Office of the
Saskatchewan Information
and Privacy Commissioner

2022/2023

ANNUAL REPORT

Data

306-787-8350 / 1-877-748-2298

intake@oipc.sk.ca

oipc.sk.ca

Office of the
Saskatchewan Information
and Privacy Commissioner

June 26, 2023

Hon. Randy Weekes
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

I am pleased to present my ninth Annual Report as Information and Privacy Commissioner for Saskatchewan. I have prepared this Annual Report in accordance with the provisions of section 62(1) of *The Freedom of Information and Protection of Privacy Act* (FOIP), section 52(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and section 60(1) of *The Health Information Protection Act* (HIPA).

I would like to thank you and the Board of Internal Economy for their support in the past year and I look forward to working with the board to provide citizens with a high level of service.

I thank the Members of the Legislative Assembly for their support of my office. Going forward, I ask for their support in modernizing the legislation.

I also thank the staff of my office for their hard work over the last year in bringing us closer to issuing reports within180 days.

Respectfully submitted,

Original signed by
Ronald J. Kruzeniski, K.C.
Information and Privacy Commissioner

Contents

Commissioner's Message

Data

In this Annual Report, I hope to focus Saskatchewan on data. We generate a lot of data. That data is stored in databases in Saskatchewan, Canada, the United States or other places in the world. Many issues arise as a result of the creation and/or assembling of data such as access, use and disclosure, retention and destruction as well as protection and security of data. Where it becomes a concern is when the data is about us – our personal information or personal health information – and is used or disclosed for purposes that we never intended. We need to consider providing the least amount of personal information or personal health information when requested and insisting that organizations only use it for its intended purpose.

System Security

There is an obligation on organizations either legislated or expected by society that the data we provide is fully protected. This means organizations in Saskatchewan, Canada and around the world need to continually assess and improve the security of their computer systems. Organizations need to train their staff annually, install software to protect against breaches, develop random audit plans and constantly monitor their systems for attack. It is not "if a breach occurs" but "when a breach occurs." Organizations need to take every opportunity to reduce the risks of a breach occurring and have protocols in place to respond effectively when something slips through the cracks.

Goals

As volumes have increased in my office, my goal for the coming year is to provide citizens, public bodies and trustees with Review and Investigation Reports much sooner. My office has a target of issuing a report within 180 calendar days and it is my hope that by December 31, 2023, we have met that target.

Legislation

FOIP is over 30 years old, LA FOIP is 30 years old and HIPA is 20 years old. Over the next year, it is my goal to outline the road ahead in terms of legislative change. It is my hope that in my next annual report, I will outline those proposed changes.

Ronald J. Kruzeniski, K.C.
Saskatchewan Information and Privacy Commissioner

About Us

The Office of the Saskatchewan Information and Privacy Commissioner (IPC) is an independent officer of the Saskatchewan Legislative Assembly. It oversees three Saskatchewan statutes:

The Freedom of Information and Protection of Privacy Act

The Local Authority Freedom of Information and Protection of Privacy Act

The Health Information Protection Act

FOIP, LA FOIP and HIPA establish the access to information and privacy rights of citizens.

Our Mission

To ensure that access to information and privacy rights in Saskatchewan are respected.

Our Mandate

The IPC ensures that public bodies respect the privacy and access rights of the citizens of Saskatchewan by:

- Informing members of the public on their information rights.
- Resolving access and privacy disputes between individuals and public bodies.
- Investigating and resolving privacy complaints.
- Making recommendations on public bodies' policies and practices.
- Commenting on proposed laws, policies and practices.

Accomplishments 2022-2023

Education and Awareness

Goals	Accomplishments
Complete and post to website Chapters 5 and 6 for *Guide to FOIP*.	Chapter 5 and Chapter 6 of the *Guide to FOIP* were posted to the website and Chapters 5 and 6 of the *Guide to LA FOIP* were also posted.

Navigating in a Digital World

Goals	Accomplishments
Review of the office's website to determine what changes and what resources should be updated.	Changes and improvements were made to the website. Our goal is to continually update the website so that it has relevant information for Saskatchewan residents.
Promote the need for a digital ID initiative.	Continue to promote a digital ID for the province.

Advocating for Improvement

Goals	Accomplishments
Promote the updating of *The Health Information Protection Regulations*.	Continue to promote HIPA regulations amendments.

