will allow identification of an individual. To use the serial numbers to identify an individual would require either access to restricted government databases that already contain personal information, or a successful effort to trick either the government or the manufacturer into releasing personal information. The evidence does not establish a serious possibility of either occurring. The respondent has not met the onus of establishing that the firearm serial numbers are “personal information.” No other grounds to exempt the information from disclosure under the *ATIA* were raised, and the serial numbers will therefore be ordered released to the requester in response to their *ATIA* request.

[4] Had I concluded that the information was personal information exempt from disclosure, I would have remitted the matter back to the Royal Canadian Mounted Police to redetermine the

1498

use of discretion under [subsection 19\(2\)](#) of the *ATIA*, as the RCMP did not reasonably

consider whether the public interest in disclosure would outweigh the invasion of privacy resulting from release.

II. Facts

A. The Request for Access to Information and Partial Release of Information

[5] In 2014, the RCMP received the following request for access to records under the *ATIA*:

I am seeking all documentation regarding a Sig Sauer P226 serial number U 120 530 which was previously issued to RCMP ‘E’ Division Emergency Response Team.

I am also seeking a copy of the “disposal list” as well as a list of all the firearms that were sent back on warranty replacement around 1986.

[6] A “Sig Sauer P226” is a firearm, specifically a model of handgun manufactured by Sig Sauer, Inc. [Sig Sauer]. As with most other firearms, each Sig Sauer P226 bears a serial number, such as the “U 120 530” referenced in the request. No two Sig Sauer P226 guns will bear the same serial number, although two or more firearms of different makes or models might, coincidentally, carry the same number, particularly if the manufacturer adopted a fairly simple numbering system. Taken together, the make, model and serial number represent a unique firearm.

[7] In response to the *ATIA* request, the RCMP identified a 13-page chart that listed information regarding 468 Sig Sauer P226 firearms. With respect to each gun, the chart sets out the serial number, the model (“SIG SAUER 226” in each case), the RCMP unit the firearm was initially issued to, the date of receipt, the disposition of the firearm (“Warranty Return” in each case), and a column for comments (largely blank, but with the comment “Cracked frame” in respect to some firearms, and the comment “Subject of ATIP” for one firearm).

[8] The RCMP determined that release of the firearm serial numbers would result in the disclosure of “personal information” within the definition of [section 3](#) of the *Privacy Act*, RSC 1985, c P-21, since disclosure of the serial numbers would result in disclosure of information about identifiable

1499

individuals. The RCMP therefore concluded that they had to refuse to disclose the serial numbers under [subsection 19\(1\)](#) of the *ATIA*.

[9] The RCMP decided not to exercise the discretion available under [subsection 19\(2\)](#) of the *ATIA* to release the personal information. The RCMP noted that there had been no consent to disclose by those affected, that it would be unreasonable to attempt to obtain that consent, that the serial numbers were not already public, and that it was not in the public interest to disclose the serial numbers. The chart was therefore released to the requester with the serial numbers of the firearms redacted.

[10] The requester advised the RCMP that the serial number of his own firearm had been redacted from the released document. In response, the RCMP released to the requester the serial number of their own firearm. However, the RCMP maintained the position that release of the other serial numbers would disclose personal information and refused to release the record with those numbers.

B. The Information Commissioner's Investigation and Recommendation

[11] The requester filed a complaint with the Information Commissioner pursuant to [paragraph 30\(1\)\(a\)](#) of the *ATIA*. During the resulting investigation, the RCMP made representations expressing the view that the serial numbers were akin to a social insurance number and were thus personal information. The RCMP indicated that of the 468 serial numbers set out in the record, 398 (or 85%) were linked to an individual in the Canadian Firearms Information System (CFIS), with information including their name, date of birth and full address. The RCMP considered that the serial numbers could therefore be used to glean personal information from the CFIS database. The RCMP noted that they had consulted with Sig Sauer, presumably pursuant to [section 27](#) of the *ATIA*, asking whether they had any objection to the release of the “comments” column in the record, and received no objection from Sig Sauer.

1500

The Information Commissioner concluded that the complaint was well-founded, as the RCMP had not established that the serial numbers constituted personal information within the meaning of [section 3](#) of the *Privacy Act*. Pursuant to [subsection 37\(1\)](#) of the *ATIA* as it then read, the Information Commissioner reported these findings to the RCMP and recommended that the RCMP disclose the serial numbers of the firearms.

[13] The RCMP considered the Information Commissioner’s recommendation, but decided not to adopt it, maintaining the view that the serial numbers were personal information associated with identifying information in the CFIS database, and noting the importance of a broad approach to the definition of “personal information.”

[14] In light of the RCMP’s decision not to follow the recommendation, the Information Commissioner brought this application under [paragraph 42\(1\)\(a\)](#) of the *ATIA* as it then read. The Information Commissioner obtained the consent of the requester as required, and named the respondent as the Minister responsible for the RCMP. The Information Commissioner seeks an order directing the RCMP to disclose the unredacted record to the requester, including the serial numbers. In the alternative, the Information Commissioner asks that the matter be sent back to the RCMP for the re-exercise of the RCMP’s discretion under [subsection 19\(2\)](#) of the *ATIA*, on the basis that the RCMP has not reasonably exercised that discretion.

C. Additional Evidence Filed by the RCMP on this Application

[15] On this application, the RCMP filed an affidavit from Crystal Holub, the access officer responsible for handling the request, and an affidavit from Murray Smith, an RCMP employee with extensive experience with firearms including firearm serial numbers, who was presented as an expert to provide opinion evidence.

[16] Ms. Holub’s affidavit describes the RCMP’s response to the access request, including the conclusion that the serial numbers were subject to exemption under [subsection 19\(1\)](#) of the *ATIA* as “personal information,” and the RCMP’s exercise of its discretion under subsection 19(2).

1501

Mr. Smith's affidavit provides information regarding the nature and use of firearm serial numbers, the various government databases in which those serial numbers reside, and the potential for personal information to be released—either from those databases or from other sources—if the serial numbers at issue are disclosed.

III. Issues

[18] This application raises two primary issues:

- A. Are the firearm serial numbers at issue “personal information” within the meaning of [section 3](#) of the *Privacy Act* and thus exempt from disclosure under [subsection 19\(1\)](#) of the *ATIA*?
- B. If so, did the RCMP reasonably exercise the discretion set out in [subsection 19\(2\)](#) of the *ATIA* in refusing to disclose the information?

[19] These two issues will be addressed after a review of the applicable statutory provisions of the *ATIA* and the *Privacy Act*, and the relevant analytical principles. The full provisions, as they stood at the time of the complaint and as currently amended, are set out in Appendices A and B respectively.

[20] For the reasons given below, I conclude that the firearm serial numbers are not “personal information,” but that if they had been, the RCMP did not reasonably exercise their discretion to assess whether the numbers should nonetheless be released.

IV. The Legislative and Analytical Framework

A. Preliminary Note: Amendments to the ATIA and the Privacy Act

[21] On June 21, 2019, the *ATIA* was amended by *An Act to amend the Access to Information Act and the Privacy Act and to make consequential amendments to other Acts*, SC 2019, c 18 (Bill C-58). These amendments were made after the commencement of this application and after the parties filed their records, including memorandums of fact and law.

The amendments to the *ATIA* include changes relating to vexatious or bad faith requests and complaints, changes to the powers of the Information Commissioner including the introduction of a power to make orders to release records, and the addition of a new part of the *ATIA* regarding proactive publication of government information. The amendments to the *Privacy Act* include an amendment to the definition of “personal information,” but not one that is relevant to this application.

[23] None of the substantive provisions relevant to this application were materially amended. In particular, the purpose section of the *ATIA* (section 2) was amended, but those amendments are in keeping with the prior jurisprudence regarding the purpose of the right to access in the *ATIA*. Section 19 was also slightly amended, to replace the word “Act” with the word “Part” and to replace the words “personal information as defined in section 3 of the *Privacy Act*” with simply the words “personal information.” However, since the definition of “personal information” that is now contained in section 3 of the *ATIA* reads “*personal information* has the same meaning as in section 3 of the *Privacy Act*,” I take the amendment to be one of drafting and clarity, rather than any change in substance.

[24] Had the amendments been in force at the time of the complaint, the matter might have taken a different route to come to this Court. In particular, the Information Commissioner might have ordered the RCMP to disclose the information after consulting with the Privacy Commissioner, and the RCMP could have then applied to this Court for review: *ATIA*, ss 36.1, 36.2, 37(1)(b), 41(2); *SC 2019, c 18*, s 45. The roles of applicant and respondent would then have been reversed on this application. However, the onus and the relevant substantive provisions are the same under the current and former versions of the *ATIA* and *Privacy Act*. The recent amendments therefore do not affect the analysis or the outcome of this application.

B. Applicable Substantive Provisions

[25] Both the right to privacy and the right of access to information in the possession of government are sufficiently important that the *ATIA* and the *Privacy Act* have each been described

quasi-constitutional” statutes: *Canada (Information Commissioner) v Canada (Minister of National Defence)*, 2011 SCC 25 at para 40; *H.J. Heinz Co. of Canada Ltd. v Canada (Attorney General)*, 2006 SCC 13 [*Heinz*] at para 28.

[26] Sections 2 and 4 of the *ATIA* set out the general principle that the public has a right to access information in records that are under the control of government. As previously stated in the jurisprudence and now express in the amended subsection 2(1) of the *ATIA*, this general principle enhances accountability and transparency in government and promotes an open and democratic society: see, e.g., *Merck Frosst Canada Ltd v Canada (Health)*, 2012 SCC 3 [*Merck Frosst*] at paras 1, 21-22.

[27] The general principle of access to information under the control of government is expressly limited by “necessary exceptions to the right of access” that are set out in the *ATIA*, which exceptions “should be limited and specific”: *ATIA*, s 2; *Merck Frosst* at para 21. The exceptions to the right of access in the *ATIA* take the form of either discretionary exemptions (information that a government institution “may” refuse to disclose) or mandatory exemptions (information that a government institution “shall” refuse to disclose).

[28] Subsection 19(1) of the *ATIA* sets out a mandatory exemption to the general principle of access in the case of records that contain “personal information,” a term that is defined in the *ATIA* with reference to section 3 of the *Privacy Act*. Subject to a discretion set out in subsection 19(2), discussed further below, a government institution must refuse release of records that contain “personal information.”

[29] Section 3 of the *Privacy Act* defines “personal information” through a general definition; a non-exhaustive and non-restrictive list of examples that do not restrict the generality of the general definition (subsections 3(a) to (i)); and a list of exceptions (subsections 3(j) to (m)). The general definition is broadly drafted: “**personal information** means information about an identifiable individual that is recorded in any form...” [Emphasis added.] Section 2 of the *Privacy Act* sets out

1504

the purpose of the statute is to “protect the privacy of individuals with respect to personal information about themselves held by a government institution and [to] provide individuals with a right of access to that information.”

[30] In *Dagg v Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 SCR 403 [*Dagg*], the Supreme Court of Canada considered both the scope of “personal information” in the *Privacy Act* and the interplay between the *Privacy Act* and the *ATIA*. Justice La Forest wrote in dissent, but spoke for the Court on the approach to interpreting the two statutes. He underscored that the *Privacy Act* and the *ATIA* must be interpreted in parallel given their overlapping subject matter and legislative history. Since both statutes contain an express exemption of personal information from disclosure, privacy rights must be recognized as “paramount” over access to the extent that information falls within the definition of “personal information,” as Justice La Forest explained at paragraph 48:

Both statutes regulate the disclosure of personal information to third parties. Section 4(1) of the *Access to Information Act* states that the right to government information is “[s]ubject to this Act”. Section 19(1) of the Act prohibits the disclosure of a record that contains personal information “as defined in section 3 of the *Privacy Act*”. Section 8 of the *Privacy Act* contains a parallel prohibition, forbidding the non-consensual release of personal information except in certain specified circumstances. Personal information is thus specifically exempted from the general rule of disclosure. Both statutes recognize that, in so far as it is encompassed by the definition of “personal information” in s. 3 of the *Privacy Act*, privacy is paramount over access. [Emphasis added.]

[31] Justice La Forest noted that the protection of privacy was a “fundamental value in modern, democratic states” and that the definition of “personal information” in section 3 of the *Privacy Act* is “undeniably expansive” and “deliberately broad”: *Dagg* at paras 65, 68-69. Its intent is to capture “any information about a specific person, subject only to specific exceptions”: *Dagg* at para 69 [Emphasis in original.]

[32] As noted above, the examples that are set out in subsections (a) to (i) of the definition of “personal information” in section 3 of the *Privacy Act* do not restrict the generality of the general

1505

Justice La Forest confirmed that they are merely examples of the type of subject matter encompassed by the general definition, such that “if a government record is captured by those opening words, it does not matter that it does not fall within any of the specific examples”: *Dagg* at para 68.

[33] The recognition in *Dagg* of the supremacy of privacy over access and the broad definition of personal information has been consistently reaffirmed over the decades since *Dagg* by the Supreme Court of Canada and the Federal Courts: *Heinz* at paras 61, 71; *Husky Oil Operations Limited v Canada-Newfoundland and Labrador Offshore Petroleum Board*, 2018 FCA 10 [*Husky Oil*] at paras 25, 55.

[34] The general definition of “personal information” requires that information must be “about an identifiable individual.” The importance of privacy rights is such that the courts have recognized that even if information may not on its face reveal anything personal, it will be “about” an identifiable individual and exempt from disclosure if there is a serious possibility that the individual could be identified through the release of the information. In *Canada (Information Commissioner) v Canada (Canadian Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, leave to appeal to SCC refused, 2007 CanLII 11607 [*NavCanada*], Justice Desjardins wrote the following at paragraph 43:

These two words, “about” and “*concernant*”, shed little light on the precise nature of the information which relates to the individual, except to say that information recorded in any form is relevant if it is “about” an individual and if it permits or leads to the possible identification of the individual. There is judicial authority holding that an “identifiable” individual is considered to be someone whom it is reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available ... [Emphasis added; citations omitted.]

[35] Relying on *NavCanada*, Justice Gibson of this Court in *Gordon v Canada (Health)*, 2008 FC 258 [*Gordon*] at paragraph 34 adopted the following test proposed by the Privacy Commissioner to determine when information is about an identifiable individual: “Information will be about an identifiable individual where there is a serious possibility that an individual could be identified

through the use of that information, alone or in combination with other available information”

[Emphasis added.] The parties were agreed on this statement of the law as set out in *Gordon*.

[36] Although personal information is subject to a mandatory exemption from release in [subsection 19\(1\)](#) of the *ATIA*, it may still be released as a discretionary matter in certain cases. Subsection 19(2) provides that personal information may disclose a record that contains personal information in one of three circumstances: (a) where the individual to whom it relates consents; (b) where the information is publicly available; or (c) where the disclosure is in accordance with [section 8](#) of the *Privacy Act*. This further cross-reference to the *Privacy Act* again highlights the interlocking nature of the two statutes.

[37] [Subsection 8\(1\)](#) of the *Privacy Act* sets out a general prohibition on disclosure of personal information without consent, mirroring the mandatory exemption from release in [subsection 19\(1\)](#) of the *ATIA*. Subsection 8(2) then sets out a series of 13 exceptions in which personal information may be disclosed, some of which are narrow (*e.g.*, paragraph 8(2)(c): for the purpose of complying with a subpoena or disclosure obligations), and some of which are broader (notably subparagraph 8(2)(m)(i): for any purpose where in the opinion of the head of the institution, the “public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure”). The combined operation of the provisions is such that where one or more of the exceptions in [subsection 8\(2\)](#) of the *Privacy Act* applies, [subsection 19\(2\)](#) of the *ATIA* permits the personal information to be released as a discretionary matter.

C. Applicable Procedural Provisions and Standard of Review

[38] As noted, this application was commenced before the recent amendments to the *ATIA* came into force. The application was brought under the former [paragraph 42\(1\)\(a\)](#) of the *ATIA*, which permitted the Information Commissioner to apply to this Court for review where a government institution declined to follow a recommendation to disclose information, if the requester has consented, as they did in this case. Such a review is effectively conducted *de novo* (*Merck Frosst* at para [53](#)), a standard confirmed in the recent amendments: *ATIA*, s 44.1.

1507

The former [section 48](#) of the *ATIA* provided that on an application under section 42, the burden of establishing that the government institution is authorized to refuse disclosure is on the government institution. Thus, as the parties agreed, the RCMP had the burden in this case to establish that the serial numbers at issue are “personal information” exempt from disclosure, even though the Information Commissioner is the applicant. Again, the amendments to the *ATIA* do not change this onus: *ATIA*, s 48(1).

[40] The parties are also in agreement as to the applicable standards of review. This Court is to reach its own conclusion as to whether the information at issue is exempt from disclosure under subsection 19(1), *i.e.*, it must determine whether the mandatory exemption has been applied correctly: *Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 at para 19; *Merck Frosst* at para 53. With respect to the exercise of discretion under subsection 19(2), however, the reasonableness standard applies: *Canada (Information Commissioner) v Canada (Prime Minister)*, 2019 FCA 95 at para 31.

[41] If the Court finds that a refusal to disclose under section 19 is not authorized by the *ATIA*, the Court shall order the disclosure of the record, subject to such conditions as the Court deems appropriate, or shall make such other order as the Court deems appropriate: *ATIA*, s 49.

[42] While the parties were in overall agreement with the foregoing principles, they disagreed with certain aspects regarding their application, both in principle and in their application to the information at issue. These disagreements are addressed in the analysis below.

V. Analysis

A. The serial numbers at issue are not “personal information”

(1) Numbers assigned to objects and numbers assigned to individuals

[43] The firearm serial numbers at issue are not inherently personal, in that on their face they neither identify an individual nor reveal any information about an identifiable individual. The numbers are assigned to and associated with a particular firearm, and will remain with that firearm

1508

regardless of who may own or possess the firearm or who may be associated with the firearm in a given database or registry. In this way, the serial numbers are primarily information “about an object,” rather than “about an identifiable individual.”

