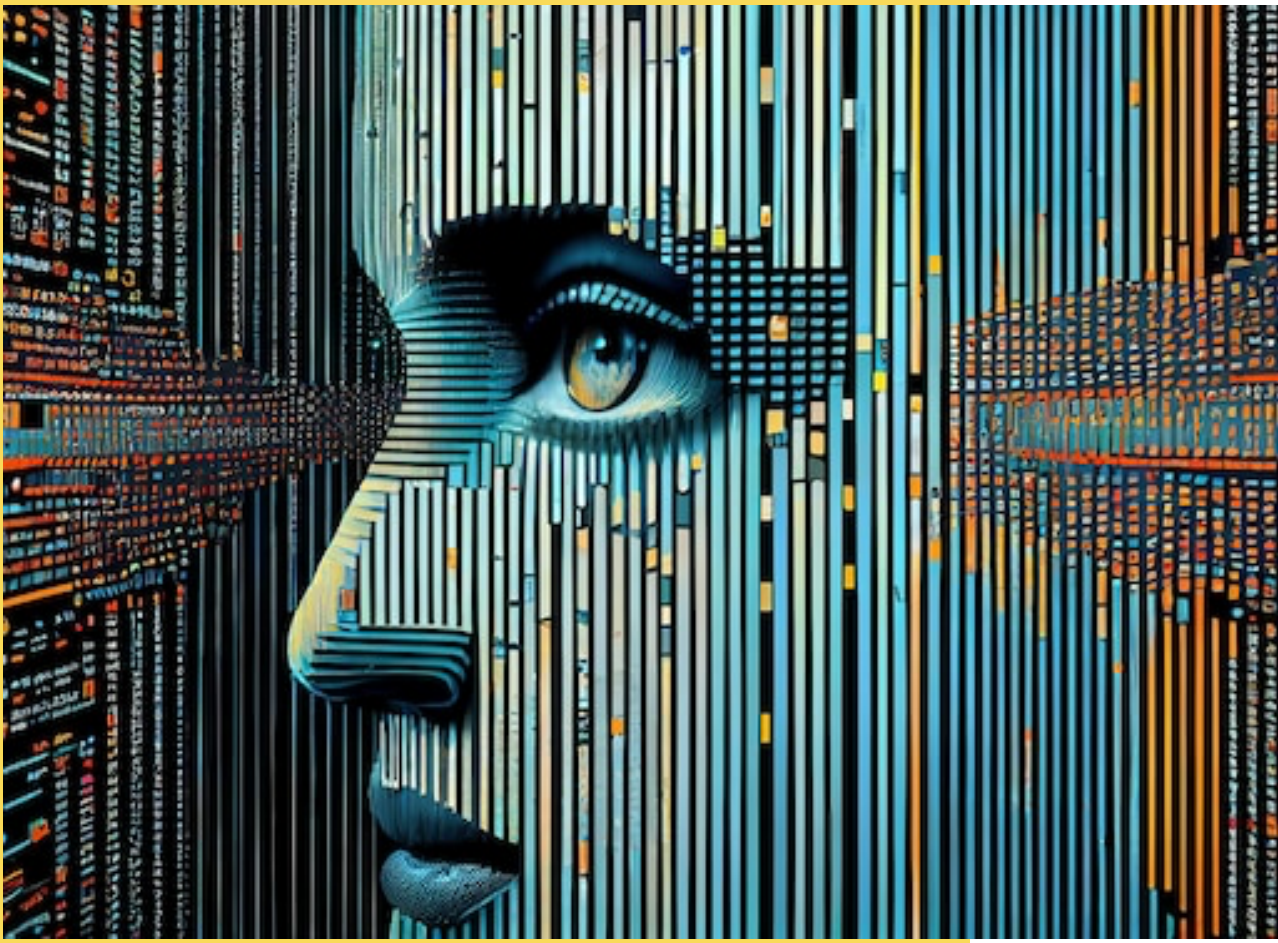
David and Goliath

Consumer protection and digital services marketplace dominance



JUNE 2023

Consumers' Association of Canada
Association des consommateurs du Canada
Manitoba

This page is left intentionally blank.

Attribution for image on cover page: Image by vecstock on Freepik

Contents

Acknowledgements

"The *Consumers' Association Canada (Manitoba)* has received funding from Innovation, Science and Economic Development Canada's Contributions Program for Non-profit Consumer and Voluntary Organizations. The views expressed in this report are not necessarily those of Innovation, Science and Economic Development Canada or of the Government of Canada."

CAC Manitoba would like to thank all those who contributed to this project. Thank you to our research team for their tireless efforts, as well as to all the contractors and consultants for their contributions to the project. Thank you as well to our methodology/gender plus reviewer for insightful input and guidance. We would also like to thank our key interviewees, focus group participants, and panel survey participants for lending their voices, and bringing a rich diversity of perspectives to the research. Their ideas, stories, and shared experiences have greatly enriched this project.

Finally we would like to thank our Advisory Committee. Their valuable feedback on each piece shaped and refined the iterative nature of the research process and enabled CAC Manitoba to address any gaps identified. The Committee offered feedback on the research methods, including which voices should be at the table in terms of the advisory panel, as well as all of the various research questions, tools, and reports and ultimately the final report and resulting recommendations. CAC Manitoba would like to thank its Advisory Committee members for their commitment to this research and for generously giving of their time, expertise, and experience to guide this work. Thank you.

Dedication

Gloria Desorcy served as the Executive Director of CAC Manitoba for thirty five years until her death in March, 2022. With kindness, compassion and good humour, Gloria dedicated her career to strengthening the consumer voice in Manitoba. Seeking fairness and justice for an accessible marketplace, consumer advocacy became her vocation. Guided by her keen understanding of the consumer interest, Gloria's many policy and research contributions, and her achievements in furthering public engagement, benefited all Manitobans.

Thus, it is with fitting gratitude and deepest honour that we dedicate this project to Gloria Desorcy.