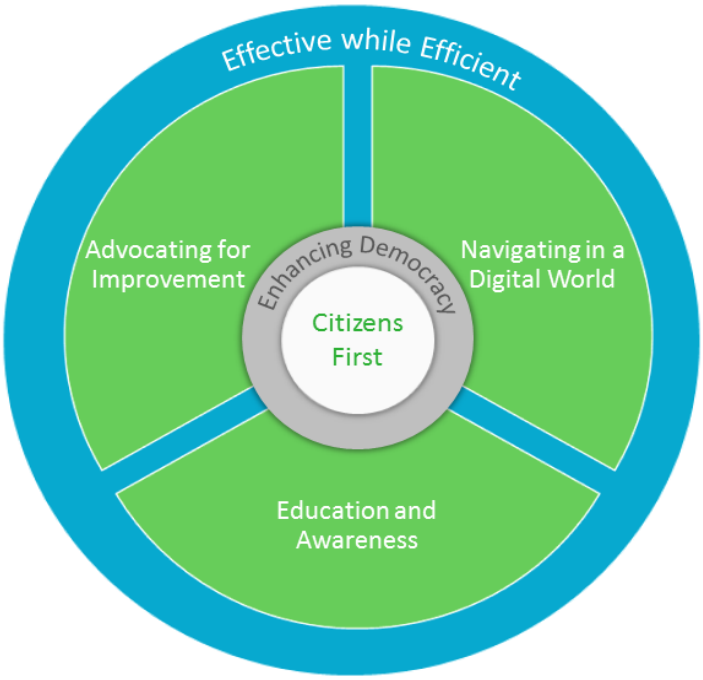
Effective While Efficient

Goals	Accomplishments
After initial contact, setup file, explore early resolution, and discontinue or assign to an Analyst within 30 calendar days.	Performed better than target at 24.8 calendar days.
Issue a Review Report or resolve a matter on review of an access request within 180 calendar days.	Did not meet target at 223.9 calendar days. It is expected we reach 180 days by December 31, 2023
Issue an Investigation Report or resolve a matter regarding breach of privacy within 180 calendar days.	Did not meet target at 214.7 calendar days. It is expected we reach 180 days by December 31, 2023
Complete or close consultation files within 30 calendar days.	Performed better than target at 11.6 calendar days
Complete or close an application to disregard within 30 calendar days.	Performed better than target at 24.7 calendar days

The Plan 2023-2024

Citizens First

Core to our work is that we support access to records as requested by citizens in a timely manner and promote protection of the privacy of those citizens wherever required. All other objectives in this document are intended to enhance and protect the rights of citizens to obtain information.



Enhancing Democracy

The freedom of information legislation in the province enshrines the principle that citizens should have access to information collected and generated by organizations supported by taxpayer dollars.

Education and Awareness

Goals
Update our website and resources to ensure that they provide citizens, public bodies and health trustees with the latest information.
Update the *Guide to FOIP*, Chapters 3 and 4.
Update the *Guide to LA FOIP*, Chapters 3 and 4.

Begin redevelopment of the *Guide to HIPA* including a completion of Chapters 1 and 2.
Promote mandatory annual access, privacy and security training for employees within public bodies and health trustees.
Promote public bodies and health trustees in making full use of their website to provide citizens with information and documents; and promote legislation requiring documents and information to be posted on an organization's website.
Promote public bodies and health trustees improving the security of their electronic systems to reduce the risk of a breach.
Promote public bodies and health trustees developing a plan for random auditing of access to their systems.

Navigating in a Digital World

Goals
Promote the need for a Digital Credentials initiative in the province.
Promote the elimination of traditional fax machines in the health sector.

Advocating for Improvement

Goals
Develop proposals for the modernization of FOIP and LA FOIP.
Develop proposals for the modernization of HIPA.
Request HIPA Regulation amendments including broadening the definition of a "trustee".
Request regulation amendments to FOIP and LA FOIP including broadening the lists of government institutions or local authorities.

Promote that all non-governmental organizations who receive government or local authority funds will be subject to Part IV of FOIP or LA FOIP (Protection of Privacy).
Promote professional regulatory bodies utilizing their websites to provide documents and information to citizens.
Promote independent schools be treated like school boards and made local authorities.