[44] This was the conclusion of the Alberta Court of Appeal in *Leon’s Furniture Limited v Alberta (Information and Privacy Commissioner)*, 2011 ABCA 94 [*Leon’s*]. A central issue in that case was whether driver’s licence numbers and vehicle licence plate numbers were “personal information” under *Alberta’s Personal Information Protection Act*, SA 2003, c P-6.5 [*PIPA*]. The Alberta statute uses a definition of personal information that is the same as the general definition in the *Privacy Act*, namely “information about an identifiable individual”: *PIPA*, s 1(1)(k). While the *PIPA* definition does not set out a list of examples and exceptions like the *Privacy Act*, examples are provided in the definition of “personal information” in subsection 1(n) of *Alberta’s Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, which has purposes equivalent to aspects of the *ATIA* and the *Privacy Act*.

[45] At paragraph 49 of *Leon’s*, Justice Slatter for the majority concluded that while driver’s licence numbers were personal information, vehicle licence plate numbers were not:

The adjudicator’s conclusion that the driver’s licence number is “personal information” is reasonable, because it (like a social insurance number or a passport number) is uniquely related to an individual. With access to the proper database, the unique driver’s licence number can be used to identify a particular person: *Gordon* [...] at paras. 32-4. But a vehicle licence is a different thing. It is linked to a vehicle, not a person. The fact that the vehicle is owned by somebody does not make the licence plate number information about that individual. It is “about” the vehicle. The same reasoning would apply to vehicle information (serial or VIN) numbers of vehicles. Likewise a street address identifies a property, not a person, even though someone may well live in the property. The licence plate number may well be connected to a database that contains other personal information, but that is not determinative. The appellant had no access to that database, and did not insist that the customer provide access to it. [Emphasis added; citation abbreviated.]

[46] Justice Conrad in dissent agreed with the conclusion of the majority regarding driver’s licence numbers, but would also have upheld the adjudicator’s conclusion that licence plate numbers were

1509

personal information.” While recognizing that the question was “not as clear” as for a driver’s licence number, Justice Conrad noted that as with a driver’s licence number, a licence plate number “when searched in the appropriate database, also produces information about the owner”: *Leon’s* at para 119.

[47] Both sets of reasons in *Leon’s* recognized that numbers that are assigned to an object are qualitatively different from those that are assigned to an individual. A number that is assigned to an individual, such as a social insurance number, health insurance number or passport number, is inherently “personal” and is recognized as “personal information” by the example in [subsection 3\(c\)](#) of the *Privacy Act*: “any identifying number, symbol or other particular assigned to the individual.” [Emphasis added.] Such information is exempt from disclosure under [section 19\(1\)](#) of the *ATIA*, without the need to establish that it could be used to obtain further personal information.

[48] A number that is assigned to an object does not have this feature of being inherently personal. The serial numbers at issue are of this nature: they are assigned to a particular firearm rather than to an individual, they do not on their face reveal personal information, and they do not fall within [subsection 3\(c\)](#) of the *Privacy Act*. However, this does not end the inquiry. As set out in *Dagg*, the question remains whether the serial numbers fall within the general definition of “personal information” by being “about an identifiable individual.” In such a case, as the RCMP submits, the information would be about both the object and the individual.

(2) The test for assessing whether information is “about” an identifiable person

[49] Even facially impersonal information may be “personal information” if it is associated with an identifiable individual in a manner or context that reveals personal information. Thus, for example, this Court in *Gordon* found that the “province” field in the Canadian Adverse Drug Reactions Information System (CADRIS) was personal information, since it could be used together with released CADRIS information and other public information such as obituaries to greatly increase the ability to identify particular individuals. In the present case, if the firearm

should numbers could be linked with identifiable individuals, this would reveal that those individuals were gun owners, which the parties agreed is “personal information.”

[50] As set out above, the Court in *Gordon* phrased the relevant question as being whether there is a “serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.” In *NavCanada*, the Federal Court of Appeal described an identifiable individual as “someone whom it is reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available.”

[51] The parties expressed disagreement with respect to three aspects of these tests: the nature of the “serious possibility” and “reasonable to expect” standards; the scope of “available information” to be considered for purposes of the assessment; and the Information Commissioner’s reliance on *NavCanada*.

(a) “*serious possibility*”/“*reasonable to expect*”

[52] The Information Commissioner submitted that the “serious possibility” and “reasonable to expect” standards were substantially the same. They submitted that “reasonable to expect” was equivalent to the “could reasonably be expected” language in [paragraph 20\(1\)\(c\)](#) of the *ATIA*, which was interpreted in *Merck Frosst* as an “expectation for which real and substantial grounds exist when looked at objectively”: *Merck Frosst* at para [204](#). The Minister disputed the applicability of *Merck Frosst*, noting that it addressed a statutory test for establishing harm, and that the section 19 exemption is a class exemption and not an injury-based one.

[53] I agree that standards and approaches applicable to [section 20](#) of the *ATIA* are not necessarily applicable to section 19, given the different nature of the interests at stake in the two sections. At the same time, however, the “serious possibility” of *Gordon* and the “reasonable to expect” of *NavCanada* both appear to convey effectively the same standard: a possibility that is greater than speculation or a “mere possibility,” but does not need to reach the level of “more likely than not”

1511

need not be “probable” on a balance of probabilities). Applying such a standard recognizes the importance of access to information by not exempting information from disclosure on the basis of mere speculative possibilities, while respecting the importance of privacy rights and the inherently prospective nature of the analysis by not requiring an unduly high degree of proof that personal information will be released.

[54] Beyond this, it seems unnecessary, and may even be impossible, to try to further subdivide or parse the requisite degree of likelihood that an individual could be identified. For ease of reference, and since both parties accepted the formulation of *Gordon*, I will use the “serious possibility” language to express the applicable standard described above.

(b) “*available information*”

[55] The parties have a more substantial disagreement regarding what should be considered “available information” for assessing whether the information at issue, in combination with other available information, could identify an individual. Is it only information that is available to the general public? Does it include more narrowly available information? Or could it even include information that is only in the hands of the government or the requester?

[56] The issue arises since the RCMP asserts that access to the serial numbers could lead to disclosure of personal information in several different ways. First, the RCMP argues that if the serial numbers were released, the owners of the firearms could each identify themselves by linking their own firearm serial number to the information disclosed. Second, the RCMP argues that the serial numbers could be linked to personal information contained in one of four government databases, namely the CFIS database, the Canadian Police Information Centre (CPIC) database, the Canadian Firearms Registry On-line (CFRO) database, and the Public Agents Firearms database. Third, the RCMP argues that the serial numbers could be linked to personal information in the hands of private businesses, such as firearms manufacturers or shooting clubs. In the RCMP’s submission, for information to fall outside the exemption in subsection 19(1), it should

1512

not be seriously possible for *anyone* to identify an individual, including the government institution itself or the very person to whom the information relates.

[57] The Information Commissioner, on the other hand, suggested that information should only be considered “available information” if it is publicly available, relying on passages in *Gordon* that refer to disclosure “in conjunction with other publicly available information.” The Information Commissioner accepted that the information need not be easily available, but suggested that it must be available to an “informed and knowledgeable member of the public.”

[58] In my view, the appropriate approach to “available information” lies between the Minister’s position and that of the Information Commissioner.

[59] I agree with the Information Commissioner that information that is kept confidential in the hands of the government institution cannot be considered “available” for purposes of the analysis. Information requested under the *ATIA* is by definition already held by a government institution. The purpose of [section 19\(1\)](#) of the *ATIA* is to avoid disclosing personal information to requesters, not to avoid “disclosing” it to the government institution that already has it.

[60] If information were to be considered personal information simply because the government institution could itself use it to identify an individual, this would effectively capture (and exempt from disclosure) a wide variety of impersonal information. Indeed, in the present case, any and all of the information in the chart at issue could be considered “personal information” on the RCMP’s approach since the RCMP—being in possession of the unredacted chart and having access to the databases—could use it to identify an individual. The same is true of a variety of documents that are commonly released with personal information such as names and addresses removed; the government institution itself would remain able to “identify” the individuals whose names have been removed simply by referring to the original document.

1513

Similarly, the fact that an individual may be able to identify themselves from released information does not make that information “personal information.” The goal of the *Privacy Act* and subsection 19(1) of the *ATIA* is to prevent the undue disclosure of one’s personal information to others, not to oneself. Indeed, the *Privacy Act* expressly provides individuals with a right of access to personal information about themselves in the hands of a government institution: *Privacy Act* at ss 2, 12. That an individual might know that it is their name that is redacted from a document, for example, does not make the remainder of the document personal information.

[62] On the other hand, limiting the approach to “available information” to information that is available to the public at large, even an “informed and knowledgeable member of the public” as proposed by the Information Commissioner, risks an inappropriate disclosure of personal information and undermines the “paramount” status of privacy rights. The importance of privacy rights is such that unauthorized release of personal information should be avoided, even if only some members of the public could draw the connections that would link the information to an identifiable individual.

[63] An example will help illustrate the concern. An employer will often have information regarding its employees that is not available to the general public. Information in a released record might allow the employer to use their special knowledge to identify an employee even if an “informed and knowledgeable member of the public” could not. The result could be the disclosure of personal information to the employer—health information, financial status, union activities, or other personal information—that they are not already privy to, contrary to the objectives of the *ATIA* and the *Privacy Act*. Thus even information not available to an informed and knowledgeable member of the general public may potentially be used to identify an individual and result in the inappropriate release of personal information.

[64] At the same time, if the record to be released would only repeat information already known to the employer (e.g., if they already possess an unredacted copy of the record in question), then the employer’s ability to “identify” the individual from the information may not mean that personal information would be disclosed by releasing the record.

1514

That “available information” may go beyond what is in the hands of an “informed and knowledgeable member of the public” is consistent with both *Gordon* and *NavCanada*. Justice Gibson in *Gordon* did conclude that the “province” field at issue in that case could be used in conjunction with other “publicly available information” to identify individuals. However, Justice Gibson does not appear to have intended to limit the analysis to information available to the public at large. At paragraphs 33-34 of his reasons, he referred to the relevant available information as “including” publicly available sources, and adopted the Privacy Commissioner’s formulation, which does not include the “publicly available” qualifier:

Thus, information recorded in any form is information “about” a particular individual if it “permits” or “leads” to the possible identification of the individual, whether alone or when combined with information from sources “otherwise available” including sources publicly available.

Counsel for the Privacy Commissioner, the Intervener, urged the adoption of the following test in determining when information is about an identifiable individual:

Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

I am satisfied that the foregoing is an appropriate statement of the applicable text. [Emphasis added.]

[66] Similarly, in *NavCanada*, the Court of Appeal adopted the “reasonable to expect” formulation referring simply to “sources otherwise available” without requiring that it be publicly available: *NavCanada* at para 43. In doing so, the Court of Appeal cited *Ontario (Attorney General) v Pascoe*, 2001 CanLII 32755 (ONSCDC), aff’d 2002 CanLII 30891 (ONCA) [*Pascoe*]. There, the Ontario Divisional Court noted that a person might be identifiable from a record “where he or she could be identified by those familiar with the particular circumstances or events contained in the record.” [Emphasis added]: *Pascoe* at para 15. The Divisional Court thus recognized that the information may be held by a smaller subset of the public and still be considered “available” in assessing whether an individual may be identified as the result of information being released.

As will be clear from the illustrative example given above and the facts in *Gordon*, *NavCanada* and *Pascoe*, the assessment of whether there is a serious possibility that an individual could be identified—by someone other than the government institution or the individual themselves—will of necessity be dependent on the particular facts, including the type of information at issue, the context in which it appears in the records at issue, and the nature of the other information that is available. The ultimate question is and should remain focused on whether release of the record will result in the disclosure of personal information, either directly or through the serious possibility that an individual could be identified.

[68] I note for clarity that [subsection 8\(2\)](#) of the *Privacy Act* contains provisions regarding the disclosure of information from one government entity to another. Those provisions do not arise in this matter and nothing in the foregoing should be taken as affecting that question.

(c) *Relevance of the “concept of privacy”*

[69] The RCMP submitted that the Information Commissioner’s reliance on *NavCanada* reflected an overly narrow approach to the concept of “personal information” by requiring that information touch on “concepts of intimacy, identity, dignity and integrity of the individual”: *NavCanada* at paras [52-54](#). The RCMP argued that the broader approach reflected in *Canada (Minister of Health) v Janssen-Ortho Inc.*, 2007 FCA 252 [*Janssen-Ortho*] is to be preferred.

[70] There has been suggestion that these two cases from the Federal Court of Appeal represent different approaches to personal information that have to be resolved. In recent companion cases, *Suncor Energy Inc v Canada-Newfoundland and Labrador Offshore Petroleum Board*, 2018 FCA [11](#) [*Suncor*] and *Husky Oil*, the Federal Court of Appeal was invited to resolve the “apparent contradiction” between *NavCanada* and *Janssen-Ortho*: *Suncor* at para [16](#); *Husky Oil* at paras [33](#), [59](#). While Justice de Montigny addressed this question, noting that in his view “these two decisions are not necessarily inconsistent,” the majority of the Court felt it unnecessary to do so: *Husky Oil* at paras [33-46](#) *per de Montigny* JA, paras [56](#), [59-60](#) *per Gauthier* JA.

1516

In the present case, the issue does not arise and the approaches in the two cases need not be addressed at length for two reasons. First, the Information Commissioner relies on *NavCanada* not for its discussion of the concept of privacy, but for its conclusion that an identifiable individual is one whom it is “reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available.” As noted above, that test is effectively the same as the test in *Gordon*, which relied on *NavCanada* and which the RCMP accepts. Second, the parties did not dispute—and the Court agrees—that whether an individual is a firearm owner constitutes personal information, regardless of whether it is viewed through the lens of *NavCanada* or *Janssen-Ortho*. To the extent that there is a difference in approach reflected in *NavCanada* and *Janssen-Ortho*, it does not affect the assessment in the current case.

- (3) There is no serious possibility that the firearm serial numbers could be used to identify an individual

[72] As set out above, the RCMP argues that if the serial numbers were released, individuals could be identified as owners of the firearms by (i) the individuals themselves recognizing their own firearm serial number; (ii) the government institution using information contained in the CFIS, CPIC, CFRO or Public Agents Firearms databases; or (iii) a third party, using the serial number(s) to obtain information from one of these databases or from a private business, such as firearms manufacturers or shooting clubs.

[73] I have explained above why I reject the RCMP’s contention that the serial numbers are “personal information” based on an individual’s ability to identify their own serial number. Similarly, I have explained why the government’s own ability to access one of the identified databases and correlate the serial number with a name does not make the serial number personal information.

[74] The RCMP’s expert, Mr. Smith, confirmed that the identified databases are government data banks, and that there are security measures in effect regarding access to them. Those with access to the database already have access to the serial number, the name and all other personal information contained in the database. Release of the serial number would therefore add nothing to their ability

1517

to access both the serial number and the personal information in the database. Mr. Smith, perhaps not surprisingly, did not give evidence suggesting that unauthorized individuals would have any serious possibility of accessing the restricted firearms databases, or that their ability to do so would be increased by having the serial numbers. Such information cannot be considered “available information” for purposes of assessing whether an individual could be identified as the result of release of the serial numbers.

[75] Mr. Smith did give evidence that there is a website associated with the CPIC database that allows the public to input a serial number to determine whether a firearm has been reported stolen. He suggested that with this information and other publicly available information, such as news reports of crime events, this could allow the serial number to be linked to a particular individual. While this evidence comes closer to the type of evidence at issue in *Gordon*, it is insufficient to go beyond mere speculation. There was no evidence filed that any of the Sig Sauer firearms in question were stolen or would be identified on the public website—Mr. Smith did not conduct such searches—or that even if they were, how crime reports could be used to link the serial number to a particular individual. This is in contrast to the evidence provided in *Gordon*, which showed that information from the CADRIS database had in fact been used to identify individuals, and that the disclosure of the “province” field increased the possibility of that occurring: *Gordon* at paras 35-43.

[76] Mr. Smith also asserted that having the serial numbers could permit someone to obtain personal information from private businesses, namely the manufacturer or a gun club. This could be done in one of two ways. First, some manufacturers will provide what is termed a “factory letter,” based on the make, model and serial number of the firearm. The factory letter sets out when the firearm was manufactured and sold, and to whom it was first sold (which could be an individual, a business or a government entity). Regardless of whether such information might be obtained in certain cases, the evidence was that Sig Sauer does not provide factory letters, so it can have no bearing on whether the serial numbers at issue are personal information.

1518

Second, Mr. Smith suggested that the serial number could be used to fraudulently obtain personal information from Sig Sauer, such as a name and address associated with a warranty registration. While this might be possible in theory, Mr. Smith provided no evidence regarding how Sig Sauer responds to requests for information, or how likely it would be that Sig Sauer would have or could be convinced to release that information. In the absence of further evidence, the suggestion that an individual could use the serial numbers to trick Sig Sauer into releasing personal information remains in the realm of speculation or “mere possibility.” I am not satisfied that the evidence shows that this is a serious possibility.

[78] Similarly, there is no evidence beyond speculation about the ability to use the serial numbers to obtain information from gun clubs. Mr. Smith indicated that the extent to which gun clubs collect personal information regarding members or visitors varies depending on the club. In any event, to the extent that a gun club obtains personal information, its use and protection of that information would be subject to privacy legislation, provincially or under the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5. Again, there was no evidence beyond mere speculation that would satisfy the RCMP’s onus to demonstrate that there is a serious possibility that an individual with access to the serial numbers could use it to convince a gun club or other business to circumvent their privacy obligations.

[79] Finally, I note that Mr. Smith gave evidence that some firearms are sufficiently rare that only one is present in Canada, such that the make and model may alone be enough to uniquely identify the firearm and link it to an individual. Accepting that this may be so, it is not the case with the Sig Sauer P226 firearms that are at issue in this case.

[80] I therefore conclude that there is no serious possibility that the Sig Sauer firearm serial numbers at issue could be used, alone or in combination with other available information, to identify an individual. The serial numbers are not “personal information” within the meaning of [section 3](#) of the *Privacy Act* and are not exempt from disclosure under [subsection 19\(1\)](#) of the *ATIA*.