Executive Summary

By: Jacqueline Wasney, CAC Manitoba Board Member

For close to eighty years, the Consumers' Association of Canada (CAC) Manitoba has championed the consumer interest in promoting and advocating for fairness and justice in our global marketplace. In recent years, however, the challenges and concerns faced by Canadian consumers in a rapidly expanding digital services marketplace have brought into question the effectiveness of principles, policies and practices designed to protect consumer rights to privacy, information, education and redress in digital platform use. In an effort to understand how to best serve consumers, CAC Manitoba embarked on a two year, comprehensive research project to investigate the impacts and consequences of consumer participation in a marketplace heavily dominated by corporate giants such as Google, Amazon, Facebook, Microsoft and Apple.

"The Consumers' Association Canada (Manitoba) has received funding from Innovation, Science and Economic Development Canada's Contributions Program for Non-profit Consumer and Voluntary Organizations. The views expressed in this report are not necessarily those of Innovation, Science and Economic Development Canada or of the Government of Canada."

Supported by this Federal funding opportunity, the research project, David and Goliath: Consumer protection and digital services marketplace dominance, examined several factors influencing digital participation including, the effectiveness of current legislation and regulations, consumer knowledge of privacy protections, consumer awareness and understanding of data collection practices and industry best practices for hosting digital platforms. More specifically, the project aimed to address the consequences of information gathered and stored by digital providers, understand consumer awareness and use of mechanisms designed to protect their collected data, and consumer knowledge of the consequences when protections are not in place.

The researchers felt it was also important to examine the impacts of the COVID-19 pandemic on digital use. During the pandemic, consumers were often required to

engage virtually in many aspects of their lives, making it possible they would be more vulnerable to such practices as personal data collection, targeted marketing, and political influence. The issue is especially relevant as we continue to see higher levels of consumer engagement with digital services in a post-pandemic world.

The research methods included a literature review, a review of Canadian and International legal protections and regulations, a national online panel survey of 1000 participants, five online focus groups from across Canada and interviews with ten individuals from key policy communities. Finally, an advisory panel was created to provide guidance to the project and feedback on the research tools and reports.

The Public Interest Law Centre (PILC) prepared an extensive literature review which examined consumer vulnerabilities and awareness of risks and protections as well as industry best practices. The use of digital services by consumers continues to grow worldwide, but at the same time they are exposing themselves to greater risk when they do not understand the value of their personal data or the measures available to protect it.

PILC also reviewed Canadian and International regulations and legislation pertaining to the digital services marketplace. Compared to other countries, Canada is falling behind when it comes to protecting consumer digital users. Canadian provinces and territories have generally robust consumer protections, but fall short in providing protections specific to the digital marketplace. Recent policy development and forthcoming legislation may substantially improve digital consumer protection for Canadians. The Digital Charter Implementation Act 2022 will govern the relationships between consumers and industry regarding the collection, use and disclosure of personal data including the provision of consent, and complementary measures creating means of redress. However, recent innovations in international jurisdictions can inform further development of protections for Canadians.

Professor Marina Pavlovic of the University of Ottawa (member of Centre for Law, Technology and Society) was retained by CAC Manitoba to conduct research and analysis of the current consumer protection framework and its responsiveness to the digital environment and provide suggestions for reform. While the Canadian consumer protection framework provides some basic protections for consumers, it is not fit for the digital age. The current consumer protection framework does not account for and

does not protect consumers against online-specific practices. Consumer protection issues such as privacy, product safety, competition and redress mechanisms, now arise in a broader context and straddle both geographical (cross-provincial/territorial and international) and substantive borders. federal, provincial and territorial consumer protection legislation requires significant reform to bring it up to date with the issues arising in the digital society.

A professional research firm, Prairie Research Associates (PRA) was contracted to carry out the survey and focus group research. The online panel survey was conducted from September 20 To October 3, 2022 and quotas were used to ensure at least 100 respondents in three key demographic groups: indigenous Canadians; those who identify as having a disability; and those living in northern Canada.

The focus groups were conducted in five provinces, or regions, across Canada. These included, the Atlantic region, Quebec (conducted in French), Ontario, Manitoba, and the Northern region of Canada with participants from Yukon, Northwest Territories, and Nunavut. To qualify for focus group participation, individuals had to be 18 years or older, use at least one online service or website weekly, and have a computer camera and microphone.

The panel survey key findings suggested that concern among Canadians is high with respect to the collection, use and storage of personal data by digital companies. Further, one-third of survey respondents, across all demographic categories, were reportedly very concerned about their personal data. Support for government interventions was also high. In addition, awareness of data collection, use and storage was generally high, but understanding of data use and storage was low. Finally, the results suggested that younger users may be more at risk as they are most likely to use digital services, but are least likely to seek out or implement data protections.

Similar to the panel survey respondents, focus group participants shared a high level of concern about their personal information, particularly with financial information such as credit cards or banking information. Few participants took steps to protect their personal data, with some reporting a reduction in the use of online services as a way to limit risk and, thus, reduce concern.

Focus group participants also discussed the impact of the COVID-19 pandemic on their use of online services. Most focus group participants reported higher use of online

services such as, video conferencing, streaming services, social media and online shopping, during the pandemic than before. As well, for most participants, the use of streaming services and social media remains high. For older participants, the use of social media started, or increased in regularity, during the pandemic but now remains high. The use of video conferencing was high during the pandemic, with it being more useful than messaging apps for group gatherings of friends and family. Its use remains high, with most participants using it for work situations. Online shopping increased during the pandemic, but has returned to pre-pandemic levels. Grocery delivery was particularly beneficial during the pandemic because it helped limit exposure to crowds.

Finally, focus group participants provided suggestions for improving personal security on digital platforms including, using opt-into rather than opt-out-of data collection measures and providing clear, easy to read, terms and conditions. Most participants did not read terms and conditions of use, some commenting they only skimmed them for pertinent information.

The key interviews were held virtually, taking approximately 30 minutes to one hour to complete. Interviewees were provided with the interview script prior to the interview. The interviewees represented a wide breadth of key policy and advocacy communities including, academia, business, consumer, disability, Indigenous, law and limited income. The interviewees also included research subject matter experts.