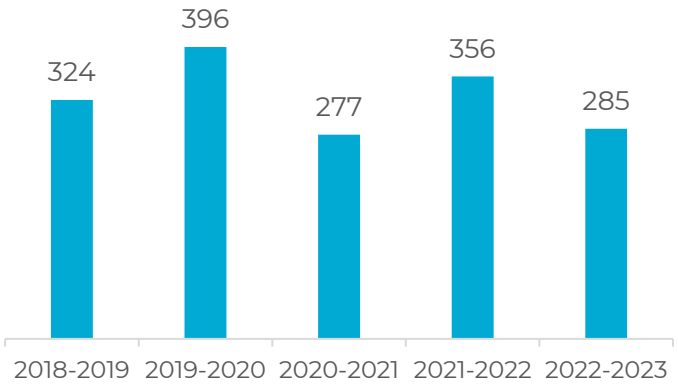
Efficient While Effective

Goals
Enhance the security protection afforded to the office's extremely confidential case files.
With an aim to continuous improvement, streamline our processes to issue our reports or close files faster.
Provide summary advice to questions posed by citizens, public bodies and health trustees within 72 hours, 90% of the time.
After initial contact, setup file, explore early resolution, and discontinue or assign to an Analyst within 30 calendar days.
Issue a Review Report or resolve a matter on review of an access request within 180 calendar days.
Issue an Investigation Report or resolve a matter regarding a breach of privacy within 180 calendar days.
Complete or close consultation files within 30 calendar days.
Complete or close an application to disregard within 30 calendar days.

Files and Reports

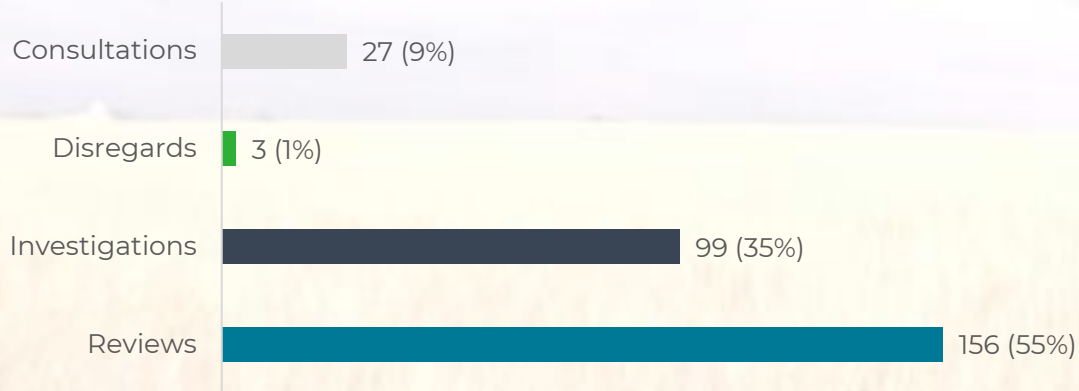
Files Opened

In 2022-23, the number of files opened, decreased and this allowed my office to close more files and deal with the outstanding older files.



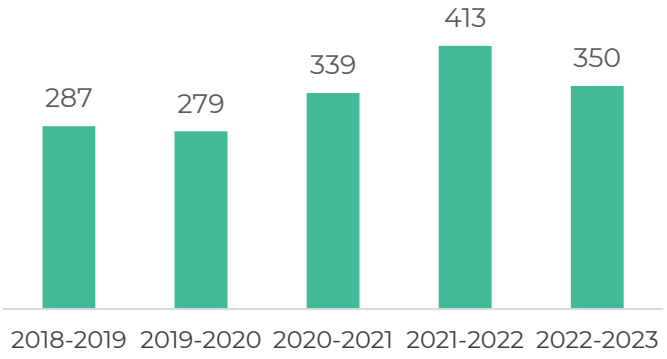
Types of Files Opened

55% of the files opened involved asking the office to do a review of the decision of a head to deny access and 35% involved files where my office was investigating a breach.



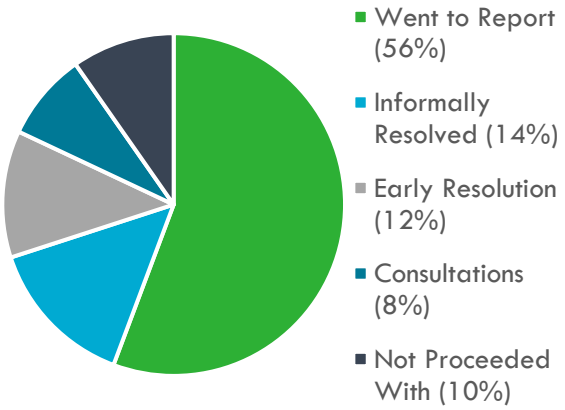
Files Closed

In 2022-23 my office closed more files than we opened and we were able to close a good number of older files.