1519

While Mr. Smith gave brief evidence, which he described as “additional considerations,” regarding the potential for use of serial numbers in other manners that might have a negative impact on law enforcement, this evidence was scant, and no claim was made by the RCMP that the serial numbers were exempt from disclosure pursuant to [section 16](#) of the *ATIA*. As no other basis for redaction was asserted by the RCMP, the serial numbers at issue will be ordered released to the requester.

B. The RCMP did not reasonably exercise its discretion under subsection 19(2) of the ATIA

[82] Having determined that the information was personal information exempt from disclosure under [subsection 19\(1\)](#) of the *ATIA*, the RCMP concluded that it should not exercise its discretion under subsection 19(2) to nevertheless release the information. As set out above, subsection 19(2) permits the head of a government institution to release the information as a discretionary matter where (a) the individual to whom it relates consents to the disclosure, (b) the information is publicly available, or (c) the disclosure is in accordance with [section 8](#) of the *Privacy Act*.

[83] As I have found that the information in question is not personal information, subsection 19(2) does not come into play. Had I concluded otherwise, I would have found that the matter should be sent back to the RCMP for redetermination, as there is no indication that the RCMP gave substantive consideration to the release of the information in the public interest.

[84] In their letter of submission to the Information Commissioner in the course of the investigation, the RCMP stated the following regarding the exercise of discretion under subsection 19(2):

As required during the course of our review, due consideration was given to the exercise of discretion as outlined in subsection 19(2) of the Act. It was established during the course of the exercise that there was no existence of consent and no likelihood of consent from individual gun owners could be obtained and would be [*sic*] unreasonable to attempt consent for release. The information ultimately withheld under 19(1) in this instance had not been previously made public. Finally, the test governing a disclosure in the public interest could not be met.

1520

Similarly, on this application, Ms. Holub provided the following evidence regarding the exercise of discretion:

The RCMP also considered the potential exercise of discretion under [subsection 19\(2\)](#) of the *ATIA*. In making the determination that discretion should not be exercised to disclose the serial numbers, the following factors were considered: (a) no consent to disclosure existed from the individual firearm owners, obtaining their consent was unlikely and attempting to obtain their consent would be unreasonable; (b) the serial numbers have not been made public; and (c) it was not in the public interest to disclose the serial numbers.

[86] The foregoing evidence confirms that [paragraphs 19\(2\)\(a\)](#) and [\(b\)](#) of the *ATIA* are not applicable, since there was no consent to release from those affected, and the serial numbers are not already public. However, with respect to [paragraph 19\(2\)\(c\)](#), the RCMP's analysis appears to be limited to bald statements that "the test governing a disclosure in the public interest could not be met" and "it was not in the public interest to disclose the serial numbers." While these statements indicate that the RCMP is aware of and has at least turned its mind to [subparagraph 8\(2\)\(m\)\(i\)](#) of the *Privacy Act*, they contain no statement of the grounds for the conclusion reached.

[87] Where a decision-maker has provided no grounds at all for having exercised their discretion, a reviewing court is effectively prevented from assessing whether the decision is a reasonable one. As the Federal Court of Appeal noted in *Leahy v Canada (Citizenship and Immigration)*, [2012 FCA 227](#) at para [121](#):

If the reasons for decision are non-existent, opaque or otherwise indiscernible, and if the record before the administrative decision-maker does not shed light on the reasons why the administrative decision-maker decided or could have decided in the way it did, the requirement that administrative decisions be transparent and intelligible is not met... [Citations omitted.]

[88] Similarly, Justice Simon Noël of this Court stated in *Canada (Information Commissioner) v Canada (Transport)*, [2016 FC 448](#) at para [66](#) that in exercising a discretion under the *ATIA*, "the decision-maker cannot simply state that he has considered all of the relevant factors; he must concretely demonstrate how he has considered them."

1521

[79] In the present case, neither the reasons nor the record provides any indication as to why or how the RCMP reached its conclusion regarding public interest. The RCMP pointed to two aspects of the record as providing a reasonable basis for the exercise of discretion. I disagree that either provides any explanation as to why the RCMP exercised the discretion as it did.

[90] First, the RCMP pointed to Mr. Smith's opinion that in light of "the impact on individuals, the effect on law enforcement, and the current practice of non-disclosure of the serial number information, that it is not good public policy, or in the public interest, to disclose serial numbers of firearms." However, as counsel accepted during argument, Mr. Smith was presented as an independent expert and not as a witness to attest to the RCMP's reasons for the exercise of the discretion. There is no evidence that the issues considered by Mr. Smith were considered by the access officer. In any event, Mr. Smith's evidence does not address the issue raised in [subparagraph 8\(1\)\(m\)\(i\)](#) of the *Privacy Act*, namely whether the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

[91] Second, during oral argument counsel suggested that the RCMP's letter to the Information Commissioner showed that in exercising discretion under paragraph 19(2)(c), the RCMP considered that there was no consent to release from the individuals and that the information was not otherwise public. However, these are simply the circumstances in which discretion may be exercised under paragraphs 19(2)(a) or (b). Paragraph 19(2)(c) is set out in the *ATIA* as a separate basis for the exercise of discretion. Even if these were the reasons given for exercise of discretion under paragraph 19(2)(c) and not—as it appears—the RCMP's conclusions with respect to paragraphs 19(2)(a) and (b), it would be insufficient and unreasonable to simply conclude that the discretion under paragraph 19(2)(c) should not be exercised because the circumstances of paragraphs 19(2)(a) and (b) are not met.

[92] I hasten to point out that the explanation given for a decision on the exercise of discretion under paragraph 19(2)(c) of the *ATIA* and [subparagraph 8\(2\)\(m\)\(i\)](#) of the *Privacy Act* need not be extensive or detailed. Similarly, an explanation need not be given for every paragraph in subsection 8(2) where, as here, it is perfectly clear that most of the exceptions can have no

1522

a application at all. However, exercise of the discretion requires a sufficiently “transparent and intelligible” explanation of why it is considered that the public interest in disclosure does or does not clearly outweigh the relevant invasion of privacy. The RCMP did not meet that standard.

VI. Conclusion

[93] The only ground raised for refusing release of the firearm serial numbers was that the numbers were “personal information.” I conclude that the serial numbers are not “personal information” within the definition of [section 3](#) of the *Privacy Act*. Having found that the refusal to disclose is not authorized by [subsection 19\(1\)](#) of the *ATIA*, and in accordance with [section 49](#) of the *ATIA*, the firearm serial numbers shall be ordered released to the requester. Neither party requested costs, and no costs are ordered.

JUDGMENT IN T-1682-18

THIS COURT’S JUDGMENT is that

1. The record identified by the Royal Canadian Mounted Police as responsive to the request for access made under the [Access to Information Act](#) shall be released to the requester without redaction of the Sig Sauer P226 firearm serial numbers.
2. There is no order as to costs.

“Nicholas McHaffie”

Judge

APPENDIX A

Statutory Provisions as They Read at the Time of the Complaint

[Access to Information Act](#), RSC 1985, c A-1

Purpose

2 (1) The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in acc

Objet

2 (1) La présente loi a pour objet d’élargir l’accès aux documents de l’administration fédérale en consacrant le principe du droit du public à leur communication, les exceptio

1523

accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government.

ns indispensables à ce droit étant précises et limitées et les décisions quant à la communication étant susceptibles de recours indépendants du pouvoir exécutif.

Complementary procedures

Étoffement des modalités d'accès

(2) This Act is intended to complement and not replace existing procedures for access to government information and is not intended to limit in any way access to the type of government information that is normally available to the general public.

(2) La présente loi vise à compléter les modalités d'accès aux documents de l'administration fédérale; elle ne vise pas à restreindre l'accès aux renseignements que les institutions fédérales mettent normalement à la disposition du grand public.

Right to access to records

Droit d'accès

4 (1) Subject to this Act, but notwithstanding any other Act of Parliament, every person who is

4 (1) Sous réserve des autres dispositions de la présente loi mais nonobstant toute autre loi fédérale, ont droit à l'accès aux documents relevant d'une institution fédérale et peuvent se les faire communiquer sur demande :

(a) a Canadian citizen, or

a) les citoyens canadiens;

(b) a permanent resident within the meaning of [subsection 2\(1\)](#) of the *Immigration and Refugee Protection Act*,

b) les résidents permanents au sens du [paragraphe 2\(1\)](#) de la *Loi sur l'immigration et la protection des réfugiés*.

has a right to and shall, on request, be given access to any record under the control of a government institution.

[...]

[...]

Personal information

Renseignements personnels

19 (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Act that contains personal information as defined in [section 3](#) of the *Privacy Act*.

19 (1) Sous réserve du paragraphe (2), le responsable d'une institution fédérale est tenu de refuser la communication de documents contenant les renseignements personnels visés à l'[article 3](#) de la *Loi sur la protection des renseignements personnels*.

1524**Where disclosure authorized**

(2) The head of a government institution may disclose any record requested under this Act that contains personal information if

(a) the individual to whom it relates consents to the disclosure;

(b) the information is publicly available; or

(c) the disclosure is in accordance with [section 8](#) of the *Privacy Act*.

Cas où la divulgation est autorisée

(2) Le responsable d'une institution fédérale peut donner communication de documents contenant des renseignements personnels dans les cas où :

a) l'individu qu'ils concernent y consent;

b) le public y a accès;

c) la communication est conforme à l'[article 8](#) de la *Loi sur la protection des renseignements personnels*.

Receipt and investigation of complaints

30 (1) Subject to this Act, the Information Commissioner shall receive and investigate complaints

(a) from persons who have been refused access to a record requested under this Act or a part thereof;

[...]

(f) in respect of any other matter relating to requesting or obtaining access to records under this Act.

[...]

Notice of intention to investigate

32 Before commencing an investigation of a complaint under this Act, the Information Commissioner shall notify the head of the government institution concerned of the inte

Réception des plaintes et enquêtes

30 (1) Sous réserve des autres dispositions de la présente loi, le Commissaire à l'information reçoit les plaintes et fait enquête sur les plaintes :

a) déposées par des personnes qui se sont vu refuser la communication totale ou partielle d'un document qu'elles ont demandé en vertu de la présente loi;

[...]

f) portant sur toute autre question relative à la demande ou à l'obtention de documents en vertu de la présente loi.

[...]

Avis d'enquête

32 Le Commissaire à l'information, avant de procéder aux enquêtes prévues par la présente loi, avise le responsable de l'institution fédérale concernée de son intention d'enq

1525

tion to carry out the investigation and shall inform the head of the institution of the substance of the complaint.

uêter et lui fait connaître l'objet de la plainte.

Findings and recommendations of Information Commissioner

Conclusions et recommandations du Commissaire à l'information

37 (1) If, on investigating a complaint in respect of a record under this Act, the Information Commissioner finds that the complaint is well-founded, the Commissioner shall provide the head of the government institution that has control of the record with a report containing

37 (1) Dans les cas où il conclut au bien-fondé d'une plainte portant sur un document, le Commissaire à l'information adresse au responsable de l'institution fédérale de qui relève le document un rapport où :

(a) the findings of the investigation and any recommendations that the Commissioner considers appropriate; and

a) il présente les conclusions de son enquête ainsi que les recommandations qu'il juge indiquées;

(b) where appropriate, a request that, within a time specified in the report, notice be given to the Commissioner of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

b) il demande, s'il le juge à propos, au responsable de lui donner avis, dans un délai déterminé, soit des mesures prises ou envisagées pour la mise en oeuvre de ses recommandations, soit des motifs invoqués pour ne pas y donner suite.

Report to complainant and third parties

Compte rendu au plaignant

(2) The Information Commissioner shall, after investigating a complaint under this Act, report to the complainant and any third party that was entitled under subsection 35(2) to make and that made representations to the Commissioner in respect of the complaint the results of the investigation, but where a notice has been requested under paragraph (1)(b) no report shall be made under this subsection until the expiration of the time within which the notice is to be given to the Commissioner.

(2) Le Commissaire à l'information rend compte des conclusions de son enquête au plaignant et aux tiers qui pouvaient, en vertu du paragraphe 35(2), lui présenter des observations et qui les ont présentées; toutefois, dans les cas prévus à l'alinéa (1)b), le Commissaire à l'information ne peut faire son compte rendu qu'après l'expiration du délai imparti au responsable de l'institution fédérale.

Matter to be included in report to complainant

Éléments à inclure dans le compte rendu

(3) Where a notice has been requested under paragraph (1)(b) but no such notice is received by the Commissioner within the time

(3) Le Commissaire à l'information mentionne également dans son compte rendu au plaignant, s'il y a lieu, le fait que, dans les ca

1526

specified therefor or the action described in the notice is, in the opinion of the Commissioner, inadequate or inappropriate or will not be taken in a reasonable time, the Commissioner shall so advise the complainant in his report under subsection (2) and may include in the report such comments on the matter as he thinks fit.

s prévus à l'alinéa (1)b), il n'a pas reçu d'avis dans le délai imparti ou que les mesures indiquées dans l'avis sont, selon lui, insuffisantes, inadaptées ou non susceptibles d'être prises en temps utile. Il peut en outre y inclure tous commentaires qu'il estime utiles.

Access to be given

(4) Where, pursuant to a request under paragraph (1)(b), the head of a government institution gives notice to the Information Commissioner that access to a record or a part thereof will be given to a complainant, the head of the institution shall give the complainant access to the record or part thereof

Communication accordée

(4) Dans les cas où il fait suite à la demande formulée par le Commissaire à l'information en vertu de l'alinéa (1)b) en avisant le Commissaire qu'il donnera communication totale ou partielle d'un document, le responsable d'une institution fédérale est tenu de donner cette communication au plaignant :

(a) forthwith on giving the notice if no notice is given to a third party under paragraph 29(1)(b) in the matter; or

a) immédiatement, dans les cas où il n'y a pas de tiers à qui donner l'avis prévu à l'alinéa 29(1)b);

(b) forthwith on completion of twenty days after notice is given to a third party under paragraph 29(1)(b), if that notice is given, unless a review of the matter is requested under section 44.

b) dès l'expiration des vingt jours suivant l'avis prévu à l'alinéa 29(1)b), dans les autres cas, sauf si un recours en révision a été exercé en vertu de l'article 44.

Right of review

(5) Where, following the investigation of a complaint relating to a refusal to give access to a record requested under this Act or a part thereof, the head of a government institution does not give notice to the Information Commissioner that access to the record will be given, the Information Commissioner shall inform the complainant that the complainant has the right to apply to the Court for a review of the matter investigated.

Recours en révision

(5) Dans les cas où, l'enquête terminée, le responsable de l'institution fédérale concernée n'avise pas le Commissaire à l'information que communication du document ou de la partie en cause sera donnée au plaignant, le Commissaire à l'information informe celui-ci de l'existence d'un droit de recours en révision devant la Cour.

Review by Federal Court

41 Any person who has been refused access to a record requested under this Act or a part thereof may, if a complaint has been made to the Information Commissioner in respect

Révision par la Cour fédérale

41 La personne qui s'est vu refuser communication totale ou partielle d'un document demandé en vertu de la présente loi et qui a déposé ou fait déposer une plainte à ce sujet

1527

of the refusal, apply to the Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Information Commissioner are reported to the complainant under subsection 37(2) or within such further time as the Court may, either before or after the expiration of those forty-five days, fix or allow.

t devant le Commissaire à l'information peut, dans un délai de quarante-cinq jours suivant le compte rendu du Commissaire prévu au paragraphe 37(2), exercer un recours en révision de la décision de refus devant la Cour. La Cour peut, avant ou après l'expiration du délai, le proroger ou en autoriser la prorogation.

Information Commissioner may apply or appear

Exercice du recours par le Commissaire, etc.

42 (1) The Information Commissioner may

42 (1) Le Commissaire à l'information a qualité pour :

(a) apply to the Court, within the time limits prescribed by section 41, for a review of any refusal to disclose a record requested under this Act or a part thereof in respect of which an investigation has been carried out by the Information Commissioner, if the Commissioner has the consent of the person who requested access to the record;

a) exercer lui-même, à l'issue de son enquête et dans les délais prévus à l'article 41, le recours en révision pour refus de communication totale ou partielle d'un document, avec le consentement de la personne qui avait demandé le document;

(b) appear before the Court on behalf of any person who has applied for a review under section 41; or

b) comparaître devant la Cour au nom de la personne qui a exercé un recours devant la Cour en vertu de l'article 41;

(c) with leave of the Court, appear as a party to any review applied for under section 41 or 44.

c) comparaître, avec l'autorisation de la Cour, comme partie à une instance engagée en vertu des articles 41 ou 44.

[...]

[...]

Burden of proof

Charge de la preuve

48 In any proceedings before the Court arising from an application under section 41 or 42, the burden of establishing that the head of a government institution is authorized to refuse to disclose a record requested under this Act or a part thereof shall be on the government institution concerned.

48 Dans les procédures découlant des recours prévus aux articles 41 ou 42, la charge d'établir le bien-fondé du refus de communication totale ou partielle d'un document incombe à l'institution fédérale concernée.

1528**Order of Court where no authorization to refuse disclosure found****Ordonnance de la Cour dans les cas où le refus n'est pas autorisé**

49 Where the head of a government institution refuses to disclose a record requested under this Act or a part thereof on the basis of a provision of this Act not referred to in section 50, the Court shall, if it determines that the head of the institution is not authorized to refuse to disclose the record or part thereof, order the head of the institution to disclose the record or part thereof, subject to such conditions as the Court deems appropriate, to the person who requested access to the record, or shall make such other order as the Court deems appropriate.

49 La Cour, dans les cas où elle conclut au bon droit de la personne qui a exercé un recours en révision d'une décision de refus de communication totale ou partielle d'un document fondée sur des dispositions de la présente loi autres que celles mentionnées à l'article 50, ordonne, aux conditions qu'elle juge indiquées, au responsable de l'institution fédérale dont relève le document en litige d'en donner à cette personne communication totale ou partielle; la Cour rend une autre ordonnance si elle l'estime indiqué.