Key messages identified in the interview data included, consumer awareness of data collection practices and data use is low, digital media literacy and algorithmic literacy are integral to understanding and mitigating privacy risks, and the lack of meaningful and clear consent with respect to privacy policies and agreements, makes it difficult for consumers to fully appreciate the risks. Further, consumer protection legislation is in need of updating and consumer awareness of protections is low. Finally, marginalized and vulnerable consumer groups may be at greater risk to exposure of digital harms.

The results of the literature and legislative reviews, the national panel survey, the five focus groups, and the key interviews, generated a broad array of recommendations for building and protecting access to the digital services marketplace for consumer users. Key themes of the recommendations were identified and included, the need for shared responsibility between industry, government, and consumers, the implementation and regular monitoring and review of legislation, the use of plain language to provide clear,

concise information pertaining to the collection, use and storage of personal data and further investigation of the benefits and risks of data portability.

Within the key themes, specific recommendations included, the use of standard formats or templates, such as those used for food nutrient labelling, the expansion of educational opportunities by government and non-government agencies to improve digital literacy, the appointment of resources to marginalized and vulnerable communities to help support greater participation in the digital marketplace, and the recognition of the diversity of consumer digital users.

A major, overarching theme of the research results and corresponding recommendations was the weakness of consumer rights in the digital services marketplace. More specifically, consumers' lack of understanding about industry data use and storage practices, poorly written agreements, confusing and limited user support mechanisms, regulatory protections that do not keep pace with industry progress, and Canadians' high level of concern about personal data risks, are examples from the research findings that point to this troubling research trend. Consumers have the right to choose, to be heard, to have access to information and education, and the rights to safety and redress. Yet, in this major marketplace where they are dominant users, the research strongly suggests that consumers have few rights. Interestingly, when valuable personal data is used by industry to create content, consumers become reluctant suppliers with few rights and no compensation.

The recommendations that flowed from the research speak to the breadth of concerns raised by respondents and, thus, should ensure that consumer rights have a firm foundation in a fair, just and accessible digital services marketplace. Consumers have responsibilities such as, questioning information sources and data use practices, taking advantage of educational opportunities to improve digital literacy and seeking redress. It is clear however, based on the findings and recommendations, that in an industry heavily dominated by corporate giants, consumers need strong rights to support their responsibilities as digital users.

An additional strong message from the findings and recommendations is the important role that education should play in strengthening consumer rights in the digital marketplace. Governments need to be at the forefront in both providing and supporting educational opportunities for all users, across all demographics. Education

should be presented and available in a variety of formats, should reflect the diversity of Canadian users and should include information about the digital architecture behind user interfaces. With government support, community organizations can provide their members with accessible educational programs that meet their needs. As well, digital literacy should be a regular part of school curricula for students of all ages.

Suggestions for further research include investigating the practices of younger digital users, the unique risks they face, and possible age-targeted protections and education. There may also be value in further investigating service providers' balancing their goal of data collection against the risks posed to their customers and the purposes of data collection, and factors which affect the weighing including privacy protections and obtaining meaningful consent.

While we must recognize the risks associated with online digital use, the growing social and economic benefits have the potential to far outweigh, and perhaps, mitigate those risks. Recognition of consumer rights and responsibilities will ensure a fair and just digital services marketplace that promotes accessibility, supports diversity, and champions democracy. If not all voices are heard, the marketplace is fundamentally flawed and the hoped for benefits will never be fully realized.

Introduction

I'm excited about this rapid technological advancement- I think we all are. There's enormous potential. But we need to make sure that while we are advancing, we should make sure we are protecting personal information and privacy. Protecting privacy is critical to ensuring a free and fair democracy.

Key Informant

I think that we can understand certain sets of risks as risks to consumers and we can understand certain sets of risks to citizens, and they overlap… The biggest risk to consumers from these technologies is the collection of large amounts of data about them without their knowledge or understanding about the use of that data by public or private entities by all sorts of analytics, of prediction and potentially to impact their liberties, their rights, their life outcome, that sort of thing. And I don't think that the risks and benefits are equal. I think that the risks…are extremely high.

Key Informant

it's invisible and it's complicated…I don't think that consumers are aware, for instance, when they are on a company's website, of how many third parties are lurking, watching what they are doing… I think that the use of information that's gathered without consumers realizing it- analyzed, shared, analyzed some more- I think there's no way consumers, I think they may be vaguely aware of it but there's no way they understand it so I think that potential for manipulation that is not in consumers' interests is just really high, and I just don't think that there's adequate protection.

Key Informant

People are clearly worried, but it's hard- they don't feel they have many remedies. First of all, it's hard to know what data organizations are collecting about you, but good luck about that. First of all, people don't realize they have that right. Secondly, it's not standardized. These are the things that make it really hard for people to navigate things like this. This sort of area is one of the most important ones in terms of looking at the future.

Advisory Panel Member

Consumer privacy issues have for some time been a topic of concern, however this topic is now more salient than it has ever been. Rapid advancement of technology has seen an ever-increasing move towards online engagement by consumers. The widespread digitization of both new services (streaming and sharing services) as well as those traditionally offered offline (such digital marketplace and educational platforms) has been greatly accelerated by the COVID-19 pandemic.

Consumers presently find themselves interwoven into in a complex web of technology, artificial intelligence, and online commerce which spans the globe in terms of reach. In this growing digital frontier, consumers are wading through data collection and use practices and trying to navigate ways to protect their privacy in a digital marketplace that has seen the rise of digital giants. In a business model that relies on the collection, analysis, and use of consumer data, consumers are more vulnerable than ever to the influence of the algorithmic architectures created by giant tech companies.

The Manitoba Branch of the Consumers' Association of Canada (CAC Manitoba) has a long history of advocating for consumers and giving voice to consumer concerns in the marketplace. Expanding this advocacy to the digital marketplace - particularly at a time where consumer protection is not keeping pace with the current shift to online engagement - is the impetus for this research.

Project Design

Background

In 2021, CAC Manitoba began to search for the resources necessary to conduct research, from a consumer perspective, into consumer protection and the impacts of data collection practices in the current digital services marketplace. As a result of the COVID-19 pandemic, consumers are now required to engage virtually in most aspects of their life rather than in person or in any other medium, making them even more vulnerable to the collection of data, targeted marketing, political influence, etc. by giant tech companies. The research sought to better understand consumer attitudes towards their rights and protections, and answer a number of questions:

- What are the potential consequences of the information gathered online by companies?
- Do consumers know what related protection is available to them?
- What are some of the potential consequences of not engaging these protections?
- What role did the legislative framework play in consumer protection, and how was that changing in this current environment?
- What can be done to enhance consumer protection? What can be learned from other jurisdictions outside of Canada?