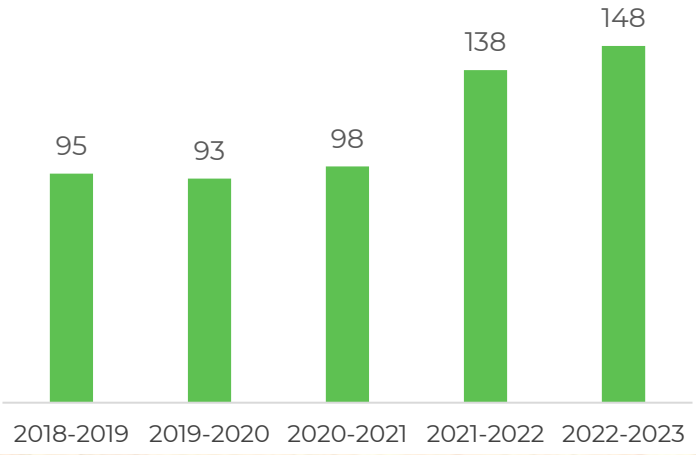
Resolution of Files

56% of the files resulted in a report, while the others were resolved in other ways.



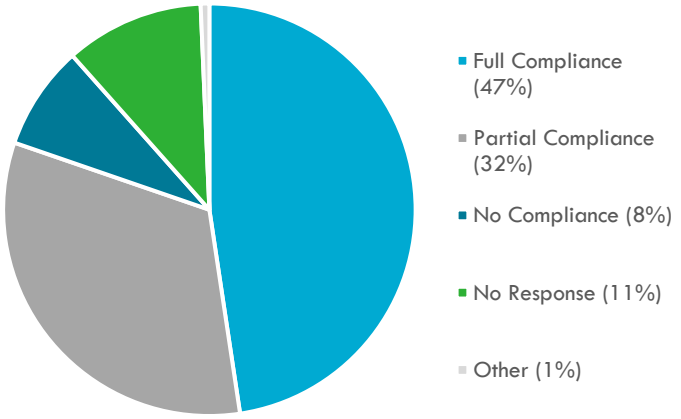
Reports Issued

My office, during this year, issued 148 reports which was the highest number of reports issued in a fiscal year.



Compliance with Recommendations

The office issued 148 reports in the 2022-2023 fiscal year. A public body or trustee is required to respond to the recommendations within 30 days of receiving the report. This is a chart showing the percentage of reports where there is full compliance, partial compliance, no compliance, and where no response was received. 47% of public bodies and health trustees were in full compliance with the recommendations.



My office is obligated to report on the recommendations that were not complied with - see FOIP, subsection 62(2); LA FOIP, subsection 52(2); and HIPA, subsection 60(2). Failure to respond to a report is considered to be non-compliance. On the following pages are three tables; the first table lists those public bodies and trustees that responded to a report with no compliance, the second table lists those public bodies and trustees that responded to a report with partial compliance, the third table lists those public bodies and trustees that did not respond at all.

NO COMPLIANCE

Government Institution	Report #	Recommendation(s) not complied with*
Ministry of Education	Review Report 274-2021	[61], [62], [63]
Ministry of Environment	Review Report 126-2022	[18]
Ministry of Environment	Review Report 204-2022	[77]
Ministry of Labour Relations and Workplace Safety	Review Report 056-2022	[37]

Saskatchewan Liquor and Gaming Authority	Review Report 225-2022	[71]
Saskatchewan Power Corporation	Review Report 243-2022	[29]
Saskatchewan Telecommunications	Review Report 106-2022	[99], [100], [101]
Local Authority	**Report #**	**Recommendation(s) not complied with***
Regina Police Service	Review Report 063-2021	[19]
RM of North Qu'Appelle No. 187	Investigation Report 062-2022	[42], [43]
Trustee	**Report #**	**Recommendation(s) not complied with***
Saskatchewan Health Authority	Investigation Report 005-2022, 006-2022	[48]
Saskatoon Obstetric & Gynecologic Consultants, Dr. Barry Gilliland, Dr. Marilyn Davidson, Dr. Natasha Payton	Investigation Report 089-2021	[61], [62], [63], [64], [65], [66], [67], [68], [69], [70]

***Refers to paragraph number in the Report. Click on the link to go directly to the Report.**

PARTIAL COMPLIANCE

Government Institution	Report #	Recommendation(s) not or partially complied with*
Ministry of Agriculture	Review Report 108-2022	[61], [62]
Ministry of Corrections, Policing & Public Safety	Investigation Report 088-2022	[56], [58]
Ministry of Environment	Review Report 128-2022	[84], [85], [88]
Ministry of Government Relations	Review Report 049-2021	[154], [155], [157], [158], [159], [160]
Ministry of Government Relations	Review Report 369-2021	[43]
Ministry of Health	Review Report 220-2021, 235-2021	[140], [141], [143], [144], [145]
Ministry of Health	Review Report 322-2021, 030-2022	[52], [55]
Ministry of Health	Review Report 003-2022	[213]
Ministry of Health	Review Report 144-2022	[30], [31]
Ministry of Health	Review Report 150-2022	[29]
Ministry of Highways	Review Report 133-2020	[208], [209]
Ministry of Highways	Review Report 323-2021	[74]
Ministry of Justice and Attorney General	Review Report 220-2020	[68], [69], [70]
Ministry of Labour Relations and Workplace Safety	Review Report 337-2021	[71]