Privacy Act, RSC 1985, c P-21

Purpose

2 The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.

Objet

2 La présente loi a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements personnels qui les concernent.

Definitions

3 In this Act

[...]

personal information means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

Définitions

3 Les définitions qui suivent s'appliquent à la présente loi.

[...]

renseignements personnels Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment :

a) les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille;

b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé;

1529

any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of [sections 7, 8 and 26](#) and [section 19](#) of the *Access to Information Act*, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

c) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre;

d) son adresse, ses empreintes digitales ou son groupe sanguin;

e) ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement;

f) toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur;

g) les idées ou opinions d'autrui sur lui;

h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions;

i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet;

toutefois, il demeure entendu que, pour l'application des articles 7, 8 et 26, et de l'[article 19](#) de la *Loi sur l'accès à l'information*, les renseignements personnels ne comprennent pas les renseignements concernant :

j) un cadre ou employé, actuel ou ancien, d'une institution fédérale et portant sur son poste ou ses fonctions, notamment :

1530

(i) the fact that the individual is or was an officer or employee of the government institution,

(i) le fait même qu'il est ou a été employé par l'institution,

(ii) the title, business address and telephone number of the individual,

(ii) son titre et les adresse et numéro du téléphone de son lieu de travail,

(iii) the classification, salary range and responsibilities of the position held by the individual,

(iii) la classification, l'éventail des salaires et les attributions de son poste,

(iv) the name of the individual on a document prepared by the individual in the course of employment, and

(iv) son nom lorsque celui-ci figure sur un document qu'il a établi au cours de son emploi,

(v) the personal opinions or views of the individual given in the course of employment,

(v) les idées et opinions personnelles qu'il a exprimées au cours de son emploi;

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

k) un individu qui, au titre d'un contrat, assure ou a assuré la prestation de services à une institution fédérale et portant sur la nature de la prestation, notamment les conditions du contrat, le nom de l'individu ainsi que les idées et opinions personnelles qu'il a exprimées au cours de la prestation;

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

l) des avantages financiers facultatifs, notamment la délivrance d'un permis ou d'une licence accordés à un individu, y compris le nom de celui-ci et la nature précise de ces avantages;

(m) information about an individual who has been dead for more than twenty years; (*renseignements personnels*)

m) un individu décédé depuis plus de vingt ans. (*personal information*)

[...]

[...]

Disclosure of personal information

Communication des renseignements personnels

8 (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

8 (1) Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article.

Where personal information may be disclosed

Cas d'autorisation

(2) Subject to any other Act of Parliament, personal information under the control of a go

(2) Sous réserve d'autres lois fédérales, la communication des renseignements personnels

1531

Government institution may be disclosed

qui relèvent d'une institution fédérale est autorisée dans les cas suivants :

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

a) communication aux fins auxquelles ils ont été recueillis ou préparés par l'institution ou pour les usages qui sont compatibles avec ces fins;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

b) communication aux fins qui sont conformes avec les lois fédérales ou ceux de leurs règlements qui autorisent cette communication;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

c) communication exigée par subpoena, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de renseignements;

[...]

[...]

(m) for any purpose where, in the opinion of the head of the institution,

m) communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(i) des raisons d'intérêt public justifient clairement nettement une éventuelle violation de la vie privée,

(ii) disclosure would clearly benefit the individual to whom the information relates.

(ii) l'individu concerné en tirerait un avantage certain.

Right of access

12 (1) Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of [subsection 2\(1\)](#) of the *Immigration and Refugee Protection Act* has a right to and shall, on request, be given access to

(a) any personal information about the individual contained in a personal information bank; and

(b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution.

Droit d'accès

12 (1) Sous réserve des autres dispositions de la présente loi, tout citoyen canadien et tout résident permanent au sens du [paragraphe 2 \(1\)](#) de la *Loi sur l'immigration et la protection des réfugiés* ont le droit de se faire communiquer sur demande :

a) les renseignements personnels le concernant et versés dans un fichier de renseignements personnels;

b) les autres renseignements personnels le concernant et relevant d'une institution fédérale, dans la mesure où il peut fournir sur leur localisation des indications suffisamment précises pour que l'institution fédérale puisse les retrouver sans problème sérieux.

APPENDIX B

Current Statutory Provisions as Amended by Bill C-58*Access to Information Act*, RSC 1985, c A-1**Purpose of Act**

2 (1) The purpose of this Act is to enhance the accountability and transparency of federal institutions in order to promote an open and democratic society and to enable public debate on the conduct of those institutions.

Specific purposes of Parts 1 and 2

(2) In furtherance of that purpose,

(a) Part 1 extends the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government; and

(b) Part 2 sets out requirements for the proactive publication of information.

Complementary procedures

(3) This Act is also intended to complement and not replace existing procedures for access to government information and is not intended to limit in any way access to the type of government information that is normally available to the general public.

[...]

Right to access to records

4 (1) Subject to this Part, but notwithstanding any other Act of Parliament, every person who is

(a) a Canadian citizen, or

Objet de la loi

2 (1) La présente loi a pour objet d'accroître la responsabilité et la transparence des institutions de l'État afin de favoriser une société ouverte et démocratique et de permettre le débat public sur la conduite de ces institutions.

Objets spécifiques : parties 1 et 2

(2) À cet égard :

a) la partie 1 élargit l'accès aux documents de l'administration fédérale en consacrant le principe du droit du public à leur communication, les exceptions indispensables à ce droit étant précises et limitées et les décisions quant à la communication étant susceptibles de recours indépendants du pouvoir exécutif;

b) la partie 2 fixe des exigences visant la publication proactive de renseignements.

Étoffement des modalités d'accès

(3) En outre, la présente loi vise à compléter les modalités d'accès aux documents de l'administration fédérale; elle ne vise pas à restreindre l'accès aux renseignements que les institutions fédérales mettent normalement à la disposition du grand public.

[...]

Droit d'accès

4 (1) Sous réserve des autres dispositions de la présente partie mais nonobstant toute autre loi fédérale, ont droit à l'accès aux documents relevant d'une institution fédérale et pe

1533

(b) a permanent resident within the meaning of [subsection 2\(1\)](#) of the *Immigration and Refugee Protection Act*,

has a right to and shall, on request, be given access to any record under the control of a government institution.

[...]

Personal information

19 (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Part that contains personal information.

Where disclosure authorized

(2) The head of a government institution may disclose any record requested under this Part that contains personal information if

(a) the individual to whom it relates consents to the disclosure;

(b) the information is publicly available; or

(c) the disclosure is in accordance with [section 8](#) of the *Privacy Act*.

Receipt and investigation of complaints

30 (1) Subject to this Part, the Information Commissioner shall receive and investigate complaints

(a) from persons who have been refused access to a record requested under this Part or a part thereof;

[...]

(f) in respect of any other matter relating to requesting or obtaining access to records under this Part.

[...]

Notice of intention to investigate

uvent se les faire communiquer sur demande :

a) les citoyens canadiens;

b) les résidents permanents au sens du [paragraphe 2\(1\)](#) de la *Loi sur l'immigration et la protection des réfugiés*.

[...]

Renseignements personnels

19 (1) Sous réserve du paragraphe (2), le responsable d'une institution fédérale est tenu de refuser la communication de documents contenant des renseignements personnels.

Cas où la divulgation est autorisée

(2) Le responsable d'une institution fédérale peut donner communication de documents contenant des renseignements personnels dans les cas où :

a) l'individu qu'ils concernent y consent;

b) le public y a accès;

c) la communication est conforme à l'[article 8](#) de la *Loi sur la protection des renseignements personnels*.

Réception des plaintes et enquêtes

30 (1) Sous réserve des autres dispositions de la présente partie, le Commissaire à l'information reçoit les plaintes et fait enquête sur les plaintes :

a) déposées par des personnes qui se sont vu refuser la communication totale ou partielle d'un document qu'elles ont demandé en vertu de la présente partie;

[...]

f) portant sur toute autre question relative à la demande ou à l'obtention de documents en vertu de la présente partie.

[...]

Avis d'enquête

1534

32 Before commencing an investigation of a complaint under this Part, the Information Commissioner shall notify the head of the government institution concerned of the intention to carry out the investigation and shall inform the head of the institution of the substance of the complaint.

32 Le Commissaire à l'information, avant de procéder aux enquêtes prévues par la présente partie, avise le responsable de l'institution fédérale concernée de son intention d'enquêter et lui fait connaître l'objet de la plainte.

Power to make order

Pouvoir de rendre des ordonnances

36.1 (1) If, after investigating a complaint described in any of paragraphs 30(1)(a) to (e), the Commissioner finds that the complaint is well-founded, he or she may make any order in respect of a record to which this Part applies that he or she considers appropriate, including requiring the head of the government institution that has control of the record in respect of which the complaint is made

36.1 (1) À l'issue d'une enquête sur une plainte visée à l'un des alinéas 30(1)a) à e), le Commissaire à l'information peut, s'il conclut au bien-fondé de la plainte, rendre toute ordonnance qu'il juge indiquée à l'égard d'un document auquel la présente partie s'applique, notamment ordonner au responsable de l'institution fédérale dont relève le document :

(a) to disclose the record or a part of the record; and

a) d'en donner communication totale ou partielle;

(b) to reconsider their decision to refuse access to the record or a part of the record.

b) de revoir sa décision de refuser la communication totale ou partielle du document.

Consulting Privacy Commissioner

Consultation du Commissaire à la protection de la vie privée

36.2 If the Information Commissioner intends to make an order requiring the head of a government institution to disclose a record or a part of a record that the head of the institution refuses to disclose under subsection 19(1), the Information Commissioner shall consult the Privacy Commissioner and may, in the course of the consultation, disclose to him or her personal information.

36.2 S'il a l'intention d'ordonner au responsable d'une institution fédérale de communiquer tout ou partie d'un document que ce dernier refuse de communiquer au titre du paragraphe 19(1), le Commissaire à l'information doit consulter le Commissaire à la protection de la vie privée et peut, dans le cadre de la consultation, lui communiquer des renseignements personnels.

Information Commissioner's initial report to government institution

Rapport à l'institution fédérale

37 (1) If, on investigating a complaint under this Part, the Information Commissioner fin

37 (1) Dans les cas où il conclut au bien-fondé d'une plainte, le Commissaire à l'inform

1535

As that the complaint is well-founded, the Commissioner shall provide the head of the government institution concerned with a report that sets out

ation adresse au responsable de l'institution fédérale concernée un rapport où :

(a) the findings of the investigation and any recommendations that the Commissioner considers appropriate;

a) il présente les conclusions de son enquête ainsi que les recommandations qu'il juge indiquées;

(b) any order that the Commissioner intends to make; and

b) il présente toute ordonnance qu'il a l'intention de rendre;

(c) the period within which the head of the government institution shall give notice to the Commissioner of the action taken or proposed to be taken to implement the order or recommendations set out in the report or reasons why no such action has been or is proposed to be taken.

c) il spécifie le délai dans lequel le responsable de l'institution fédérale doit lui donner avis soit des mesures prises ou envisagées pour la mise en oeuvre de l'ordonnance ou des recommandations, soit des motifs invoqués pour ne pas y donner suite.

Final report to complainant, government institution and other persons

Compte rendu au plaignant, à l'institution fédérale et autres personnes concernées

(2) The Information Commissioner shall, after investigating a complaint under this Part, provide a report that sets out the results of the investigation and any order or recommendations that he or she makes to

(2) Le Commissaire à l'information rend compte des conclusions de son enquête, de toute ordonnance qu'il rend et de toute recommandation qu'il formule :

(a) the complainant;

a) au plaignant;

(b) the head of the government institution;

b) au responsable de l'institution fédérale;

(c) any third party that was entitled under paragraph 35(2)(c) to make and that made representations to the Commissioner in respect of the complaint; and

c) aux tiers qui pouvaient, en vertu de l'alinéa 35(2)c), lui présenter des observations et qui lui en ont présentées;

(d) the Privacy Commissioner, if he or she was entitled under paragraph 35(2)(d) to make representations and he or she made representations to the Commissioner in respect of the complaint. However, no report is to be made under this subsection and no order is to be made until the expiry of the time within which the notice referred to in paragraph (1)(c) is to be given to the Information Commissioner.

d) au Commissaire à la protection de la vie privée si celui-ci pouvait, en vertu de l'alinéa 35(2)d), lui présenter des observations et lui en a présentées. Toutefois, le Commissaire à l'information ne peut faire son compte rendu ou rendre une ordonnance qu'après l'expiration du délai imparti au responsable de l'institution fédérale au titre de l'alinéa (1)c).

Contents of report

Contenu du compte rendu

1536

(3) The Information Commissioner may include in the report referred to in subsection (2) any comments on the matter that he or she thinks fit and shall include in that report

(a) a summary of any notice that he or she receives under paragraph (1)(c);

(b) a statement that any person to whom the report is provided has the right to apply for a review under section 41, within the period specified for exercising that right, and that the person must comply with section 43 if they exercise that right;

(c) a statement that if no person applies for a review within the period specified for doing so, any order set out in the report takes effect in accordance with subsection 36.1(4); and

(d) a statement, if applicable, that the Information Commissioner will provide a third party or the Privacy Commissioner with the report.

Publication

(3.1) The Information Commissioner may publish the report referred to in subsection (2).

Limitation

(3.2) However, the Information Commissioner is not to publish the report until the expiry of the periods to apply to the Court for a review of a matter that are referred to in section 41.

Access to be given

(4) If the head of a government institution gives notice to the Information Commissioner under paragraph (1)(c) that access to a record or a part of a record will be given to a complainant, the head of the institution shall give the complainant access to the record or the part of the record

(a) on receiving the report under subsection (2) or within any period specified in the Commissioner's order, if only the complainant and the head of the institution are provided with the report; or

(3) Le Commissaire à l'information peut inclure dans son compte rendu tous commentaires qu'il estime utiles. En outre, il doit y inclure les éléments suivants :

a) un résumé de tout avis reçu en application de l'alinéa (1)c);

b) la mention du droit de tout destinataire du compte rendu d'exercer un recours en révision au titre de l'article 41 et du délai pour ce faire, ainsi que du fait que s'il exerce ce droit, il doit se conformer à l'article 43;

c) la mention qu'à défaut de l'exercice du recours en révision dans ce délai, toute ordonnance contenue dans le compte rendu prendra effet conformément au paragraphe 36.1(4);

d) si un tiers ou le Commissaire à la protection de la vie privée sont des destinataires du compte rendu, la mention de ce fait.

Publication

(3.1) Le Commissaire à l'information peut publier le compte rendu visé au paragraphe (2).

Délai

(3.2) Il ne peut toutefois le publier avant l'expiration des délais prévus à l'article 41 pour l'exercice d'un recours en révision devant la Cour.

Communication accordée

(4) Dans les cas où il avise le Commissaire à l'information, en application de l'alinéa (1)c), qu'il donnera communication totale ou partielle d'un document, le responsable de l'institution fédérale est tenu de donner cette communication au plaignant :

a) dès la réception du compte rendu visé au paragraphe (2) ou dans tout délai imparté dans l'ordonnance du Commissaire, dans les cas où seuls le plaignant et le re

(b) on the expiry of the 40th business day after the day on which the head of the government institution receives the report under subsection (2) or within any period specified in the Commissioner's order that begins on the expiry of that 40th business day, if a third party or the Privacy Commissioner are also provided with the report, unless a review is applied for under section 41.

Deemed date of receipt

(5) For the purposes of this section, the head of the government institution is deemed to have received the report referred to in subsection (2) on the fifth business day after the date of the report.

Review by Federal Court — complainant

41 (1) A person who makes a complaint described in any of paragraphs 30(1)(a) to (e) and who receives a report under subsection 37(2) in respect of the complaint may, within 30 business days after the day on which the head of the government institution receives the report, apply to the Court for a review of the matter that is the subject of the complaint.

Review by Federal Court — government institution

(2) The head of a government institution who receives a report under subsection 37(2) may, within 30 business days after the day on which they receive it, apply to the Court for a review of any matter that is the subject of an order set out in the report.

Review by Federal Court — third parties

(3) If neither the person who made the complaint nor the head of the government institution makes an application under this section within the period for doing so, a third party who receives a report under subsection 37(2) may, within 10 business days after the expiry of the period referred to in subsection

sponsable de l'institution sont les destinataires du compte rendu;

b) dès l'expiration du quarantième jour ouvrable suivant la date à laquelle le responsable de l'institution fédérale reçoit le compte rendu en application du paragraphe (2) ou dans tout délai imparti dans l'ordonnance suivant l'expiration de ce quarantième jour ouvrable, si un tiers ou le Commissaire à la protection de la vie privée sont également des destinataires du compte rendu, sauf si un recours en révision a été exercé au titre de l'article 41.

Date réputée de réception

(5) Pour l'application du présent article, le responsable de l'institution fédérale est réputé avoir reçu le compte rendu visé au paragraphe (2) le cinquième jour ouvrable suivant la date que porte le compte rendu.

Révision par la Cour fédérale : plaignant

41 (1) Le plaignant dont la plainte est visée à l'un des alinéas 30(1)a) à e) et qui reçoit le compte rendu en application du paragraphe 37(2) peut, dans les trente jours ouvrables suivant la réception par le responsable de l'institution fédérale du compte rendu, exercer devant la Cour un recours en révision des questions qui font l'objet de sa plainte.

Révision par la Cour fédérale : institution fédérale

(2) Le responsable d'une institution fédérale qui reçoit le compte rendu en application du paragraphe 37(2) peut, dans les trente jours ouvrables suivant la réception du compte rendu, exercer devant la Cour un recours en révision de toute question dont traite l'ordonnance contenue dans le compte rendu.

Révision par la Cour fédérale : tiers

(3) Si aucun recours n'est exercé en vertu des paragraphes (1) ou (2) dans le délai prévu à ces paragraphes, le tiers qui reçoit le compte rendu en application du paragraphe 37(2) peut, dans les dix jours ouvrables suivant l'expiration du délai prévu au paragraphe (1), exercer devant la Cour un recours en ré

1538

(4), apply to the Court for a review of the application of any exemption provided for under this Part that may apply to a record that might contain information described in subsection 20(1) and that is the subject of the complaint in respect of which the report is made.