In the spring of 2021, the organization was awarded funding to conduct this research by Innovation, Science and Economic Development Canada's Office of Consumer Affairs, through its Contributions Program.

The project was designed to span roughly 24 months, beginning in May of 2021. It included a number of research tools:

- Creation of an Advisory Committee to ensure the research encompassed a broad spectrum of perspectives
- Review of relevant literature and research
- Review of provincial, federal, and international legislative and regulatory mechanisms relating to consumer privacy and online consumer protection

- Field research focused on understanding the gaps/shortcomings of the current "traditional" consumer protection regime in the digital environment, consumer rights and privacy protections
- Quantitative survey conducted by a contracted professional research firm to determine consumers' knowledge of data privacy and information gathering, as well as their own rights as consumers (1,000 consumers across Canada, including northern and remote populations)
- Online focus groups conducted by a contracted professional research firm in five provinces/territories (including one in French, and one in a northern region) to build upon and deepen the understanding of data gathered through earlier methods
- Key informant interviews including a wide variety of stakeholder or policy community perspectives

The workplan was designed for the research pieces to be iterative, each one informing the next, or to work in tandem with other ongoing aspects. For example, themes from the review of literature informed the development of panel survey and focus group questions, and the results from all three informed the key informant interviews. The field research and regulatory framework reviews were companion pieces, working in tandem. All aspects worked together to inform the final recommendations.

The literature review was conducted in 2022. Later that fall, a panel survey of 1,000 Canadian consumers was conducted. The focus groups were conducted in late 2022 and early 2023. The legislative review was completed in spring of 2023, and the key interview recruitment and meetings were ongoing from fall of 2022 to early 2023.

In the past, engagement sessions such as workshops and surveys would have been conducted in person. The reality of an increasingly digital post-pandemic world, however, is that such sessions are increasingly being conducted online. This advantageously created opportunities for engagement with panel participants, and focus groups in various regions of Canada, including northern and rural communities, as well as key informant interviews with stakeholders across Canada and beyond.

About this report

Many of the research tools were contracted, by CAC Manitoba, to academics, external researchers, and consultants working in related or complimentary fields. The following sections of this document will review each individual aspect of the research. In some cases, the contractor report is included in the main body of this document. In some cases, excerpts or summaries of the contractor reports are included in the main body, and in those cases the full report is appended.

The final sections will be devoted to a discussion of overall project results, leading to CAC Manitoba's recommendations.

Advisory Committee

Purpose and Participation

An important part of guiding this project was the assembly of an Advisory Committee. This group was intended to be diverse, and included representation from business, academia, government, and community organizations. The role of this group was to provide insights and feedback on various research pieces so that the research included the widest possible spectrum of perspectives on this issue.

Participants were promised anonymity so that they could advise CAC Manitoba freely, without concern for repercussions. The Committee met virtually twice over the two-year project period, and offered insight and feedback numerous times by e-mail during that time period. Consultant Wendy Nur became the liaison between the Advisory Committee and CAC Manitoba.

We are grateful to our Advisory Committee for sharing their time, experience, and expertise to help guide this research. Thank you.

Review of Literature

The Public Interest Law Centre was retained to conduct a literature review to identify:

1. The risks and vulnerabilities to which consumers are exposed when participating in digital services marketplaces;
2. The extent to which consumers are aware of their vulnerability when participating in digital services marketplaces;
3. In the form of a high-level summary, the various protections, regulatory or otherwise, which are in place or available to consumers to respond to the risks identified under Objective 1; and
4. The extent to which consumers avail themselves of these protections or otherwise take steps to respond to perceived risk and vulnerability.

The purpose of this literature review is to provide CAC Manitoba with an operational understanding of the issue it intends to learn more about through this project for the purposes of informing future project phases, including the development of survey questions and scripts for focus groups and key stakeholder interviews.

The literature confirms that consumers' reliance on online services worldwide is continuing to grow. Simultaneously, consumers are exposing themselves to significant risks through their participation in the online marketplace, and are frequently doing so without the benefit of an informed understanding of the nature or extent of the risk, or of the value of the personal data which they may be giving away.

Consumers' abilities to adequately protect themselves in the digital services marketplace are significantly impaired by service providers' failures to provide adequate information about their data collection and use practices, their failure to provide consumers with meaningful opportunities to protect their personal data without sacrificing access to the marketplace, and their failure to permit consumers to exercise meaningful control over personal data that has been collected.

Despite the presence of a selection of promising regulatory solution, consumers' participation in the digital services marketplace is marked by both opportunity and significant risk.

The full *Review of Literature* can be found in Appendix A.

Key Informant Interviews

Introduction

This summary of the key interview findings focuses on the ideas and themes which arose in the key interview data. Given that CAC Manitoba represents the consumer interest in, the demand side of the marketplace, we made efforts to speak with representatives of stakeholder organizations with a view to broaden the perspective of this research and to capture important pieces of information, issues, or concerns that could impact the results of the research. This summary describes the methodology informing the key interviews and key themes arising from the qualitative data. Included as well are several recommendations as so eloquently stated by the key interviewees themselves.

Methods

Policy Community Perspectives

Ten key interviews were conducted with representatives of stakeholder organizations in order to capture a variety of perspective.[1] We spoke with:

- Representatives of policy communities/advocacy and interest groups (a representative from an organization representing low-income consumers; a representative from an organization advocating for digital and media literacy for Canadians and youth in particular; a representative of a consumer advocacy organization)
- A representative of a government department
- A Representative of an Indigenous organization

[1] As outlined in the project application, stakeholders include but are not limited to government, industry, business, academics/researchers, student, organizations representing vulnerable consumer groups and Indigenous consumers. The advisory panel, the research team, and interviewees themselves were consulted in order to include as many stakeholder perspectives as possible. We additionally reached out to educators, representatives of Indigenous groups representing, seniors, youth, and technology, however were constrained by their interest or ability to participate. Efforts were also made to speak with interviewees beyond Canadian borders. We were able to meet with an interviewee who worked for an organization located in the United States.