Ministry of Labour Relations and Workplace Safety	Review Report 047-2022	[52]
Ministry of Labour Relations and Workplace Safety	Review Report 155-2022	[99], [102], [105]
Ministry of Social Services	Review Report 138-2021, 185-2021	[240]
Ministry of Social Services	Review Report 139-2021, 203-2021	[137]
Ministry of Social Services	Review Report 140-2021, 186-2021	[129]
Ministry of Social Services	Review Report 269-2021	[38], [39]
Ministry of Social Services	Review Report 142-2022	[57], [59]
Saskatchewan Human Rights Commission	Review Report 140-2022, 141-2022	[150], [151]
Saskatchewan Human Rights Commission	Review Report 145-2022	[68], [70], [71], [72]
Saskatchewan Power Corporation	Review Report 004-2022	[142], [144], [145], [146]
Local Authority	Report #	Recommendation(s) not or partially complied with*
City of Prince Albert	Review Report 037-2022	[91], [93], [94]
City of Regina	Review Report 224-2021	[99], [101]
City of Saskatoon	Review Report 115-2021	[52]
City of Saskatoon	Review Report 119-2022	[85]
Moose Jaw Police Service	Review Report 055-2021, 056-2021	[50]
Moose Jaw Police Service	Review Report 196-2021	[50]
Regina Police Service	Review Report 284-2020	[53]

Regina Police Service	Investigation Report 208-2021	[53]
Regina Police Service	Review Report 129-2022	[38], [39]
Regina Police Service	Review Report 132-2022	[38], [40]
Resort Village of Candle Lake	Review Report 214-2022	[15]
Resort Village of Kivimaa-Moonlight Bay	Investigation Report 250-2021	[51]
RM of North Qu'Appelle No. 187	Investigation Report 154-2021	[58], [59], [60]
Saskatoon Police Service	Review Report 215-2020	[61]
Saskatoon Police Service	Review Report 043-2022	[75]
Saskatoon Police Service	Review Report 111-2022	[95], [97], [98], [100], [101]
Saskatoon Police Service	Review Report 210-2022	[38]
Weyburn Police Service	Review Report 156-2022	[41], [43]
Trustee	Report #	Recommendation(s) not or partially complied with*
Dr. Lalita Malhotra	Investigation Report 154-2022	[73]
Saskatchewan Health Authority	Investigation Report 126-2021	[38]
Saskatchewan Health Authority	Investigation Report 272-2021	[38], [39]
Saskatchewan Health Authority	Investigation Report 032-2022	[47], [48]
Saskatchewan Health Authority	Investigation Report 080-2022	[62], [63], [64], [65], [66], [67], [68]

Saskatchewan Health Authority	Investigation Report 081-2022	[59], [60], [62]
Saskatchewan Health Authority	Investigation Report 120-2022, 135-2022	[72], [73], [74], [77], [78], [79], [80]

***Refers to paragraph number in the Report. Click on the link to go directly to the Report.**

NO RESPONSE RECEIVED

Government Institution	Report #	Recommendation(s) not complied with*
Ministry of Corrections, Policing & Public Safety	Review Report 164-2021	[138], [139]
Ministry of Corrections, Policing & Public Safety	Review Report 160-2022	[50]
Ministry of Corrections, Policing & Public Safety	Review Report 244-2022	[29]
Ministry of Highways	Review Report 324-2021	[46], [47]
Ministry of Justice and Attorney General	Review Report 289-2021	[42]
Ministry of Justice and Attorney General	Review Report 346-2021	[19]
Public Complaints Commission	Review Report 104-2022	[19], [20]
Saskatchewan Government Insurance	Review Report 147-2020	[64], [65]
Local Authority	**Report #**	**Recommendation(s) not complied with***
Living Sky School Division No. 202	Review Report 019-2022	[20]
Living Sky School Division No. 202	Investigation Report 092-2022	[44], [45]
Moose Jaw Board of Police Commissioners	Investigation Report 152-2022	[62], [63]