Review by Federal Court — Privacy Commissioner

(4) If neither the person who made the complaint nor the head of the institution makes an application under this section within the period for doing so, the Privacy Commissioner, if he or she receives a report under subsection 37(2), may, within 10 business days after the expiry of the period referred to in subsection (1), apply to the Court for a review of any matter in relation to the disclosure of a record that might contain personal information and that is the subject of the complaint in respect of which the report is made.

Respondents

(5) The person who applies for a review under subsection (1), (3) or (4) may name only the head of the government institution concerned as the respondent to the proceedings. The head of the government institution who applies for a review under subsection (2) may name only the Information Commissioner as the respondent to the proceedings.

Deemed date of receipt

(6) For the purposes of this section, the head of the government institution is deemed to have received the report on the fifth business day after the date of the report.

Information Commissioner may appear

42 The Information Commissioner may

(a) appear before the Court on behalf of a complainant; or

(b) appear as a party to any review applied for under section 41 or, with leave of the

vision de l'application des exceptions prévues par la présente partie pouvant s'appliquer aux documents susceptibles de contenir les renseignements visés au paragraphe 20(1) et faisant l'objet de la plainte sur laquelle porte le compte rendu.

Révision par la Cour fédérale : Commissaire à la protection de la vie privée

(4) Si aucun recours n'est exercé en vertu des paragraphes (1) ou (2) dans le délai prévu à ces paragraphes, le Commissaire à la protection de la vie privée qui reçoit le compte rendu en application du paragraphe 37(2) peut, dans les dix jours ouvrables suivant l'expiration du délai prévu au paragraphe (1), exercer devant la Cour un recours en révision de toute question relative à la communication d'un document susceptible de contenir des renseignements personnels et faisant l'objet de la plainte sur laquelle porte le compte rendu.

Défendeur

(5) La personne qui exerce un recours au titre des paragraphes (1), (3) ou (4) ne peut désigner, à titre de défendeur, que le responsable de l'institution fédérale concernée; le responsable d'une institution fédérale qui exerce un recours au titre du paragraphe (2) ne peut désigner, à titre de défendeur, que le Commissaire à l'information.

Date réputée de réception

(6) Pour l'application du présent article, le responsable de l'institution fédérale est réputé avoir reçu le compte rendu le cinquième jour ouvrable suivant la date que porte le compte rendu.

Comparution du Commissaire à l'information

42 Le Commissaire à l'information a qualité pour comparaître :

a) devant la Cour au nom du plaignant;

b) comme partie à une instance engagée au titre de l'article 41, et, avec l'autorisation

e Court, as a party to any review applied for under section 44.

tion de la Cour, comme partie à une instance engagée au titre de l'article 44.

Burden of proof — subsection 41(1) or (2)

48 (1) In any proceedings before the Court arising from an application under subsection 41(1) or (2), the burden of establishing that the head of a government institution is authorized to refuse to disclose a record requested under this Part or a part of such a record or to make the decision or take the action that is the subject of the proceedings is on the government institution concerned.

Charge de la preuve : paragraphes 41(1) et (2)

48 (1) Dans les procédures découlant des recours prévus aux paragraphes 41(1) et (2), la charge d'établir le bien-fondé du refus de communication totale ou partielle d'un document ou des actions posées ou des décisions prises qui font l'objet du recours incombe à l'institution fédérale concernée.

Burden of proof — subsection 41(3) or (4)

(2) In any proceedings before the Court arising from an application under subsection 41(3) or (4), the burden of establishing that the head of a government institution is not authorized to disclose a record that is described in that subsection and requested under this Part or a part of such a record is on the person who made that application.

Charge de la preuve : paragraphes 41(3) et (4)

(2) Dans les procédures découlant des recours prévus aux paragraphes 41(3) et (4), la charge d'établir que la communication totale ou partielle d'un document visé à ces paragraphes n'est pas autorisée incombe à la personne qui exerce le recours.

Order of Court where no authorization to refuse disclosure found

49 Where the head of a government institution refuses to disclose a record requested under this Part or a part thereof on the basis of a provision of this Part not referred to in section 50, the Court shall, if it determines that the head of the institution is not authorized to refuse to disclose the record or part thereof, order the head of the institution to disclose the record or part thereof, subject to such conditions as the Court deems appropriate, to the person who requested access to the record, or shall make such other order as the Court deems appropriate.

Ordonnance de la Cour dans les cas où le refus n'est pas autorisé

49 La Cour, dans les cas où elle conclut au bon droit de la personne qui a exercé un recours en révision d'une décision de refus de communication totale ou partielle d'un document fondée sur des dispositions de la présente partie autres que celles mentionnées à l'article 50, ordonne, aux conditions qu'elle juge indiquées, au responsable de l'institution fédérale dont relève le document en litige d'en donner à cette personne communication totale ou partielle; la Cour rend une autre ordonnance si elle l'estime indiqué.

Privacy Act, RSC 1985, c P-21

Purpose

2 The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government

Objet

2 La présente loi a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès de

1540

institution and that provide individuals with a right of access to that information.

Definitions

3 In this Act,

[...]

personal information means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual b

s individus aux renseignements personnels qui les concernent.

Définitions

3 Les définitions qui suivent s'appliquent à la présente loi.

[...]

renseignements personnels Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable, notamment :

a) les renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille;

b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé;

c) tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre;

d) son adresse, ses empreintes digitales ou son groupe sanguin;

e) ses opinions ou ses idées personnelles, à l'exclusion de celles qui portent sur un autre individu ou sur une proposition de subvention, de récompense ou de prix à octroyer à un autre individu par une institution fédérale, ou subdivision de celle-ci visée par règlement;

f) toute correspondance de nature, implicitement ou explicitement, privée ou confidentielle envoyée par lui à une institution fédérale, ainsi que les réponses de l'institution dans la mesure où elles révèlent le contenu de la correspondance de l'expéditeur;

g) les idées ou opinions d'autrui sur lui;

h) les idées ou opinions d'un autre individu qui portent sur une proposition de subvention, de récompense ou de prix à lui octroyer.

1541

y an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of [sections 7, 8 and 26](#) and [section 19](#) of the [Access to Information Act](#), does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

(i) the fact that the individual is or was an officer or employee of the government institution,

(ii) the title, business address and telephone number of the individual,

(iii) the classification, salary range and responsibilities of the position held by the individual,

(iv) the name of the individual on a document prepared by the individual in the course of employment, and

(v) the personal opinions or views of the individual given in the course of employment,

(j.1) the fact that an individual is or was a ministerial adviser or a member of a ministerial staff, as those terms are defined in subsection 2(1) of the Conflict of Interest Act, as well as the individual's name and title,

(k) information about an individual who is or was performing services under a contract for a government institution that relates to the services performed, including the terms of the contract, the na

oyer par une institution, ou subdivision de celle-ci, visée à l'alinéa e), à l'exclusion du nom de cet autre individu si ce nom est mentionné avec les idées ou opinions;

i) son nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet;

toutefois, il demeure entendu que, pour l'application des articles 7, 8 et 26, et de l'[article 19](#) de la [Loi sur l'accès à l'information](#), les renseignements personnels ne comprennent pas les renseignements concernant :

j) un cadre ou employé, actuel ou ancien, d'une institution fédérale et portant sur son poste ou ses fonctions, notamment :

(i) le fait même qu'il est ou a été employé par l'institution,

(ii) son titre et les adresse et numéro de téléphone de son lieu de travail,

(iii) la classification, l'éventail des salaires et les attributions de son poste,

(iv) son nom lorsque celui-ci figure sur un document qu'il a établi au cours de son emploi,

(v) les idées et opinions personnelles qu'il a exprimées au cours de son emploi;

j.1) un conseiller ministériel, au sens du paragraphe 2(1) de la Loi sur les conflits d'intérêts, actuel ou ancien, ou un membre, actuel ou ancien, du personnel ministériel, au sens de ce paragraphe, en ce qui a trait au fait même qu'il soit ou ait été tel et à ses nom et titre;

k) un individu qui, au titre d'un contrat, assure ou a assuré la prestation de services à une institution fédérale et portant sur la nature de la prestation, notamment les conditions du contrat, le nom de l'individu a

1542

me of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years; (*renseignements personnels*)

[...]

Disclosure of personal information

8 (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where personal information may be disclosed

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

[...]

insi que les idées et opinions personnelles qu'il a exprimées au cours de la prestation;

l) des avantages financiers facultatifs, notamment la délivrance d'un permis ou d'une licence accordés à un individu, y compris le nom de celui-ci et la nature précise de ces avantages;

m) un individu décédé depuis plus de vingt ans. (*personal information*)

[...]

Communication des renseignements personnels

8 (1) Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article.

Cas d'autorisation

(2) Sous réserve d'autres lois fédérales, la communication des renseignements personnels qui relèvent d'une institution fédérale est autorisée dans les cas suivants :

a) communication aux fins auxquelles ils ont été recueillis ou préparés par l'institution ou pour les usages qui sont compatibles avec ces fins;

b) communication aux fins qui sont conformes avec les lois fédérales ou ceux de leurs règlements qui autorisent cette communication;

c) communication exigée par subpoena, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de renseignements;

[...]

1543

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

Right of access

12 (1) Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of [subsection 2\(1\)](#) of the [Immigration and Refugee Protection Act](#) has a right to and shall, on request, be given access to

(a) any personal information about the individual contained in a personal information bank; and

(b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution.

[...]

m) communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

(i) des raisons d'intérêt public justifient nettement une éventuelle violation de la vie privée,

(ii) l'individu concerné en tirerait un avantage certain.

Droit d'accès

12 (1) Sous réserve des autres dispositions de la présente loi, tout citoyen canadien et tout résident permanent au sens du [paragraphe 2 \(1\)](#) de la [Loi sur l'immigration et la protection des réfugiés](#) ont le droit de se faire communiquer sur demande :

a) les renseignements personnels le concernant et versés dans un fichier de renseignements personnels;

b) les autres renseignements personnels le concernant et relevant d'une institution fédérale, dans la mesure où il peut fournir sur leur localisation des indications suffisamment précises pour que l'institution fédérale puisse les retrouver sans problèmes sérieux.

[...]

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:

T-1682-18

STYLE OF CAUSE:

THE INFORMATION COMMISSIONER OF CANADA v
THE MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS

PLACE OF HEARING:

OTTAWA, ONTARIO

DATE OF HEARING:

SEPTEMBER 18, 2019

JUDGMENT AND REASONS:

MCHAFFIE J.

1544

DATED:

OCTOBER 9, 2019

APPEARANCES:

Marie-Josée Montreuil
Aditya Ramachandran

FOR THE APPLICANT

Michael Roach

FOR THE RESPONDENT

SOLICITORS OF RECORD:

Office of the Information Commiss
ioner of Canada
Gatineau, Quebec

FOR THE APPLICANT

Attorney General of Canada
Ottawa, Ontario

FOR THE RESPONDENT

Fabunmi v. Canada (Citizenship and Immigration), 2020 FC 1009 (CanLII)

Source:	Federal Court
Date:	2020-10-26
File number:	IMM-5106-19
Citation:	Fabunmi v. Canada (Citizenship and Immigration), 2020 FC 1009 (CanLII), < https://canlii.ca/t/jb8f2 >, retrieved on 2026-06-27

Date: 20201026

Docket: IMM-5106-19

Citation: 2020 FC 1009

Ottawa, Ontario, October 26, 2020

PRESENT: The Honourable Madam Justice Fuhrer

BETWEEN:

BIOLA FALILAT FABUNMI

Applicant

and

THE MINISTER OF CITIZENSHIP AND IMMIGRATION

Respondent

I. Overview

[1] The Applicant, Ms. Biola Falilat Fabunmi and her daughter fear persecution and harm on the basis of their sexual orientations; they are citizens of Nigeria who claim they are bisexual and that they had same-sex relationships in Nigeria. They also claim that in-laws, community vigilantes and police are searching for them in Nigeria. The Refugee Appeal Division [RAD], like the Refugee Protection Division [RPD] before it, found Ms. Fabunmi and her daughter were not credible because of inconsistencies in their evidence, and concluded they were neither Convention refugees nor persons in need of protection. They sought judicial review of the RAD's decision.

[2] Ms. Fabunmi's daughter was a co-applicant until this Court ordered the daughter removed, further to the Notice of Discontinuance served and filed in December 2019. Ms. Fabunmi thus is now the sole Applicant. The RAD's decision concerning the daughter no longer is in issue before this Court, contrary to the submission of the Applicant's counsel at the hearing of this matter (held by teleconference in light of COVID-19).

[3] The main issue for consideration is whether the RAD's decision was unreasonable and procedurally unfair. I disagree with the Applicant that the RAD: (i) breached procedural fairness by making new credibility findings without affording the Applicant a hearing; (ii) erred in its final decision after finding the RPD erred in several of its implausibility findings; (iii) improperly assessed the documents before it; and (iv) erred by failing to conduct a separate section 97 analysis (under the *Immigration and Refugee Protection Act*, SC 2001, c 27 [IRPA]). I therefore dismiss this judicial review application, for the reasons that follow.

II. Standard of Review

[4] The presumptive standard of review is reasonableness: *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 [*Vavilov*] at para 10. It is not a "rubber-stamping" exercise, but rather a robust form of review: *Vavilov*, above at para 13. A reasonable decision must be "based on an internally coherent and rational chain of analysis" and it must be justified in relation to the

1547

procedural and legal constraints applicable in the circumstances: *Vavilov*, at para 85. Courts should intervene only where necessary. To avoid judicial intervention, the decision also must bear the hallmarks of reasonableness – justification, transparency and intelligibility: *Vavilov*, at para 99. The Court must avoid reassessing and reweighing the evidence before the decision maker; a decision may be unreasonable, however, if the decision maker “fundamentally misapprehended or failed to account for the evidence before it”: *Vavilov*, above at paras 125-126. The party challenging the decision has the onus of demonstrating that the decision is unreasonable: *Vavilov*, at para 100.

[5] Breaches of procedural fairness in administrative contexts have been considered reviewable on a correctness standard or subject to a “reviewing exercise ... ‘best reflected in the correctness standard’ even though, strictly speaking, no standard of review is being applied”: *Canadian Pacific Railway Company v Canada (Attorney General)*, 2018 FCA 69 at para 54. The duty of procedural fairness “is ‘eminently variable’, inherently flexible and context-specific”; it must be determined with reference to all the circumstances, including the *Baker* factors: *Vavilov*, above at para 77. In sum, the focus of the reviewing court is whether the process was fair.

III. Analysis

i) *Did the RAD breach procedural fairness by making new credibility findings without affording the Applicant a hearing?*

[6] In my view, the RAD did not make new credibility findings warranting a hearing, absent evidence permitted pursuant to IRPA s 110(4). Contrary to the Applicant’s submission, this is clear in paragraph 14 of the RAD’s decision: “I will briefly touch upon the [RPD’s] findings that the Appellants have challenged on appeal and those [of the RPD’s findings] that I have independently found to be in error before I analyze the [RPD’s] strong findings.” I consider the bracketed wording that I added implicit in the RAD’s statement. It is clear from this “roadmap,” and from the RAD decision as a whole, that the RAD addressed the matters in issue before the RPD. It did not raise a new issue but “rather it was addressing the very issue raised by the applicant”: *Ibrahim v Canada (Citizenship and Immigration)*, 2016 FC 380 [*Ibrahim*] at para 30.

1548

When the credibility of a refugee applicant is at the heart of the RPD's decision and the grounds of appeal before the RAD, "the RAD is entitled to make independent findings in this regard, without having to question the applicant or giving the applicant another opportunity to make submissions": *Corvil v Canada (Minister of Citizenship and Immigration)*, 2019 FC 300 at para 13.

[8] As part of its correctness review, the RAD was obligated to review and assess the evidence anew which in my view it did: *Zhao v Canada (Citizenship and Immigration)*, 2019 FC 1593 at para 33. Unless it is clearly explained why the RPD enjoys a meaningful advantage in assessing an applicant's credibility, the RAD must conduct its own credibility assessment, which I also find it did in this case: *Manan v Canada (Citizenship and Immigration)*, 2020 FC 150 at para 38. Further, "[t]he fact that it saw some of the evidence differently [or, in my view, confirmed a negative credibility finding with a more logical or rational chain of analysis] is not a basis to challenge the decision on fairness grounds when no new issue was raised": *Ibrahim*, above at para 30; *Iqbal v Canada (Citizenship and Immigration)*, 2020 FC 170 at para 55. In the case before me, the Applicant has challenged the RAD's findings without explaining why the RPD has a meaningful advantage over the RAD in assessing credibility in the circumstances.

[9] In any event, the "new credibility findings" alleged by the Applicant pertain to the Applicant's daughter who no longer is a party to this proceeding. Accordingly, I need not address the issue further.

ii) *Did the RAD err in its final decision after finding the RPD erred in several of its implausibility findings?*

[10] I am not persuaded that the RAD erred as argued on this point. The Applicant submits that the RAD arrived at its decision, basing it on inconsistencies and implausibilities found by the RPD. Further, the RAD should have sent the matter back to the RPD for redetermination, "knowing full well it was not preview to the oral testimony of the Applicants, rather than assume based on these faulty implausibility findings." In my view, however, when the RAD finds an error with the RPD's decision, it can confirm the decision on another basis: *Canada (Citizenship and Immigration) v*

1549*Huruglica*, 2016 FCA 93 [*Huruglica*] at para 78. As discussed below, I find that the RAD's

correctness determinations are “based on an internally coherent and rational chain of analysis” such that they are intelligible, transparent and justified.

[11] Though IRPA s 111(1) contemplates redetermination, among the three options for decision making available to the RAD, IRPA s 111(2) limits the RAD's ability to do so. The latter provision prescribes a two-part conjunctive test for a redetermination finding. The RAD must be of the opinion that: first, the RPD erred in law, fact or mixed fact and law; **and** second, the RAD cannot confirm the RPD's decision, set it aside or substitute its own decision without hearing the evidence presented to the RPD.