- A representative of a business offering social network and digital media education, specializing in accessible digital architecture
- Subject matter experts (an academic; a representatives of an umbrella organization representing Canadian businesses; a member of an association which works to connect and empower the tech community; a representative of an organization with expertise related to digital privacy laws)[2]

Interview Questions

An iterative approach was used to generate interview questions. As themes arose from the initial pieces of research-mainly the literature review, the national online panel survey, and the national virtual focus groups- these were noted and they informed the interview questions.[3]

Some of the key questions were:

- What are some of the benefits/risks for consumers in today's digital marketplace?
- How would you rate the level of consumer awareness about these risks ?
- What are some protections currently available to consumers?
- In your opinion, do you think consumers are aware of these options and are they implementing them?
- Are there regulatory protections available in other regions that you think should be in place in Canada (policy recommendations)?
- The interview questions were shared with the research team for review and feedback. Members of the advisory panel provided valuable guidance to the research team, and their input helped to shape the research process.

[2] A more detailed table correlating interviewee codes to policy community perspectives is included in Appendix 6.2 of the Key Interview Report

[3] The complete set of interview questions is appended to the key interview report (Appendix 6.1).

Interviewee Recruitment

Potential interviewees were identified by members of the research team and approached regarding potential interviews.[4] Efforts were made to contact individuals both across Canada and beyond our borders. A total of ten interviews were conducted, nine with individuals from both Eastern and Western Canada, and one interview with an interviewee in the United States. Two interviewees were recruited using the snowball method.[5]

Interviews

The interviews were approximately thirty to sixty minutes in length. Interviewees were promised both confidentiality with regard to their participation and were provided written copies of the interview questions in advance. Due to the constrictions incurred by the pandemic, all interviews were conducted virtually (Zoom/Microsoft Teams). Informed and ongoing consent was obtained verbally and practiced for each interview and recordings were made (with consent) for later reference.

Approach to Data Analysis

The goal of the key interviews was to speak with stakeholders who represented a wide variety of perspectives, the approach to data analysis was similar, seeking to capture all of the potential risks to consumers noted by interviewees, and to identify potential gaps and policy recommendations that arose either in discussions with interviewees.

Due to the diversity of perspectives and limited number of interviews, an intuitive approach was applied to the qualitative data analysis. Underlying the analysis was the set of primary research questions:

---

[4] The assumption of CAC Manitoba in identifying stakeholder groups upon the writing of the project application, as well as during the recruiting process, was that key interviewees' responses to questions would be reflect the views of their organizations, and therefore the demographics of the key interviewees was not of primary interest, but rather those on whose behalf their respective organizations advocated .

[5] Interviewees were asked at the end of the interview, "Who else should we talk to." Efforts were made to recruit suggested policy community advocates, and in one instance, a colleague was directly referred upon the suggestion of the interviewee.

- What are the potential consequences of the information gathered online by companies;
- Do consumers know what related protection is available to them?; and
- What are the potential consequences of not engaging these protections?

Key Themes Arising in the Results

All interviewees agree that online engagement of all kinds has increased during or after the pandemic, pointing to a trend towards an increasingly digital marketplace which has been accelerated by the pandemic. While most interviewees expressed that the benefits for consumers generally outweighed the risks, they expressed concern about the potential consequences of information gathered online by companies. Key interviewees identified several potentially negative consequences for consumers in terms of the information gathered online by companies- not only about the types of consumer information that is collected while transacting in the digital marketplace, but also the about the amount of data collected and the risks posed to consumers by the collection of these data. A particular concern underscoring the data is one that most interviewees raised- consumers are not able to fully calculate the risks involved, pointing to a gap in consumer knowledge data collection practices and data use.

The following key themes emerged as most salient:

1. Consumer awareness of data collection practices and data use is low.
2. Digital media literacy and algorithmic literacy are key factors in begin able both to understand and to mitigate privacy risks.
3. There is a lack of meaningful consent with regard to privacy agreements. Privacy policies are generally unclear, being over-long and written in "legalize", rendering them difficult to read and understand. Consumers often do not read or understand what they are consenting to and therefore cannot fully appreciate the risks.
4. Consumer protection legislation is in need up updating, and consumer awareness of current protections is low.
5. Marginalized consumer groups are more vulnerable, and therefore at increased risk in the digital marketplace.

Consumer Education, Digital Media & Algorithmic Literacy are Needed

One concern shared among interviewees was that despite the potential risks to consumers with respect to the information gathered online by companies, consumer awareness of this risk remains low.

> *People don't understand that they are the commodity, their attention is the commodity, (P6)*
>
> *We don't have that experience with personal information and data collection in general. We don't understand the cost, we don't understand the rights that we are giving up, we don't understand that use can change over time, we don't understand the impact of even relatively benign or ostensibly benign practices such as anonymization or de-identification or aggregation of data. We don't understand as individuals how that can come back to impact us at all, and so it gets very difficult to say that it's a fair transaction or a just transaction or that it's unobjectionable. (P1)*
>
> *Because it's invisible and it's complicated…I don't think that consumers are aware, for instance, when they are on a company's website, of how many third parties are lurking, watching what they are doing- some of which are associated with that website but some of which are not! … I think that the use of information that's gathered without consumers realizing it- analyzed, shared, analyzed some more- I think there's no way consumers, I think they may be vaguely aware of it but there's no way they understand it so I think that potential for manipulation that is not in consumers' interests is just really high, and I just don't think that there's adequate protection.* (P7)

In particular, media literacy and algorithmic literacy are low. Consumers do not have a comprehensive understanding of data gathering and data use practices in the digital marketplace, and therefore are not able to fully appreciate the risks. Consumer education is one potential response to address gaps in consumer awareness and knowledge.