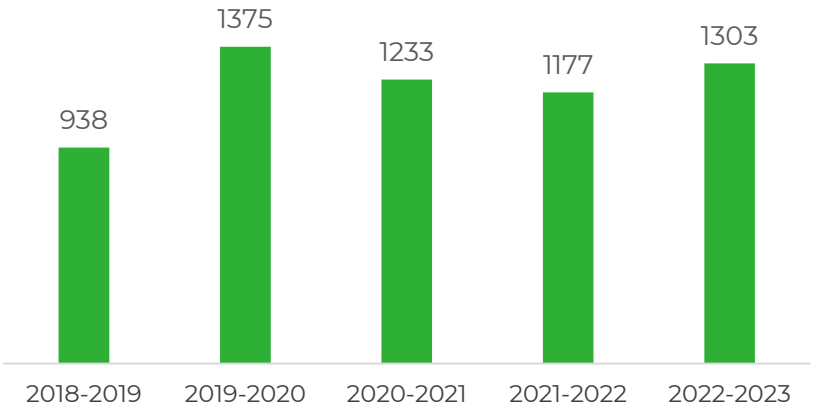
Moose Jaw Police Service	Review Report 093-2022, 117-2022	[64]
RM of North Qu'Appelle No. 187	Review Report 098-2022	[82], [83]
RM of North Qu'Appelle No. 187	Investigation Report 112-2022	[29], [30]
RM of Rosthern No. 403	Review Report 165-2022	[40], [41]
Town of Ituna	Review Report 077-2022	[24]

Trustee	Report #	Recommendation(s) not complied with*
Brightwater Senior Living	Review Report 290-2021, 023-2022	[43], [44]
Metis Addictions Council of Saskatchewan Inc.	Investigation Report 158-2022	[66], [67], [68], [69]

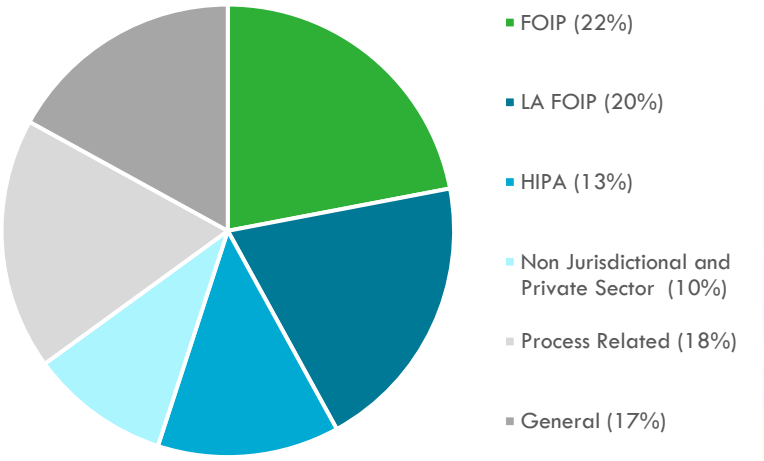
***Refers to paragraph number in the Report. Click on the link to go directly to the Report.**

Summary Advice

In 2022-23 my office provided advice to residents of Sask in 1303 instances. This was the 2nd highest year.



From the chart to the right, it is clear that the office gives advice related to the three main statutes where the office has jurisdiction; 55% of summary advice was given related to these pieces of legislation.

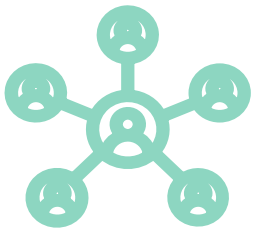


Data

We, as Saskatchewan residents and Canadians, generate a lot of data every day. We do so on our computers, laptops and cell phones. A lot of it is data about you, but do you know who has it and what they do with it? Below, we will reflect on some of those issues.

Throughout this Annual Report, I will provide links to resources which include information about data and the related issues. Let me start by referring to a recently published book, "Your Data, Their Billions: Unraveling and Simplifying Big Tech" by Jane S. Hoffman.

Collection of data



Each time we do a search on the internet, go to a website, log into an account, purchase something online, check our bank balance or post a blog or video, we create data and add to the content on the internet. We call it collection of data. That data is being stored on a server locally, nationally or internationally. Our province may legislate provincially regarding the collection of data. If data is held nationally, our country can legislate. However, if our data is stored internationally, the country where it is held may have legislation or may not. It really comes down to who has possession/custody or control of the data in terms of what access/privacy law will apply.

Provincially our province has passed legislation to address these concerns in *FOIP*, *LA FOIP* and *HIPA*. Canada has passed the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and currently is considering Bill C-27, the *Consumer Privacy Protection Act*, the *Personal Information and Data Protection Tribunal Act* and the *Artificial Intelligence and Data Act*, which I discuss below.

Provincially the legislation mentioned above applies to government ministries, Crown corporations, school boards, universities, municipalities, cities, towns, villages and health trustees, among others. PIPEDA applies to many organizations in Saskatchewan (i.e., federally regulated entities and organizations carrying on "commercial activities") and Bill C-27 will apply to more organizations in Canada.