[12] As Justice Gauthier explained, IRPA s 111(2) is based on the principle that there are cases where the RPD enjoys a meaningful advantage over the RAD in making findings arising out of the oral evidence: *Huruglica*, above at para 70. On the other hand, Justice Gauthier also made it clear that in each case, there is a two-step test to meet: “...the RAD ought to determine whether the RPD truly benefited from an advantageous position, and if so, whether the RAD can nevertheless make a final decision in respect of the refugee claim”: *Huruglica*, above at para 70. Justice Gauthier clarified that the RPD may have no real advantage over the RAD if the RAD can identify an error based on common sense, such as in cases where a claimant was not found credible because their story was not plausible: *Huruglica*, above at para 72.

[13] The first part of the IRPA s 111(2) test was met in the case before me when the RAD found that the RPD erred in making the following implausibility findings regarding the Applicant, and explained why:

- 1) the Applicant feeling happy and positive about realizing she was bisexual - the RAD stated that the process of self-discovery is a very personal one;
- 2) the varied spelling of the name of the Applicant's alleged same-sex partner was implausible and not supported by documentary evidence - the RAD was not sure to what kind of documentary evidence the RPD was referring because the RAD found that the three forms of the partner's name are in common use in Nigerian cultures; and

1550

3) the Applicant's minor injuries, whereas her husband died, because of an alleged attack by a group of boys while she was driving with her husband resulting in the car rolling over and crashing; the gang then lit the car on fire, shouting gays and lesbians were not wanted - the RAD found the RPD has no expertise in car crash reconstruction and therefore no reliable way of assessing the plausibility of this evidence.

[14] In my view, however, the second part of the [IRPA s 111\(2\)](#) test was not met. The RAD concluded, after reviewing the entirety of the transcript for all three hearing dates, the evidence and the RPD record, that the RPD had no meaningful advantage. The RAD thus proceeded with its IRPA s 111(1) mandate. In this case, the RAD confirmed the RPD correctly assessed the following inconsistencies that were material (with one possible exception) to the Applicant's claim and hence, the RPD was correct that the Applicant's testimony and documentary evidence lacked credibility; again, the RAD explained why:

1) *Canadian Visa Applications*: The Applicant (and her daughter) applied for Canadian visas. The information in the visa applications regarding siblings and the Applicant's children is inconsistent with the information in the refugee claims. The RAD found the two documents appear to refer to completely different people, meaning that at least one of the documents contained fraudulent or omitted information. The RAD also noted that, when questioned at the RPD hearing, the Applicant replied her brother and a travel agent helped them prepare the visa applications. She could not explain why the information was incorrect. The RAD found that the visa applications were "part of the constellation of evidence central to establishing [their] identities and relationships with family members, which [they] testified are highly relevant to their claims." Even if this were a peripheral issue, the RAD concluded it still would be a minor part of the overall conclusion that the Applicant's evidence was highly inconsistent and therefore unreliable.

2) *Applicant's Relationship with Alleged Same-sex Partner* (whose name has varied spelling): The Applicant alleged, in her Basis of Claim or BOC narrative and her testimony, that they met in January 2012 while Ms. Fabunmi was working as a hairdresser at Midas Touch Salon; documentary evidence, however, pointed to Ms. Fabunmi working or training at Midas Touch Salon in 2003-2004, a difference of 8 or 9 years. When asked about the inconsistency, she replied that she forgot the correct date. The RAD found this a serious material inconsistency central to the Applicant's claim. Ms.

Fabunmi testified that the relationship lasted approximately 4 years and ended shortly before the alleged attack against Ms. Fabunmi and her husband that occurred in early 2016.

3) *UK Visa Applications*: In her BOC, Ms. Fabunmi also alleged that she applied for two UK visas in 2012 and 2015 in order to meet up with her same-sex partner but the applications were denied. UK biometric evidence, however, pointed to the applications having been made in 2010 and 2013 instead. The RAD found the latter evidence reliable and the discrepancy problematic: if the 4-year relationship commenced in 2003-2004, it would have been long over by 2010; if, however, the relationship commenced in 2012, the first UK visa application would have been made two years before Ms. Fabunmi even met her alleged same-sex partner. When the RPD confronted Ms. Fabunmi with these inconsistencies, she responded she forgets issues and did not remember. The RAD found the explanation unacceptable because these two issues go to the nature of the relationship that led to the Applicant's alleged persecution in Nigeria. The RAD therefore concluded that on a balance of probabilities, there was no romantic relationship as described by the Applicant.

4) *Attack on Ms. Fabunmi and Her Husband*: In her BOC narrative, Ms. Fabunmi describes that after she and her same-sex partner last saw each other in December 2015, the partner reconnected with an ex-girlfriend whose husband caught them having sex. The husband arranged for the gang of boys to attack Ms. Fabunmi and her husband; the partner was in hiding from the same man at the time of the attack. Documentary evidence comprised of a letter from the Riverdale Immigrant Women's Centre, however, describes that the attack was arranged by the same-sex partner who was jealous of the time the Applicant was spending with her family, based on information provided by Ms. Fabunmi. The Applicant was unable to explain why the inconsistency existed, and related testimony was vague and confusing.

The RAD found the inconsistency material because it goes to the core of the alleged danger faced in Nigeria. The RAD also noted that the RPD received no corroborating evidence of the death of Ms. Fabunmi's husband, nor their hospital stays, and no explanation why the evidence was not available. I note Ms. Fabunmi had time and opportunity to obtain the documentation - the RPD hearing spanned three days, commencing in November 2017, one year after she arrived in Canada, and ending in August 2018: *Canadian Association of Refugee Lawyers v Canada (Citizenship and Immigration)*, 2019 FC 1126 at para 184; *Fatoye v Canada (Citizenship and Immigration)*, 2020 FC 456 at para 35.

5) *Hiding from Police and Community*: Ms. Fabunmi's testimony and BOC narrative differed concerning when the police came looking for her. For

example, she testified that: it was made public; she found out from her maid; she found out from her former same-sex partner. In her BOC narrative, however, she described that her brother told her when they were heading to the airport to leave Nigeria. Further, the accounts of both Ms. Fabunmi and her daughter of when, where and why they went into hiding were inconsistent.

[15] The RAD therefore confirmed the decision that the Applicant is not a Convention Refugee nor a person in need of protection. (These confirmations also applied to the Applicant's daughter who no longer is a party to this judicial review application.) Apart from the RPD's errors that the RAD identified, the numerous inconsistencies in the evidence were obvious and sufficiently central to permit the RAD to confirm the correctness of the RPD's other findings.

iii) *Did the RAD improperly assess the documents before it?*

[16] This issue relates more specifically to the Canadian visa applications and the documentary evidence concerning the Applicant's employment or training at Midas Touch Salon from 2003-2004. I am not persuaded that the RAD improperly assessed either set of evidence.

[17] As I noted in point 1) under paragraph 14, the RAD found that in light of the inconsistent information regarding siblings and the Applicant's children as between the Canadian visa applications and the refugee claims, **at least one of the documents contained fraudulent or omitted information**. I find this conclusion is somewhat speculative and, on the whole, unnecessary. That said, it does not detract, in my view, from the reasonableness of the RAD's consideration of this evidence, the uncontradicted finding of inconsistency, and the lack of explanation why the information was incorrect.

[18] The Applicant argues, however, that the use of fraudulent documents to escape persecution is peripheral to any claim, citing *Rasheed v Canada (Citizenship and Immigration)*, 2004 FC 587 [Rasheed] and *Fajardo v Canada (Minister of Employment and Immigration)*, 1993 CanLII 17640 (FCA), [1993] FCJ No 915. While I do not disagree with this general principle, in my view it does not apply to the circumstances of the case before me. First, the inconsistent information pertains to

1553

family members as opposed to the Applicant's own identity. This matter does not involve an applicant who lied about their own identity or entered Canada using fraudulent **foreign** documents, as occurred in *Rasheed*. Second, the Applicant did not make the argument before the RAD, and thus, it is not proper to advance it in this judicial review. I agree with the Respondent that it is tantamount to a request to reconsider and reweigh this evidence.

[19] Regarding the Applicant's employment or training at Midas Touch Salon from 2003-2004, I find the RAD's articulation of its concerns (in points 2) and 3) under paragraph 14 above) intelligible, transparent and justified. Contrary the Applicant's argument before this Court, inconsistencies between different types of evidence, including testimony, permit the decision maker to draw adverse credibility findings: *Lawani v Canada (Citizenship and Immigration)*, 2018 FC 924 at para 21, citing *Lin v Canada (Citizenship and Immigration)*, 2010 FC 183 at para 19.

[20] The Applicant argued that "oral testimony is generally allowed to provide additional details of a claimant's narrative and it should not be a basis for impugning credibility," citing *Selvakumaran v Canada (Citizenship and Immigration)*, 2002 FCT 623 [*Selvakumaran*] at para 20 (incorrectly identified as paragraph 21 in its written submissions). The court qualified this principle, however, as follows: "the case law has allowed that oral testimony may provide details not included in the PIF [Personal Information Form], and that this will not serve to impugn the applicant's credibility **unless the incident omitted is a significant one to the claim**" [emphasis added]: *Selvakumaran*, at para 20. Contrary to the circumstances of the case before me, the court in *Selvakumaran* concluded in the same paragraph that "[n]ot only is the evidence in the applicant's PIF consistent with his oral testimony, but the missing details are not significant." Contrary to the Applicant's argument, I am not persuaded that the case before me involves a failure by the RAD to take into account material evidence or to overlook a piece of relevant evidence. I therefore am not prepared to find unreasonable the RAD's reconsideration of the applicable evidence and testimony, and its conclusions, concerning the applicant's relationship with the alleged same-sex partner and the UK visa applications.

iv) *Did the RAD err by failing to conduct a separate section 97 analysis?*

1554

am not persuaded that the RAD erred in this respect. The gist of the Applicant's argument appears to be that because the analysis under [sections 96 and 97](#) of the [IRPA](#) differ, separate treatment is warranted; the RPD's and RAD's failure to do so in this case resulted in procedural unfairness. The Respondent, on the other hand, argues that there is no obligation for the RAD to conduct a further section 97 analysis because the Applicant's arguments were the same under section 96: *Kaur v Canada (Citizenship and Immigration)*, [2012 FC 1379](#) at para [51](#). The RPD, having considered the Applicant's claim that she was at risk as a result of her bisexuality in Nigeria and found that it lacked credibility, was not required to conduct an additional section 97 analysis. I agree.

[22] Drawing from *Canada (Citizenship and Immigration) v Sellan*, [2008 FCA 381](#) at paras [2-3](#), the Court previously has held that "the RAD and the RPD are not obligated to undertake a section 97 analysis when faced with a case where the claimant lacks credibility": *Chinwuba v Canada (Citizenship and Immigration)*, [2019 FC 312](#) at para [31](#); *Huseynov v Canada (Citizenship and Immigration)*, [2019 FC 1392](#) at paras [7 and 19](#); *Ikeme v Canada (Immigration, Refugees and Citizenship)*, [2018 FC 21](#) at paras [40-42](#); and *Alkurd v Canada (Citizenship and Immigration)*, [2019 FC 298](#) at para [27](#). I see no reason to depart from this line of cases in the present circumstances.

IV. Conclusion

[23] I therefore find that the Applicant has failed to discharge her onus of demonstrating that the RAD's decision is unreasonable. I also find that the RAD's decision was procedurally fair. Neither party proposed a serious question of general importance for certification and thus, I further find that none arises.

JUDGMENT in IMM-5106-19

THIS COURT'S JUDGMENT is that this judicial review application is dismissed, and there is no serious question of general importance for certification.

"Janet M. Fuhrer"

FEDERAL COURT**SOLICITORS OF RECORD**

DOCKET: IMM-5106-19

STYLE OF CAUSE: BIOLA FALILAT FABUNMI v THE MINISTER OF CITIZENSHIP AND IMMIGRATION

PLACE OF HEARING: TORONTO, ONTARIO (VIA TELECONFERENCE)

DATE OF HEARING: JUNE 4, 2020

REASONS FOR JUDGMENT AND JUDGMENT: FUHRER J.

DATED: OCTOBER 26, 2020

APPEARANCES:

Jerome Olorunpomi FOR THE APPLICANT

Idorenyin Udoh-Orok FOR THE RESPONDENT

SOLICITORS OF RECORD:

Jerome Olorunpomi FOR THE APPLICANT
Legal Aid Ontario
Toronto, Ontario

Attorney General of Canada FOR THE RESPONDENT
Ottawa, Ontario

1556

[Home](#) > [FCA Decisions Menu](#) > [Decisions](#) > [Federal Court of Appeal Decisions](#) >

Canadian Broadcasting Corporation v. Canada (Parole Board)

1557

Federal Court of Appeal Decisions

Canadian Broadcasting Corporation v. Canada (Parole Board)

Court (s) Database: Federal Court of Appeal Decisions

Date: 2023-07-27

Neutral citation: 2023 FCA 166

File numbers: A-251-21

Notes: [Reported Decision](#)

Date: 20230727

Docket: A-251-21

Citation: 2023 FCA 166

CORAM: PELLETIER J.A.
WEBB J.A.
RIVOALEN J.A.

BETWEEN:

CANADIAN BROADCASTING CORPORATION

Appellant

and

PAROLE BOARD OF CANADA

Respondent

Heard at Toronto, Ontario, on January 23 and 24, 2023.

Judgment delivered at Ottawa, Ontario, on July 27, 2023.

1558

REASONS FOR JUDGMENT BY:

PELLETIER J.A.

CONCURRED IN BY:

WEBB J.A.
RIVOALEN J.A.

Date: 20230727

Docket: A-251-21

Citation: 2023 FCA 166

CORAM: PELLETIER J.A.
WEBB J.A.
RIVOALEN J.A.

BETWEEN:

CANADIAN BROADCASTING CORPORATION

Appellant

and

PAROLE BOARD OF CANADA

Respondent

REASONS FOR JUDGMENT

PELLETIER J.A.

I. Introduction

[1] This is an appeal from a decision of the Federal Court dismissing an application for judicial review of a decision of the Parole Board of Canada (the Board) refusing to provide the Canadian Broadcasting Corporation (the CBC) with “a complete copy of the audio recordings of parole hearings of Paul Bernardo, held on October 17, 2018; Ethan Simon Templar MacLeod, formerly known as William Shrubsall, held on or about November 7, 2018; and Craig Munro, held on February 26, 2009, March 16, 2010, March 30,

and July 29, 2015”: Appeal Book (AB) at p. 351. I will refer to the individuals involved as the “Offenders”.

[2] The Board declined to provide the requested audio recordings on the grounds that the open court principle invoked by the CBC did not apply since the Parole Board is not a quasi-judicial body and that the public interest in the hearings did not outweigh the privacy interests of the Offenders.

[3] The CBC’s application was heard together with the applications of the families of the victims of Mr. Bernardo and Mr. Munro, and others, seeking disclosure, under the *Access to Information Act*, R.S.C. 1985, c. A-1 (the AIA), to a mass of documents, including the documents put before the Board at the parole hearings of the Offenders as well as copies of audio recordings of certain Board hearings in relation to the Offenders. These reasons deal only with the CBC’s application. The families’ applications for records held by Corrections Canada and the Board will be dealt with in separate reasons.

[4] For the reasons that follow, I would allow the CBC’s appeal; however, I would not grant the CBC all of the remedies it seeks.

II. Facts and Procedural History

[5] Each of the Offenders is notorious. Mr. Bernardo is a violent sexual offender who was convicted of the horrific murder of two young women, Leslie Mahaffy and Kristen French. Mr. Munro was convicted of the murder of Michael Sweet, a Toronto police constable, who bled to death while being held hostage by Mr. Munro in the course of a botched robbery. Mr. MacLeod was convicted of crimes of violence and sexual offences in 1998 and was subsequently paroled on the basis that he would be deported to the United States to serve the balance of his lengthy sentence. It turned out that he will be eligible for release in the United States far sooner than he would have been in Canada.

[6] The CBC is able to attend parole hearings and to report on them without being restrained by the Board as to what it can report. To state the obvious, this case is not about the CBC’s access to Board hearings. The CBC’s request is that it be given the same rights to the recordings as it enjoys with respect to exhibits filed in open court. Thus, while the CBC’s memorandum of fact and law refers to access to or disclosure of the

recordings, its request to the Board was that it be given a physical copy of the recordings.

A. The Board's Decision

[7] The Board's decision is found in a letter from its Executive Director General dated October 21, 2019 to the CBC's legal counsel. This letter, found at pages 351 to 355 of the Appeal Book, was in response to an email from the CBC's legal counsel dated June 4, 2019, found at pages 5574 to 5575 of the Appeal Book. In that email, the CBC argued that the open court principle applied to the Board as an administrative tribunal exercising judicial or quasi-judicial functions. In the CBC's view, the Board was required to produce the audio recordings of past hearings, which it characterized as adjudicative records, by virtue of the open court principle and consistent with the fact that Board hearings are presumptively open to the public.

[8] The CBC went on to argue that the Board was bound to act consistently with the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [Charter] in exercising its statutory functions. To the extent that the Board sought to limit the provision of copies of audio recordings, it could only do so in a manner consistent with section 2(b) of the Charter and the test articulated by the Supreme Court in *Dagenais v. Canadian Broadcasting Corp.*, [1994] 3 S.C.R. 835, 120 D.L.R. (4th) 12 and in *R. v. Mentuck*, 2001 SCC 76, [2001] 3 S.C.R. 442 (the *Dagenais/Mentuck* test).

[9] The CBC also argued that subsection 140(13) of the *Corrections and Conditional Release Act*, S.C. 1992, c. 20 (the Act), which allows victims and members of their families to listen to audio tapes of hearings, did not preclude providing copies of audio recordings to the press and to members of the public who were entitled to such access, subject only to the *Dagenais/Mentuck* test. Further, if subsection 140(13) was interpreted in such a way as to preclude providing copies of audio recordings to the press, this would be a violation of section 2(b) of the Charter, which guarantees both freedom of expression and freedom of the press, and would not be saved by section 1 of the Charter.

[10] Finally, the CBC argued that the *Privacy Act*, R.S.C. 1985, c. P-21 did not prohibit providing copies of the audio recordings since the information in the recordings was available to the public as a result of the open court principle and as a result of having been disclosed in a hearing which was presumptively open to

[11] The Board rejected the CBC's request for copies of the audio recordings.