> *Another huge thing as a lack of algorithmic literacy on the part of many, many users online. And that's important because you know we may be signing up for an app because we are using the app for fitness or social connection, but the ways in which our online engagements are worked and the ways in which information is*

shared across platforms, the ways in which our data is being used to train algorithms that then in some ways feed us certain forms of other information or potential opportunities, then that's really - I think that's where a lot of problems now lie. And again, on the whole we don't have a lot of supports that for folks to help them understand what algorithms are, how they are working how is artificial intelligence now becoming really ingrained in these processes of scraping, collecting, and utilizing data. (P3)

I don't think we are necessarily aware how that information is being used. I think we give our approval away with that one "I agree". Absolutely, I think that information is used to sell us things, that information is sold to other organizations or companies to sell us things or to know about us, you know, everything from how we are going to vote potentially and what our , you know, if we live in a particular neighbourhood or we have a particular income level or we like certain things. You know, all the algorithms that put that together and what that could actually mean. I think it gives us less freedom, and so I think that's very concerning when it comes to democracy. (P6)

Meaningful Consent is Key

Exacerbating the issue of the consumer knowledge gap in terms of information gathering practices and the use of this information online is the issue of meaningful consent. While there is value in incorporating digital media and algorithmic literacy into educational models at all levels, a pivotal way to address the current consumer knowledge gap in terms of information-gathering and information-use practices is a via a more meaningful consent process. Consumers would be more apt to read consent policies if they were easier to understand. A plainer, clearer, more transparent, consistent, standardized (across Canada), and accessible (for those with assistive technologies) consent format with multiple options for consent would serve to educate, inform, and empower Canadian citizens to make a more informed choice when providing consent in the digital marketplace.

it's about the meaningful consent to the use of that data, which I don't think on the whole is something that users have an awareness of or the capacity to really give given the current ways in which privacy consent is collected. So to me, it's less

about the forms of data collected and more about the way it is collected- the lack of meaningful consent, the way in which privacy policy and terms of service are filled with legal jargon and take an advanced law degree and four days to comprehensively understand for an adult- let alone a child. (P3)

I don't think we are necessarily aware how that information is being used. I think we give our approval away with that one "I agree". Absolutely, I think that information is used to sell us things, that information is sold to other organizations or companies to sell us things or to know about us, you know, everything from how we are going to vote potentially and what our, you know, if we live in a particular neighbourhood or we have a particular income level or we like certain things. You know, all the algorithms that put that together and what that could actually mean. I think it gives us less freedom, and so I think that's very concerning when it comes to democracy. (P10)

(Consumers) don't read them. They don't understand them, and I would say this is not the fault of consumers… These conditions are written to be obfuscatory. They are written to not be understood. They are written in such a way that even if you think they say one thing, there are enough legal caveats to allow them to do whatever they want. So no, in terms of consent regime around digital technology is completely broken. (P9)

Consumer Protection Legislation Needs to be Updated

Finally, consumer protection legislation is not keeping pace with the risks to consumers in the digital marketplace and the awareness of consumers and tools to avail themselves of current protections is low. The result is that consumers who are not aware of potential risks nor of the current protections often fail to (or simply cannot) avail themselves of appropriate protections. Care must be exercised however that the burden for consumer privacy protection does not fall too heavily on consumers themselves. An over-emphasis on consumer education at best falls short of the goal of consumer protection, and at worst, ignores the how the online architectures shape both consumer experience and privacy, and how legislation plays a critical role in regulating these structures.

You know, we all do government and consumer organizations, we all offer information to consumers about how to do some of the things that they are likely wanting to do and how to protect themselves and their kids and um, it puts a tremendous burden on people to protect themselves, and despite all of the tools that are out there, it's still a lot to ask people to do. (P7)

Yeah, it's very challenging…you're so imbricated, you're so caught in not just your phone but other people's phones, you know…It's like, at a consumer level, individual level protections, it's a bit like climate change-it's a bit like greenwashing. It's not a bad thing to try and protect your data and have some security. You obviously have your own personal security around data, that's helpful at the level of individual data breaches or hacks, but when it comes up as kind of broader or societal-level threat of your data being used, collected, transmitted, and analyzed. There's almost nothing you can do about it. (P9)

Facilitating consumer awareness of and access to current regulatory protections and mechanisms would be helpful, as well. This is especially important as consumer legislation for Canadians is not keeping up with current rapid technological advancements. Consumers either are not aware of protections and resources for redress or assume that they are protected in specific ways online when they, in fact, are not.

I think that people sometimes think there are protections that don't exist, frankly, because it just would make sense. (P7)

In terms of the ability to actually act on these problems, and an understanding g of what policy or activism will address these problems, I think it's a zero…I think people are resigned; they are confused. So I think they are worried but they can do nothing about it. These are forces that are well, not just outside their control, they seem like forces that are out of the control of politicians as well, and regulators. And so, I think that's a big and difficult paradox. (P9)

Marginalized Groups are More Vulnerable

Consumer privacy risks in the digital marketplace are compounded for vulnerable group such as children, seniors, or other marginalized communities, and AI (Artificial

Intelligence), algorithms, and online architectures intersect to compound these risks. Those already experiencing marginalization due to socio-structural barriers are at risk of further marginalization and/or exclusion due to potential negative impacts of algorithms which manage information and access in the digital marketplace.

> *Generally, digital media systems amplify already existing asymmetries of power in society. So the people who already had power back in the day have more power. In some ways that, to me, means that groups already at risk- women, minorities, etc., will be even more at risk. (P9)*

> *I know we talked about the access issue, but if we look at folks in vulnerable populations or at-risk populations- that's a better way to put it- because our communities have been made deliberately vulnerable by the systems and structures that are in place, but absolutely Indigenous communities would be more vulnerable, for sure. …If you are a First Nations child in Manitoba, you have a better chance of growing up in poverty than graduating from high school. You have a 53 percent chance of growing up in poverty. Poverty makes people more vulnerable. … If you don't have housing, that creates vulnerabilities….for sure, I would imagine it would be the same in other racialized communities in Canada, for persons with disabilities, etc. because poverty is the great equalizer in that it makes everybody in that low income category…more vulnerable. (P10)*

> *As always, the equality angles are important because I think we do see a disparate impact or a different impact on some communities, so everything that we've been talking about. It's very different when you understand how these technologies and the consents that you give can be used against you if you're a women in a situation of domestic violence, when you are fleeing and looking for safety. All of a sudden, all of those consents and all of those issues become much more personally significant. That's a perspective that often is ignored. (P2)*

These compounded risks therefore require an intersectional approach to consumer education and awareness on all topics related to consumer privacy protection in the digital marketplace, including informing consumers about regulatory protections. There are many ways these vulnerabilities can overlap, and while this research cannot address all of these possibilities, this report proposes that an intersectional lens will be

beneficial in identifying those who may be and greater risk and therefore in need of additional supports.