If an organization operates in Alberta, British Columbia or Quebec that provincial legislation might apply to operations there.

There are rules that might apply to those that hold your personal information provincially or in Canada, but what about internationally; what rules apply to those that hold your information in other countries? Since many Big Tech companies operate in the United States (US), and US laws apply to them, consideration is needed as to whether the US law helps us. There have been proposals for privacy legislation federally with a number of states having introduced privacy legislation including California with the *Consumer Privacy Protection Act* (CPPA).

Privacy

With so much information about us, we should be concerned about our privacy. Privacy is a difficult term to define and each of us might define it differently but overall, all of us can point to information about us that we don't want others to know, which generally falls into the category of personal information. The best way of accommodating our differing views is to provide us with the choices as to how much information about us can be collected, used, stored or disclosed.

The Privacy Commissioner of Canada, in his annual report has recognized that with all the data collected, it is a pivotal time for privacy.

Consent

As we do our work or socialize on the internet, we login and set up accounts and we consent to the use and collection of our information. How many of us read those consents which include terms and conditions? How often do we just click "yes" and proceed? What are we consenting to, what uses are we agreeing to and do we think about who else personal information will be disclosed to and for what purpose? Are we giving companies permission to almost do whatever they want with our data without thinking about the consequences?

Different kinds of data

There is personal information (birth date, telephone numbers, our personal opinions), personal health information (diagnosis, medication taken, surgery performed), and then there is just data. Some of that data is sensitive and we would not want others to have or know that about us. Other data we just do not care about. Collectively Big Tech and data brokers have a lot of data about us.

Use of data

I mentioned consents that we all may not fully read or consider. Well, we probably are agreeing to companies using our data as they wish or as they specify and, in many cases, we are agreeing to the transfer of data to others. We don't know what those others are doing with that data and how that may come back to haunt us down the road.

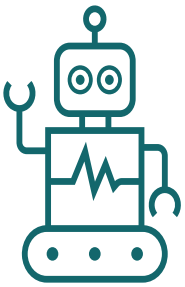
TikTok

When you upload a video to TikTok you are adding to the data collected about you. The federal government and many provinces have banned TikToK from government provided devices. Announcement: Commissioners launch joint investigation into TikTok - Office of the Privacy Commissioner of Canada.

In the future it will be necessary for all of us to make decisions regarding which apps we have on our work devices and which apps we have on our personal devices. Use of fewer apps reduces the data you are giving to others.

Artificial Intelligence (AI)

There has been a lot of talk about AI in the last few years. Artificial intelligence suggests that a computer can take data about us, analyze it and make predictions about us or make decisions regarding us. Similarly, AI can take data of many people and make predictions or decisions about the group. The predictions and decisions are very dependent on the assumptions built into the AI program. There are concerns about the program (algorithms) and the biases that might be built into the program code. You can find more on this on the Office of the Privacy Commissioner of Canada "Privacy Tech-Know blog: When worlds collide – The possibilities and limits of algorithmic fairness (Part 2)".



Bill C-27 now considered by the parliament of Canada, introduces a new Act called the *Artificial Intelligence and Data Act*. For a good summary on this new proposed Act, see "The Artificial Intelligence and Data Act (AIDA) Companion document."

Generative AI

Recently an AI program, ChatGPT has been released and millions have rushed to experiment with the application resulting in various articles being published regarding usability. The concept is that you can ask this application to write an essay for you, a poem or compose a song. It can even be used to generate a piece of music that imitates a well know singer. Articles have suggested it will affect some people's work. Each time we use ChatGPT, we in fact create more data about us.

The Privacy Commissioner of Canada has launched an active investigation of ChatGPT. See my offices' blog on "Chatbots and Security."

Protection of all that data

So, we are all offering up all that data, but what happens to it afterwards? I am sure most of us would say we expect the organization we are dealing with will protect our data. Provincially, FOIP requires government institutions to protect the data they have about us. Provincial legislation applies to some, but not necessarily all organizations. Canadian legislation, PIPEDA and C-27 applies to many organizations but not all. Internationally we are subject to the protections of the country where the data is stored.

Breaches

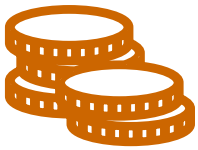
Media headlines flag the many breaches that are taking place in our country and in the world. We have had attacks on eHealth Saskatchewan, Saskatchewan Health Authority, Ministry of Health and Saskatchewan Liquor and Gaming Authority. In Canada we have had attacks on Eastern Health in Newfoundland, and Sick Children's Hospital in Ontario to name a few. It has become profitable for rogue elements in other countries to breach our systems and hold the organization for ransom. When those breaches occur, our information is exposed or at risk of exposure. For some discussion on breaches in 2022, you can read the December 20, 2022, Security News Digest.