[12] The Board began its analysis by addressing the open court principle which, in its view, applied only to bodies that act in a quasi-judicial capacity. The Board pointed out that it did not function like a court: hearings were not adversarial, counsel, if present, had a very limited role, and it did not determine rights but rather assessed risk based on statutory criteria. The Board added that while observers could apply to attend, its hearings were not open to the public.

[13] The Board relied on the Supreme Court's decision in *Mooring v. Canada (National Parole Board)*, [1996] 1 S.C.R. 75, 132 D.L.R. (4th) 56 [*Mooring*], which held that the Board did not act in a judicial or quasi-judicial capacity. Instead, the Supreme Court described the Board's proceedings as inquisitorial. While recognizing that the open court principle favours accountability, the Board listed the accountability measures to which it is subject and, in the end, concluded that "scrutiny can be achieved by other means than [the open court principle]": AB at p. 352.

[14] After noting that individuals could apply to attend Board hearings and receive copies of its decisions, the Board concluded that "allowing access to the audio recordings of the offender's parole hearings is not necessary to ensure accountability and transparency in the decision making process of the Board": AB at p. 353.

[15] The Board then addressed the issue of the *Privacy Act*. It reasoned that, in light of its conclusion that it was not subject to the open court principle, the CBC's request was, in effect, an invocation of section 2(b) of the Charter to access information in the hands of a government entity. The Board noted that the Supreme Court had recently decided that the Charter does not guarantee access to all government documents. Access is provided only when it is shown to be necessary to permit meaningful discussion on a matter of public importance. The Board noted that the CBC did not provide any evidence to demonstrate that access to the recordings was necessary to ensure meaningful public discussion, which militated against its position, especially when one considered that the media had received copies of the decisions, attended some of the

hearings and were able to report on them afterwards.

[16] The Board addressed the CBC's argument about subsection 140(13) of the Act which, in the Board's view, is not only specific to victims but, even then, access to specific information can be limited when certain safety or privacy considerations apply.

[17] Finally, the Board addressed the weighing of interests mandated by subparagraph 8(2)(m)(i) of the *Privacy Act*, which permits the release of personal information where the head of the institution is satisfied that the public interest in disclosure outweighs the invasion of privacy. The Board pointed out that, by virtue of subsection 140(14) of the Act, the exception to sections 7 and 8 of the *Privacy Act* – found at subsection 69(2) of the *Privacy Act* – does not apply to Board hearings. This is so because information disclosed in a Board hearing at which observers are present is deemed not to be publicly available for that reason alone.

[18] The Board indicated that its decisions must be “consistent with the protection of society and are limited to only what is necessary and proportionate to the purpose of conditional release, which is to facilitate the rehabilitation of offenders and their reintegration into the community as law-abiding citizens”: AB at p. 354. The Board's decisions are made on the basis of ongoing observation and assessment of the offender and focus on the risk involved in the offender's re-entry into the community. According to the Board:

An appropriate balance must be maintained between the offender's right to privacy, which in turn contributes to the quality of information used for decision-making, and the public's right to know. The [*Corrections and Conditional Release Act*] achieves this balance by providing for the attendance of observers at hearings, and for access to the Board's reasons for decision, both in accordance with established criteria.

AB at p. 354

[19] In the end, the Board determined that the public interest in disclosure had not been sufficiently demonstrated and that, in any event, it would not outweigh the offender's privacy interests. The Board believed that it was not possible to overlook the adverse consequences of disclosure to an offender, including the risk of the derailment of their reintegration potential, even if the public interest had been demonstrated in this case.

B. The Federal Court Decision

[21] Since these reasons deal only with the CBC's request for the provision of copies of audio recordings, I will limit my review of the Federal Court's reasons to the issues that are relevant to that request.

[22] The Federal Court found that the Board was not a quasi-judicial tribunal. The proceedings before it were not adversarial but rather were inquisitorial in nature. As a result, the Court found that the Board was not bound to produce copies of audio recordings under the open court principle. In addition, the Court found that the principle enunciated in *Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23, [2010] 1 S.C.R. 815 [*Criminal Lawyers' Association*] was not applicable. That principle allows the press and the public access to documents in the government's hands "only where it is shown to be a necessary precondition of meaningful expression, does not encroach on protected privileges, and is compatible with the function of the institution concerned": *Criminal Lawyers' Association* at para. 5. The Federal Court found that disclosure was not a precondition to meaningful expression given that the public and the press could attend Board hearings.

[23] The CBC argued before the Federal Court that the Board erred in failing to adopt a contextual analysis of privacy, instead relying on "a blanket assertion" that disclosing the recordings would constitute an invasion of privacy. The Federal Court disagreed and found that the Board had considered the privacy interests of the Offenders. It noted that the Board considered that the Offenders expected that their personal information would be protected from public disclosure.

[24] The Federal Court found that the Board's decision did not engage the framework established in the cases of *Doré v. Barreau du Québec*, 2012 SCC 12, [2012] 1 S.C.R. 395 [*Doré*] and *Loyola High School v. Quebec (Attorney General)*, 2015 SCC 12, [2015] 1 S.C.R. 613 [*Loyola*], collectively the *Doré/Loyola* framework. In particular, the Court found that the CBC's Charter rights had not been limited. The Court also found that the Board's decision was reasonable.

[25] In the result, the Federal Court dismissed the CBC's application for judicial review.

[26] The CBC based its demand for copies of the audio recordings of parole hearings on the open court principle, which is nourished by the Charter's section 2(b) protection of "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication". The CBC based its position that the open court principle is fortified by section 2(b) on *Canadian Broadcasting Corp. v. Ferrier*, 2019 ONCA 1025, 441 D.L.R. (4th) 632 [*Ferrier*]: see paragraphs 43, 62. In the end, the CBC relied upon both the open court principle and section 2(b) to support its demand for copies of the audio recordings. The CBC also relied on the limits on a court's ability to withhold information from the public, as set out in the *Dagenais/Mentuck* framework.

[27] In the event that its primary argument was unsuccessful, the CBC invoked the balancing provision found at subparagraph 8(2)(m)(i) of the *Privacy Act* which provides as follows:

8 (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

...

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

8 (2) Sous réserve d'autres lois fédérales, la communication des renseignements personnels qui relèvent d'une institution fédérale est autorisée dans les cas suivants :

...

m) communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

(i) des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée,

(ii) l'individu concerné en tirerait un avantage certain.

[28] In the result, the following issues arise in this appeal:

A. What is the standard of review?

B. Is the Board subject to the open court principle?

C. Is the CBC otherwise entitled to audio recordings of Board hearings?

A. Standard of Review

[29] The Supreme Court's jurisprudence teaches that an appellate court sitting on appeal from a trial court sitting in judicial review must first decide if the latter properly identified the standard of review and then assess whether the standard of review was properly applied: *Agraira v. Canada (Public Safety and Emergency Preparedness)*, 2013 SCC 36, [2013] 2 S.C.R. 559 at para. 45 [*Agraira*]. In practice, this means that the appellate court steps into the shoes of the court of revision and focuses on the administrative decision: *Agraira* at para. 46, *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3, [2012] 1 S.C.R. 23 at para. 247.

[30] The standard of review for questions of law, fact, or mixed fact and law is to be decided in the light of *Canada (Minister of Citizenship and Immigration) v. Vavilov*, 2019 SCC 65, [2019] 4 S.C.R. 653 [*Vavilov*] according to which the presumptive standard of review of an administrative decision is reasonableness: *Vavilov* at para. 10. The presumption may be rebutted in certain circumstances, one of which is when the rule of law requires that the correctness standard be applied, such as when dealing with constitutional questions: *Vavilov* at para. 17.

[31] The correctness standard in relation to constitutional questions is limited to "[q]uestions regarding the division of powers between Parliament and the provinces, the relationship between the legislature and the other branches of the state, the scope of Aboriginal and treaty rights under s. 35 of the *Constitution Act, 1982*, and other constitutional matters [that] require a final and determinate answer from the courts": *Vavilov* at para. 55. In other words, not every question involving the Constitution, including the Charter, is to be reviewed on the correctness standard. Charter questions that arise in the course of administrative decisions stand on a different footing:

When *Charter* values are applied to an individual administrative decision, they are being applied in relation to a particular set of facts. *Dunsmuir* tells us this should attract deference (para. 53; see also *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1, [2002] 1 S.C.R. 3, at para. 39).

Doré at para. 36

[32] The first issue before the Board was whether the open court principle, fortified by section 2(b) of the

1566

er, applied to it. This brings the case within the principle set out in *Ferrier*, reproduced below:

The issue before the decision maker was *whether* the *Dagenais/Mentuck* test had a bearing on the discretionary decision he had to make. That is not the same as the issue presented in *Doré* and *Episcopal* of *how* the s. 2(b) *Charter* right impacted or affected the discretionary decision he had to make. The decision maker did not reach the point of factoring the *Dagenais/Mentuck* test into his discretionary decision because he decided that it did not apply. A reasonableness standard assumes a range of possible outcomes all of which are defensible in law: see *Vavilov*, at para. 83. That standard is inappropriate here. The *Dagenais/Mentuck* test either applied or it did not.

Ferrier at para. 37 (emphasis in original)

[33] In the present case, the Board resolved the question of the CBC's access to copies of the audio recordings by deciding that the open court principle did not apply to the Board. As in *Ferrier*, either the open court principle applied or it did not. As a result, the correctness standard applies to that question.

[34] The second question in this appeal, that is, whether the CBC was otherwise entitled to production of the audio recordings, is to be reviewed on the reasonableness standard.

B. Is the Board subject to the open court principle?

[35] As indicated earlier in these reasons, the CBC framed its argument about access to copies of the audio recordings of Board hearings in terms of the open court principle:

The open court principle, including the presumption of open access to adjudicative records, applies to administrative tribunals as well as to courts. This presumption extends to providing access to audio recordings of past hearings to members of the public and the media, similar to those available in the courts. This is also in line with the fact that Parole Board hearings are presumptively open to the public.

AB at p. 5574

[36] As can be seen from this passage, the CBC alleges that the open court principle applies to Board hearings, which is confirmed by the fact that Board hearings are presumptively open to the public. The CBC then posits that the open court principle, as applied to tribunals, includes the right of access to adjudicative records, which includes audio recordings: CBC's memorandum of fact and law at para. 26.

[37] An examination of subsection 140(4) of the Act shows that Board hearings are presumptively open to

1567

public, subject to appropriate restrictions arising from the subject matter of the hearing and the locations at which Board hearings are held. Subsection 140(4) of the Act provides as follows (underline added):

140 (4) Subject to subsections (5) and (5.1), the Board or a person designated, by name or by position, by the Chairperson of the Board shall, subject to such conditions as the Board or person considers appropriate and after taking into account the offender's views, permit a person who applies in writing therefor to attend as an observer at a hearing relating to an offender, unless the Board or person is satisfied that

(a) the hearing is likely to be disrupted or the ability of the Board to consider the matter before it is likely to be adversely affected by the presence of that person or of that person in conjunction with other persons who have applied to attend the hearing;

(b) the person's presence is likely to adversely affect those who have provided information to the Board, including victims, members of a victim's family or members of the offender's family;

(c) the person's presence is likely to adversely affect an appropriate balance between that person's or the public's interest in knowing and the public's interest in the effective reintegration of the offender into society; or

(d) the security and good order of the institution in which the hearing is to be held is likely to be adversely affected by the person's presence. (my emphasis)

140 (4) Sous réserve des paragraphes (5) et (5.1), la Commission, ou la personne que le président désigne nommément ou par indication de son poste, doit, aux conditions qu'elle estime indiquées et après avoir pris en compte les observations du délinquant, autoriser la personne qui en fait la demande écrite à être présente, à titre d'observateur, lors d'une audience, sauf si elle est convaincue que, selon le cas :

a) la présence de cette personne, seule ou en compagnie d'autres personnes qui ont demandé d'assister à la même audience, nuira au déroulement de l'audience ou l'empêchera de bien évaluer la question dont elle est saisie;

b) sa présence incommodera ceux qui ont fourni des renseignements à la Commission, notamment la victime, la famille de la victime ou celle du délinquant;

c) sa présence compromettra vraisemblablement l'équilibre souhaitable entre l'intérêt de l'observateur ou du public à la communication de l'information et l'intérêt du public à la réinsertion sociale du délinquant;

d) sa présence nuira à la sécurité ou au maintien de l'ordre de l'établissement où l'audience doit se tenir.

[38] The wording of the subsection is clear that a person who applies in writing to attend a hearing as an observer shall be permitted to attend unless the Board or its designate is satisfied the admission of that person will give rise to one or more of the circumstances set out in paragraphs (a) to (d). While the courts do not have a pre-screening process like the Board has, limits can be placed on attendance at a court hearing. For example, in Ontario, subsections 135(1) and (2) of the *Courts of Justice Act*, R.S.O. 1990, c. C.43 provide:

135 (1) Subject to subsection (2) and

135 (1) Sous réserve du paragraphe (2) et

1568

rules of court, all court hearings shall be open to the public.

des règles de pratique, les audiences des tribunaux sont publiques.

(2) The court may order the public to be excluded from a hearing where the possibility of serious harm or injustice to any person justifies a departure from the general principle that court hearings should be open to the public.

(2) Le tribunal peut ordonner le huis clos si la possibilité qu'une personne subisse un préjudice important ou une injustice grave justifie une dérogation au principe général de la publicité des audiences des tribunaux.

[39] There is a similar provision in the *Criminal Code*, R.S.C. 1985, c. C-46 at subsections 486(1) and (2):

486 (1) Any proceedings against an accused shall be held in open court, but the presiding judge or justice may, on application of the prosecutor or a witness or on his or her own motion, order the exclusion of all or any members of the public from the court room for all or part of the proceedings, or order that the witness testify behind a screen or other device that would allow the witness not to be seen by members of the public, if the judge or justice is of the opinion that such an order is in the interest of public morals, the maintenance of order or the proper administration of justice or is necessary to prevent injury to international relations or national defence or national security.

486 (1) Les procédures dirigées contre l'accusé ont lieu en audience publique, mais si le juge ou le juge de paix qui préside est d'avis qu'il est dans l'intérêt de la moralité publique, du maintien de l'ordre ou de la bonne administration de la justice ou que cela est nécessaire pour éviter toute atteinte aux relations internationales ou à la défense ou à la sécurité nationales, il peut, sur demande du poursuivant ou d'un témoin ou de sa propre initiative, ordonner que soit exclu de la salle d'audience l'ensemble ou tout membre du public, pour tout ou partie de l'audience, ou que le témoin témoigne derrière un écran ou un dispositif lui permettant de ne pas être vu du public.

...

...

(2) In determining whether the order is in the interest of the proper administration of justice, the judge or justice shall consider

(2) Pour décider si l'ordonnance est dans l'intérêt de la bonne administration de la justice, le juge ou le juge de paix prend en considération les facteurs suivants :

(a) society's interest in encouraging the reporting of offences and the participation of victims and witnesses in the criminal justice process;

a) l'intérêt de la société à encourager la dénonciation des infractions et la participation des victimes et des témoins au processus de justice pénale;

(b) the safeguarding of the interests of witnesses under the age of 18 years in all proceedings;

b) la sauvegarde de l'intérêt des témoins âgés de moins de dix-huit ans dans toute procédure;

(c) the ability of the witness to give a full and candid account of the acts complained of if the order were not made;

c) la capacité d'un témoin, si l'ordonnance n'est pas rendue, de fournir un récit complet et franc des faits sur lesquels est fondée l'accusation;

(d) whether the witness needs the order for their security or to protect them from

d) la nécessité de l'ordonnance pour assurer la sécurité d'un témoin ou le

for their security or to protect them from
intimidation or retaliation;

assurer la sécurité d'un témoin ou le
protéger contre l'intimidation et les
représailles;

(e) the protection of justice system
participants who are involved in the
proceedings;

e) la protection des personnes associées
au système judiciaire qui prennent part à
la procédure;

(f) whether effective alternatives to the
making of the proposed order are
available in the circumstances;

f) l'existence dans les circonstances
d'autres moyens efficaces que celui de
rendre l'ordonnance;

(g) the salutary and deleterious effects of
the proposed order; and

g) les effets bénéfiques et préjudiciables
de l'ordonnance demandée;

(h) any other factor that the judge or
justice considers relevant.

h) tout autre facteur qu'il estime
pertinent.

[40] The point of drawing attention to these statutory provisions is simply to show that, even before the courts where it is applied most rigorously, the open court principle is not absolute. As a result, the conditions set out at paragraphs 140(4)(a) to (d) of the Act do not, in and of themselves, mean that Board hearings are not presumptively open to the public.

[41] But the fact that Board hearings are open to the public, while relevant, does not resolve the issue of the application of the open court principle. The following paragraph sets out the core of the Board's reasoning on the open court principle:

It is also important to note that the function of the Board is significantly different from a court in a number of ways. A parole hearing is inquisitorial in nature, not adversarial and although counsel may be present at a hearing, they have a very limited function. Put another way, the state's interests are not represented and there are no contending parties. The Board does not have powers to summons, examine witnesses or to apply traditional rules of evidence. There is no determination of rights, but rather, an assessment of risk predicated on criteria set out in law. The information reviewed is highly personal, involving third parties, and is often medical or psychological in nature. Although observers can apply to attend, hearings are not open to the public. This also makes sense when one considers the correctional environment within which parole hearings are conducted.

AB at p. 352

[42] The key point in the Board's reasoning is that its proceedings are inquisitorial, not adversarial in nature, as evidenced by the fact that the state's interests are not represented and there are no contending parties: AB at p. 352. The conclusion that the Board does not act quasi-judicially flows from the Supreme Court's

decision in *Mooring*, which was relied upon by the Federal Court as well. The balance of the Board's

1570

justification rests on the fact that the proceedings are not adversarial.