Conclusion

In conclusion, the risks to consumer privacy in connection with information gathered online by companies are considerable, and are compounded by several factors. Firstly, consumer awareness of these potential risks is low. There is a knowledge gap concerning data gathering practices and data use and this gap in knowledge results in an increased risk of negative impacts to consumers. Secondly, privacy policies are not consistently transparent; they are difficult to read and understand, and provide few options for consumers, resulting in the lack of meaningful consent. Thirdly, consumer awareness of protections (and by extension consumer engagement of these protections) is limited. Consumers are aware of some personal approaches to protecting their privacy, but are challenged in activating these. Fourthly, regarding regulatory protections available, consumers have a limited knowledge of what these are, much less an understanding of how to avail themselves of these protections. Finally, certain groups are more at risk than others. Those already experiencing marginalization due to socio-structural barriers are at risk of further marginalization and/or exclusion due to potential negative impacts of algorithms which manage information and access in the digital marketplace.

Recommendations

The following recommendations arise from the key informant interview data:

1. Ongoing consumer education on the topics digital media and algorithmic literacy, information gathering and use, consent, and regulatory protections will help to mitigate risks to consumer privacy.
2. Care must be taken to ensure that consumers do not bear an unfair share of the burden for their own privacy protections.
3. Consumer privacy protection legislation needs to be updated to ensure that privacy policies are clear, and that consumers can easily access, read, and understand what information will be collected and how this information will be used.

4. Tools and resources for consumer privacy protection and redress should be made easily available to consumers.
5. Canadian policy makers would benefit from looking at jurisdictions beyond Canada who are actively incorporating these concepts into their consumer privacy legislation.

The full *Key Informant Interview Report* is available in Appendix B .

Digital Technology Survey

A national survey was conducted with a national panel of consumers across Canada. A professional research firm, Prairie Research Associates (PRA), was contracted to conduct the sessions. The script for the sessions was developed by the research firm with the advice and input of the project research team.

Methods

PRA conducted an online survey using a national panel[6], gathering responses from 1,000 respondents from September 20 to October 3, 2022. All results in this report are presented out of the total n-size of 1,000 unless otherwise stated. Quotas were used to ensure at least 100 respondents in three key demographic groups – Indigenous Canadians, those who identify as having a disability, and those living in northern Canada.

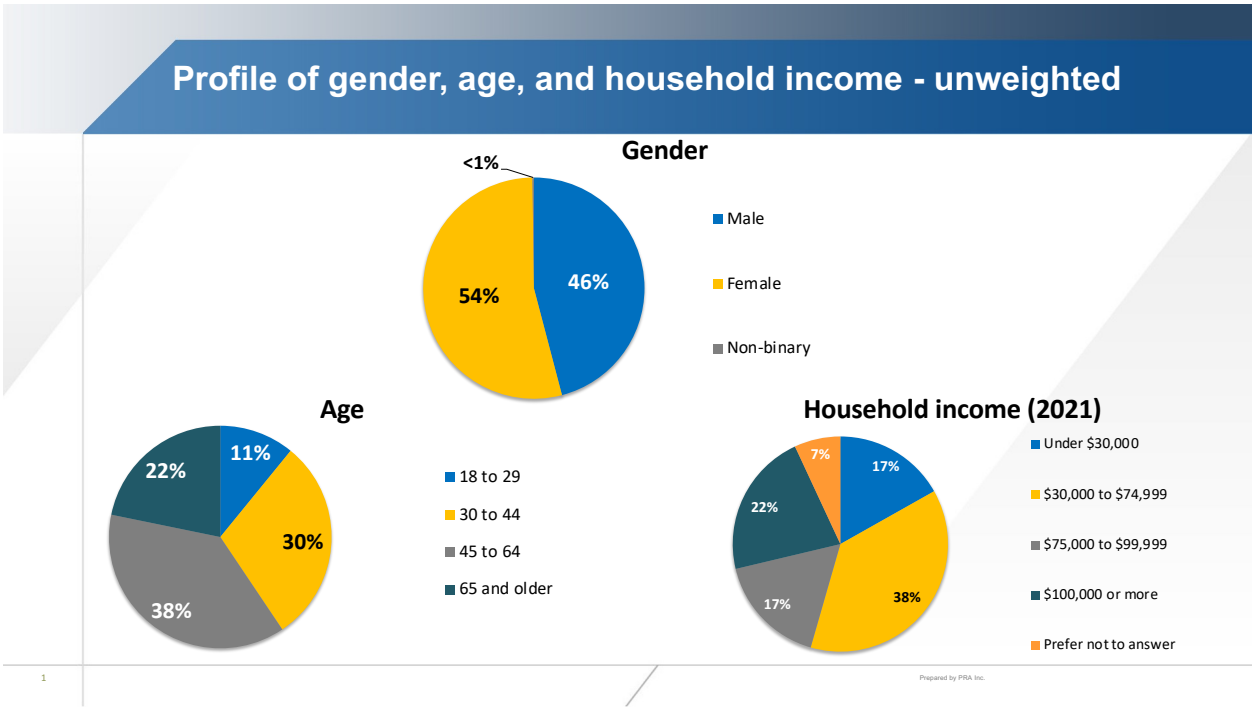
A similar survey with a random sample of 1,000 would result in an error rate of ± 3.1% (19 times out of 20). For this study, the sample is weighted to the general population data for Canada to correct for differences in age, gender, region, and income. Proportions in this report are weighted unless otherwise stated. A demographic profile of respondents can be found in Appendix A. Data in charts may not always sum to 100% due to rounding.