Are we prepared?

In Cisco's Cybersecurity Readiness Index they found that only nine per cent of the organizations surveyed were well prepared to prevent breaches. Thus, ninety-one per cent, were not! Our information is stored in all those organizations (prepared and not prepared).

Cost of a breach

In a webinar (March 29, 2023) "Canada is Vulnerable to Cyber Attacks, What businesses do to protect themselves from getting burned?", one of the panelists, Mandy D'Autremont, estimated the cost of breaches ranged from $26,000 to $1,000,000. Other studies have shown the costs to remedy a breach is substantial.



Detection and prevention of breaches

In 2017, my office and eHealth Saskatchewan worked on developing *Audit and Monitoring Guidelines for Trustees*.

In a breach of privacy investigation, auditing and monitoring are not only ways to detect employee snooping but can also be used to prevent it. In a recent case, Investigation Report 197-2022, 215-2022 involving employees of the Ministry of Corrections, Policing & Public Safety, the Commissioner recommended that the Ministry implement a proactive random sampling/audit schedule to deal with a case of chronic snooping into its Criminal Justice Information Management System. If employees are aware that the random auditing is occurring and it happens on a regular basis, it might actually act as a deterrent or at least catch snoopers sooner rather than later. Subpoena

Increased Security

This brings us to a discussion of what we as citizens and organizations have to do. We have to be careful about the data we create and offer up, and we have to insist organizations take all necessary steps to protect our data. We need to advocate for greater security, locally, nationally and internationally.

Below I list a number of actions you can ask yourself, your family members, your friends, colleagues at work and organizations to do.

My focus for the last while is to encourage every organization to get very serious about increasing the security protection of their databases.

Security experts will say many breaches start by an employee not following the rules or very innocently clicking on a link that facilitates the breach. Thus, training of employees becomes absolutely necessary. I have advocated for privacy training on an annual basis and how that training, if it did not have it before, needs to have modules on security. The training needs to make employees aware of suspicious emails. There are services which will provide this

security training and in fact create simulated phishing attacks. You can see how alert your organization is to phishing attacks.

Of course, we all have heard about secure passwords and dos and don'ts re: those passwords. Microsoft has some suggestions. This is a matter we should all pay attention to.

I recall the Panama papers data breach of 11.5 million leaked documents by a law firm where the firm had not installed patches right away. Software manufacturers send out patches for a reason. They have discovered a difficulty with their system, and they want to correct it right away. Organizations should never delay in installing those patches. In fact, we should have a person assigned to monitor and check for notices of patches and then ensure that the patches get installed.

Many organizations use Microsoft products and their product Windows Defender, which checks for viruses in the system. One should be using this product, but it is possible to spend more money and become more rigorous about malware protection. There are vendors who can provide your organization with software, which is resident on every desktop, laptop and smart phone that will monitor 24-7 for attempted breaches. You can go one step further and engage a Security Operations Center where staff will monitor your systems constantly and alert you of threats and take protective action immediately.

In the past, it may have been enough to be reactive to cybersecurity threats. But being proactive is more important than ever. Organizations should be evaluating their IT and physical security posture minimally on an annual basis. Do you have the capability to conduct system activity audits? Do those audits show any suspicious activity? Are there any faults in your system configuration which could be exploited to compromise data, and do you have personnel who can find those faults? Is the configuration your IT department suggested five years ago still functional, or is there a better or more secure way? Have access permissions been properly applied by user or role, or is it a free for all once a user has system access? Organizations need to proactive and routinely assess the components which make up their security posture to keep pace with the tactics bad actors will utilize.

Better security will cost more but will reduce the risks. I encourage all to take steps they can within the funding they have to protect our data.

What will it take?

It will take all of us, to be conscious, learning more and encouraging all to be cautious and taking steps to reduce the risks of a breach.

Conclusion

We are providing more data to be stored in more databases housed in Saskatchewan, Canada, the United States and other places. There is a need for greater protection of that data and more security to reduce the risks of a breach. In order to assure your data is protected, you need to think before you click and offer up your data.

Office of the
Saskatchewan Information
and Privacy Commissioner

503 - 1801 Hamilton Street
Regina SK S4P 4B4

Phone: 306-787-8350
Toll Free: 1-877-748-2298

Email: intake@oipc.sk.ca
Twitter: @SaskIPC

W W W. O I P C. S K .C A