[43] The debate before the Federal Court on the open court principle turned on whether the Board is a quasi-judicial body. In *Mooring*, the issue was whether the Board was a court of competent jurisdiction so as to have jurisdiction to award remedies under subsection 24(2) of the Charter. In the course of its reasoning, the Supreme Court noted that the Board did not act in a judicial or quasi-judicial manner. This conclusion was founded, in part, on the fact that the Board did not hear evidence but, instead, proceeded on the basis of the information available to it: *Mooring* at paras. 25-26. The Supreme Court went on to observe that:

The language of the *Corrections and Conditional Release Act* confers on the Board a broad inclusionary mandate. Not only is it not bound to apply the traditional rules of evidence, but it is required to take into account “all available information that is relevant to a case”. No mention is made of any power to apply exclusionary rules of evidence. Indeed, such a provision would conflict with its duty to consider “all available information that is relevant”.

Mooring at para. 29 (emphasis in original)

[44] The Supreme Court concluded that:

I conclude from the foregoing that the Board does not have jurisdiction over the remedy sought [the exclusion of evidence]. It is not, therefore, a court of competent jurisdiction within the meaning of s. 24 of the *Charter*.

Mooring at para. 30

[45] The Supreme Court found that the Board was not a court of competent jurisdiction in that it did not have the power to reject evidence, given that it was required to take into account “all available information that is relevant” to a case. The characterization of the Board’s proceedings as neither judicial nor quasi-judicial, while a consideration, was not determinative of the Supreme Court’s conclusion as to whether the Board was a court of competent jurisdiction for the purposes of section 24 of the Charter. The only link between *Mooring* and the application of the open court principle to the Board is its determination that the Board was not a quasi-judicial tribunal.

[46] While this Court’s focus is on the Board’s decision, it is worth noting that in the course of its analysis of *Mooring*’s relevance, the Federal Court held that the Supreme Court’s decision in *Minister of National Revenue v. Coopers and Lybrand*, [1979] 1 S.C.R. 495, 92 D.L.R. (3d) 1 [*Coopers and Lybrand*] was of no

1571

assistance. That case dealt with this Court's jurisdiction in judicial review which, at the time, applied only to a "... decision or order other than a decision or order of an administrative nature not required by law to be made on a judicial or quasi-judicial basis ...": *Coopers and Lybrand* at p. 499.

[47] Notwithstanding the fact that the Supreme Court changed its position in *R. v. Bird*, 2019 SCC 7, [2019] 1 S.C.R. 409 [*Bird*] and found that the Board was a court of competent jurisdiction for the purpose of subsection 24(2) of the Charter, the Federal Court considered that *Bird* served only to distinguish *Mooring* on that issue. The Federal Court held that *Bird* did not overrule or displace *Mooring* on the issue of whether the Board is a quasi-judicial tribunal: Decision at para. 88.

[48] With all due respect, the judicial/quasi-judicial distinction has outlived its usefulness in its application to the open court principle. The difficulty with relying on the characterization of a tribunal as quasi-judicial is that it focuses on the Board's processes and formal characteristics rather than its function. The public interest in court proceedings does not arise from a court's procedural characteristics but from the fact that it decides questions of rights and duties as between citizens and as between citizens and the state.

[49] Much of the jurisprudence on the open court principle and administrative tribunals is based on the decision of the Federal Court of Canada in *Southam Inc. v. Canada Minister of Employment and Immigration*, [1987] 3 F.C. 329, 13 F.T.R. 138 (T.D.) [*Southam*], where the following appears at page 336:

That decision [*Re Southam Inc. and The Queen (No. 1)* (1983), 1 O.R. (2d) 113, 146 D.L.R. (3d) 408 (C.A.)] arose in the context of a court proceeding. The detention review hearing in this case involves a statutory body exercising its functions and it is to be determined if they are judicial or quasi-judicial in nature and by implication subject to accessibility; does the openness rule apply to their proceedings. Mr. Justice Dickson, as he then was, in *Minister of National Revenue v. Coopers and Lybrand*, [1979] 1 S.C.R. 495 determined that a proceeding can be found to be judicial or quasi-judicial if it met certain tests. ...

(emphasis added)

[50] The rationale for focusing on judicial or quasi-judicial tribunals was laid out in *Travers v. Canada (Chief of Defence Staff)*, [1993] 3 F.C. 528, 18 C.R.R. (2d) 135 (T.D.) [*Travers*]:

Since the adoption of the Charter, it is true that the open door doctrine [the open court principle] has been applied to certain administrative tribunals. While the bulk of precedents have been in the context of court proceedings, there has been an extension in the application of the doctrine to those proceedings where tribunals exercise quasi-judicial functions which

of the doctrine to those proceedings where tribunals exercise quasi-judicial functions, which is to say that, by statute, they have the jurisdiction to determine the rights and duties of the parties before them.

This more extensive doctrine would appear to be entirely consistent with its original purpose. If justice is to be patently and evidently done in the courts, there is no reason why it should not also be done when a tribunal exercises substantially the same judicial functions.

Travers at p. 532

[51] There are two threads in this explanation. The first follows from the observation in *Southam*, quoted above, that the tribunal in that case was “a statutory body exercising its functions”. *Travers* completes this by noting that tribunals to whom the open court principle had been extended were tribunals where “by statute, they have the jurisdiction to determine the rights and duties of the parties before them”. The second is that the legitimacy of tribunals whose function closely resembles that of the courts rests on the same public oversight of their work by the media. This is consistent with the conclusion reached by the Court in *Southam*:

After all, statutory tribunals exercising judicial or quasi-judicial functions involving adversarial-type processes which result in decisions affecting rights truly constitute part of the “administration of justice”. The legitimacy of such tribunals' authority requires that confidence in their integrity and understanding of their operations be maintained, and this can be effected only if their proceedings are open to the public.

Southam at p. 336 (emphasis added)

[52] As these passages demonstrate, the application of the open court principle, while linked to a tribunal’s quasi-judicial status, rests on a broader footing. If the quasi-judicial distinction has outlived its usefulness, the question that arises is what will replace it as an indicator of the applicability of the open court principle.

[53] It appears that, whatever other distinctions may exist between different kinds of administrative tribunals, the fact that a tribunal presides over adversarial proceedings as an adjudicative body is a reliable indicator that the tribunal is subject to the open court principle. It is the fact of adjudicating competing interests that imposes the duty of fairness and impartiality which gave rise to the description of some tribunals as quasi-judicial. In *Toronto Star Newspapers Ltd. v. Ontario (Attorney General)*, 2018 ONSC 2586, 142 O.R. (3d) 266, such tribunals were described as adjudicative tribunals. The characteristic that gives rise to the application of the open court principle to an administrative tribunal is the presence of an adversarial process, as opposed to the formalities by which that adversarial process is conducted. In short,

[54] Is the Board an adjudicative tribunal? The Board says that it is not because its proceedings are inquisitorial – not adversarial – in that the Board is engaged in a risk assessment process in the course of which it receives information from Corrections Canada and submissions from the offender and victims. The offender is not opposed by a representative of the state, as is the case, for example, in a sentencing hearing. Similarly, the offender’s counsel, if they have one, has a limited role in Board hearings.

[55] The CBC argues that the open court principle applies (or should apply) because of the public interest in the subject matter of a hearing. At paragraph 32 of its memorandum of fact and law, the CBC argues that the open court principle, as recognized in section 2(b) of the Charter, arises from “the public’s right to express ideas about public institutions and obtain information about their functioning”, sentiments that are expressed in *Southam* and *Travers* quoted earlier in these reasons. This casts a wider net than does the categorization of a tribunal as “quasi-judicial” or “adjudicative”. While the public has an interest in knowing about the functioning of all public bodies, the open court principle has to date been limited to those public bodies whose resemblance to courts invites the same degree of public oversight represented by the open court principle. It may be that, at some point, a broader foundation for the “openness” will be articulated, but the facts of this case do not justify that change.

[56] In the result, the Board and the Federal Court did not err in concluding that the open court principle does not apply to the Board’s proceedings. This creates the anomalous situation in which a tribunal whose hearings are presumptively open to the public is not subject to the open court principle. There are many public agencies whose meetings are open to the public but that are not subject to the open court principle. This is not to say that section 2(b) of the Charter does not apply to them, simply that openness is more nuanced and may not be as fulsome as it is in relation to adjudicative tribunals that are subject to the open court principle. The fact that an administrative body opens its doors to the public is not sufficient, in and of itself, to trigger the application of the open court principle.

[57] While I have differed somewhat from the Board’s analysis, I come to the same conclusion on the question of the applicability of the open court principle. As a result, it cannot be said that the Board’s

1574
 decision was in error.

[58] With that in mind, I now turn to the question of whether the CBC is otherwise entitled to copies of the audio recordings.

C. Access to the audio recordings

[59] The CBC couched its alternative arguments for disclosure in constitutional terms and so the debate that ensued was largely framed in constitutional terms. But it is worth pausing for a moment to take stock of the more mundane issues in this debate.

[60] In the first place, this is not a debate about whether the CBC can report on Board hearings. As noted earlier, Board hearings are presumptively open to the public, so the CBC and other members of the press are able to attend and to report on what takes place at those hearings. In fact, the Board noted that the CBC has attended hearings in at least one of the cases for which it has requested copies of the audio recordings. At this stage of the argument, the debate is about whether the CBC should be able to access audio recordings of Board hearings on the same basis as it attends the hearings themselves.

[61] This would permit the CBC and other media organizations to cover hearings that they could not attend in person, either because they were not advised of their scheduling or because of resource constraints. Disclosure of the audio recordings would also allow the media to ensure that their reporting is accurate.

[62] The first potential hurdle the CBC identified that might stand in its way was subsection 140(13) of the Act which provides as follows:

140 (13) Subject to any conditions specified by the Board, a victim, or a person referred to in subsection 142(3), is entitled, on request, after a hearing in respect of a review referred to in paragraph (1)(a) or (b), to listen to an audio recording of the hearing, other than portions of the hearing that the Board considers

140 (13) La victime ou la personne visée au paragraphe 142(3) a le droit, sur demande et sous réserve des conditions imposées par la Commission, une fois l'audience relative à l'examen visé aux alinéas (1)a) ou b) terminée, d'écouter l'enregistrement sonore de celle-ci, à l'exception de toute partie de l'enregistrement qui, de l'avis de la Commission :

(a) could reasonably be expected to jeopardize the safety of any person or

a) risquerait vraisemblablement de mettre en danger la sécurité d'une personne ou

reveal a source of information obtained in confidence; or

de permettre de remonter à une source de renseignements obtenus de façon confidentielle;

(b) should not be heard by the victim or a person referred to in subsection 142(3) because the privacy interests of any person clearly outweighs the interest of the victim or person referred to in that subsection.

b) ne devrait pas être entendue par la victime ou la personne visée au paragraphe 142(3) parce que l'intérêt de la victime ou de la personne ne justifierait nettement pas une éventuelle violation de la vie privée d'une personne.

[63] The CBC argued that subsection 140(13) did not mean that audio recordings could not be provided to the public.

[64] The Board responded to the CBC's argument by conceding that the CBC was correct that the provision did not bar the Board from providing the CBC with copies of audio recordings. However, the Board was silent on whether the provision required the Board to do so. Judging from its refusal to provide the copies, the Board concluded that subsection 140(13) did not compel production.

[65] The restrictions on disclosing personal information in the *Privacy Act* and subsection 140(14) of the Act are another obstacle in the CBC's way. While the CBC did not make its request under the AIA, it is nonetheless relevant that section 19 of the AIA prohibits government institutions from disclosing personal information unless certain conditions are met, one of which is that the information is publicly available. Subsection 8(1) of the *Privacy Act* restates the prohibition on disclosure of personal information by stipulating that personal information under the control of a government institution cannot be disclosed by the institution except with the consent of the individual concerned or in accordance with the provisions of subsection 8(2). There is exemption from section 8 in subsection 69(2) of the *Privacy Act*, which concisely provides that section 8 does not apply to information that is publicly available.

[66] The difficulty, from the CBC's point of view, is subsection 140(14) of the Act which is reproduced below:

140 (14) If an observer has been present during a hearing or a victim or a person has exercised their right under subsection (13), any information or documents discussed or referred to during the

140 (14) Si un observateur est présent lors d'une audience ou si la victime ou la personne visée au paragraphe 142(3) a exercé ses droits au titre du paragraphe (13), les renseignements et documents qui

1576

hearing shall not for that reason alone be considered to be publicly available for purposes of the *Access to Information Act* or the *Privacy Act*.

y sont étudiés ou communiqués ne sont pas réputés être des documents accessibles au public aux fins de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*.

[67] Subsection 140(14) creates a legal fiction by stipulating that information and documents discussed in a Board hearing which – it will be recalled, is presumptively open to the public – are not publicly available solely by reason of the fact that observers are present at the hearing. The purpose of allowing observers at a hearing is to make the information discussed at the hearing available for different public views. Given the right of media representatives to attend Board hearings and the absence of restriction on what they can report, it is difficult to see the logic of subsection 140(14).

[68] The objective of allowing observers to attend, as stated by the Board in its letter to the CBC, is to address the public's right to know. Allowing the press to access audio recordings of Board hearings on the same basis as the press' access to the hearings themselves would serve exactly the same goal as that now served by the attendance of observers.

[69] As the Supreme Court explained in *R. v. Vice Media Canada Inc.*, 2018 SCC 53, [2018] 3 S.C.R. 374 [*Vice Media*] at paragraph 125 of its decision:

Section 2(b) sets out generous protections designed to facilitate the healthy functioning of our democracy. But they are incomplete if s. 2(b) is viewed only as an individual right to freedom of expression, reading out protection of “freedom of the press”. A vigorous, rigorous, and independent press holds people and institutions to account, uncovers the truth, and informs the public. It provides the public with the information it needs to engage in informed debate. In other words, it is the public's “right to know” that explains and animates the distinct constitutional protection for freedom of the press [citations omitted].

[70] Subsection 140(14) is unambiguous in its terms. It specifically addresses the fact that “information” disclosed or discussed at a Board hearing is not publicly available for the purposes of the *Privacy Act* solely because an observer was present. Given the Supreme Court's comments in *Vice Media*, the temptation to plead the unconstitutionality of subsection 140(14) arises. But that temptation should be resisted unless it is shown that there is no other way for the CBC to obtain the information it seeks.

1577

[71] Provision does exist for the disclosure of personal information in certain circumstances, notably under paragraph 8(2)(m) of the *Privacy Act*, which I reproduce once more for the sake of convenience:

8 (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

...

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

8 (2) Sous réserve d'autres lois fédérales, la communication des renseignements personnels qui relèvent d'une institution fédérale est autorisée dans les cas suivants :

...

m) communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

(i) des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée,

(ii) l'individu concerné en tirerait un avantage certain.

[72] The CBC invoked subsection 8(2) in its email requesting the audio recordings and the Board addressed this provision in its decision.

[73] The Board began by observing that, “under the [*Privacy Act*], there is a presumption of non-disclosure unless the individual consents or it is authorized under subsection 8(2) of the [*Privacy Act*]”: AB at p. 354. Much umbrage was taken at this suggestion of a presumption of non-disclosure, resulting in arguments that unless disclosure is prioritized, the scheme is unconstitutional. With respect, there is no presumption of non-disclosure. There is qualified prohibition on disclosure of personal information in section 19 of the AIA, and a framework is provided for the release of that information in defined circumstances. Such a scheme is not unconstitutional in and of itself.

[74] The protection of privacy has been recognized as a protected interest, even in a constitutional context:

First, this Court has often observed that privacy is a fundamental value necessary to the preservation of a free and democratic society (*Lavigne v. Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, [2002] 2 S.C.R. 773, at para. 25; *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 S.C.R. 403, at paras. 65-66, per La Forest J. (dissenting but not on this point); [*Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 SCR 480, 139 D.L.R. (4th) 385], at para. 40).

1578

Courts have invoked privacy, in some instances, as the basis for an exception to openness under the *Sierra Club* test (see, e.g., *R. v. Henry*, 2009 BCCA 86, 270 B.C.A.C. 5, at paras. 11 and 17).

Sherman Estate v. Donovan, 2021 SCC 25, 458 D.L.R. (4th) 361 at para. 31

[75] The fact that personal information is protected in courtrooms under certain circumstances is a clear indication that interference with the public disclosure of personal information is not, in and of itself, unconstitutional.

[76] After discussing the mandate of the Board and how it differs from the sentencing process, the Board wrote:

Thus the nature of the process itself, calls on the offender to divulge highly sensitive and personal information which, if disclosed to the public, would undermine the effectiveness of the legislative scheme and the ability to assess risk to public safety. ...

An appropriate balance must be maintained between the offender's right to privacy, which in turn contributes to the quality of information used for decision-making, and the public's right to know. The [*Corrections Act*] achieves this balance by providing for the attendance of observers at hearings, and for access to the Board's reasons for decision, both in accordance with established criteria.

AB at p. 354

[77] This leaves the impression that the measures that the Board identified are the full extent of the Board's obligation to recognize the public's and the press' right to disclosure of personal information. That impression is confirmed in the following paragraph:

In this case, I have determined that the public interest has not been sufficiently demonstrated. Furthermore, I am not satisfied that the public interest in disclosure of the information would clearly outweigh the privacy interests of the individuals involved. Conversely, the invasion of privacy is clear. It is not possible to overlook the consequences that would likely result from a discretionary release of personal information if public interest were to have been demonstrated in this case. Where there is a possible invasion of privacy balanced against a public interest, consideration may be given to who would be receiving the information and whether any controls can be placed on further use or release. In my informed opinion, any offender in such a circumstance would be at very real risk of having his reintegration potential as a law-abiding citizen compromised or derailed by the high degree of media and/or public scrutiny that could reasonably be anticipated.

AB at p. 354

[78] It is striking that the Board reacted to the request for the audio recordings of Board hearings as though

1579

if there a request for the Offenders' complete files. The personal information on the audio recordings has already been disclosed, even though it is deemed not to be publicly available, though it may well be so if media representatives have attended the hearing and reported on it. The threats and dangers arising from "a discretionary release of personal information" are significantly overstated in that the personal information has already been disclosed.

[79] The other striking feature of the Board's response is its apparently closed mind to the possibility of

and the disclosure of the information of the Board's decision and the availability of Board decisions.

🔔 Recent Additions ✉ Mailing List

norma
by Lexum

Website last modified:

2026-06-26