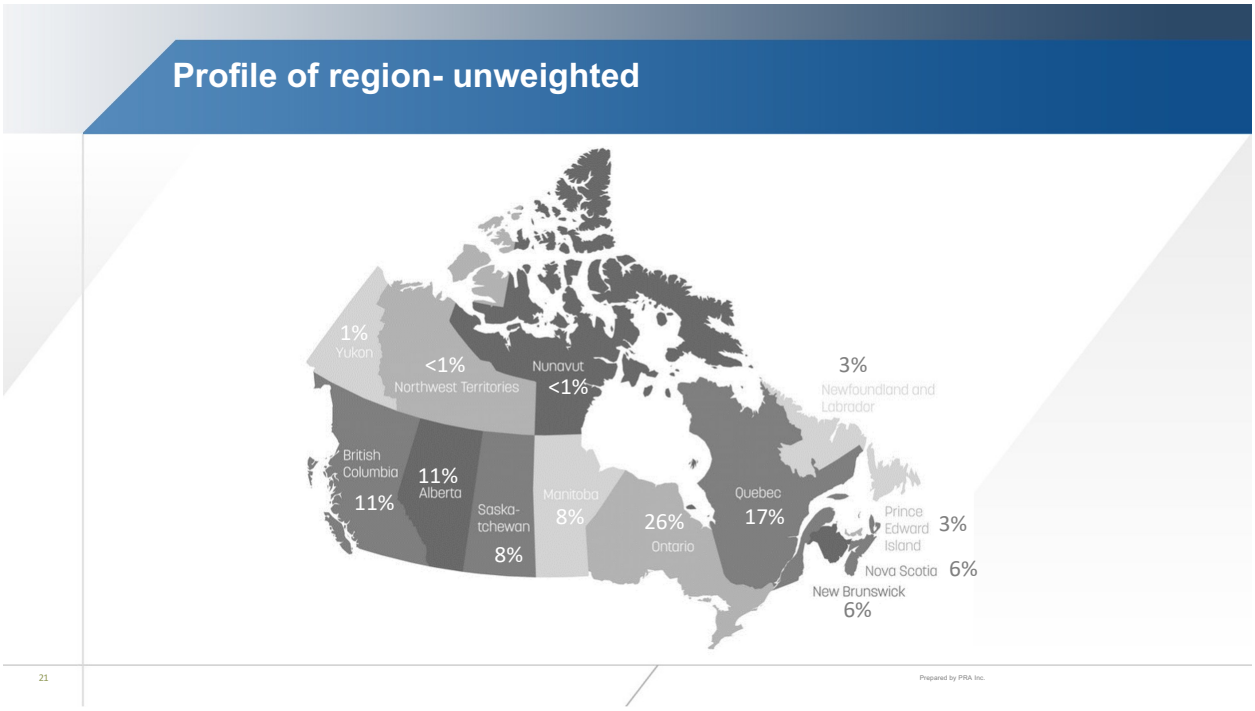
Results in this report were analyzed to determine statistical differences by age groups; gender; region (Western, Ontario, Québec, Atlantic); household income; Indigenous respondents; those who identify as having a disability; those who speak English as an additional language; those with children under 18 years of age; and respondents living in northern Canada.

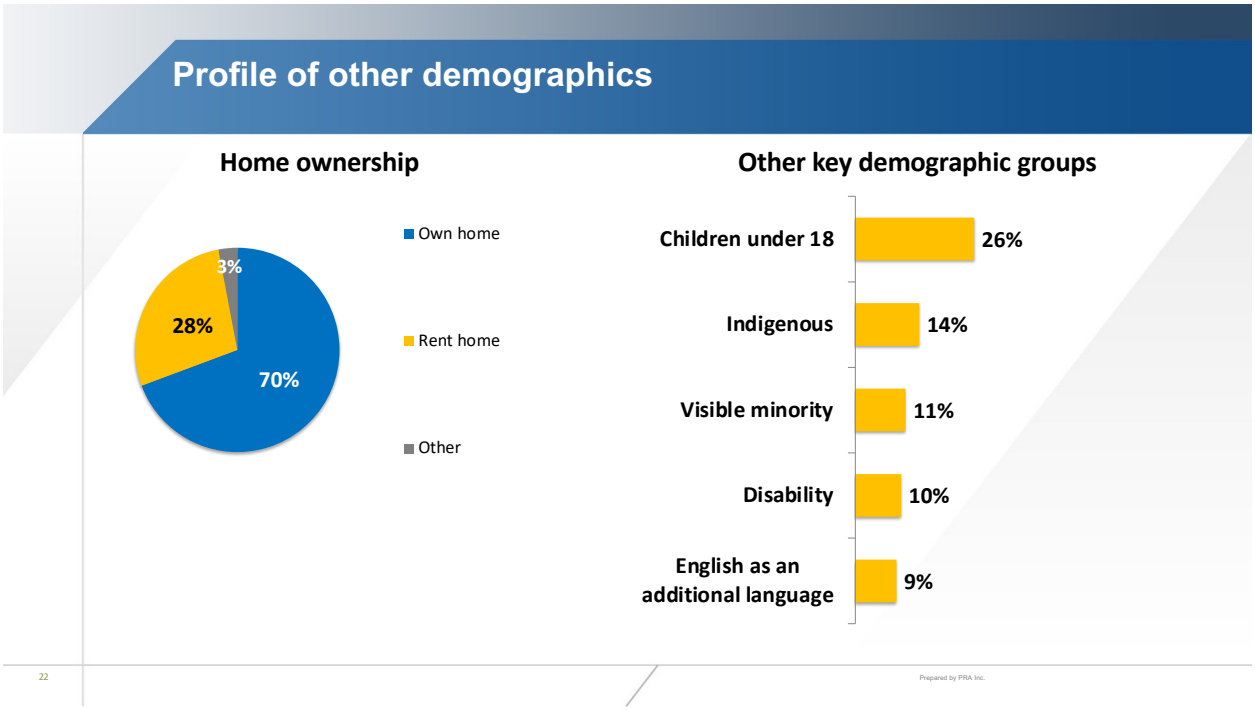
[6] Figures illustrating the various demographic information of respondents and a map of the region sampled can be found in the full report, appended to this report as Appendix D

Demographics

The following slides represent the demographic profile of respondents







Results

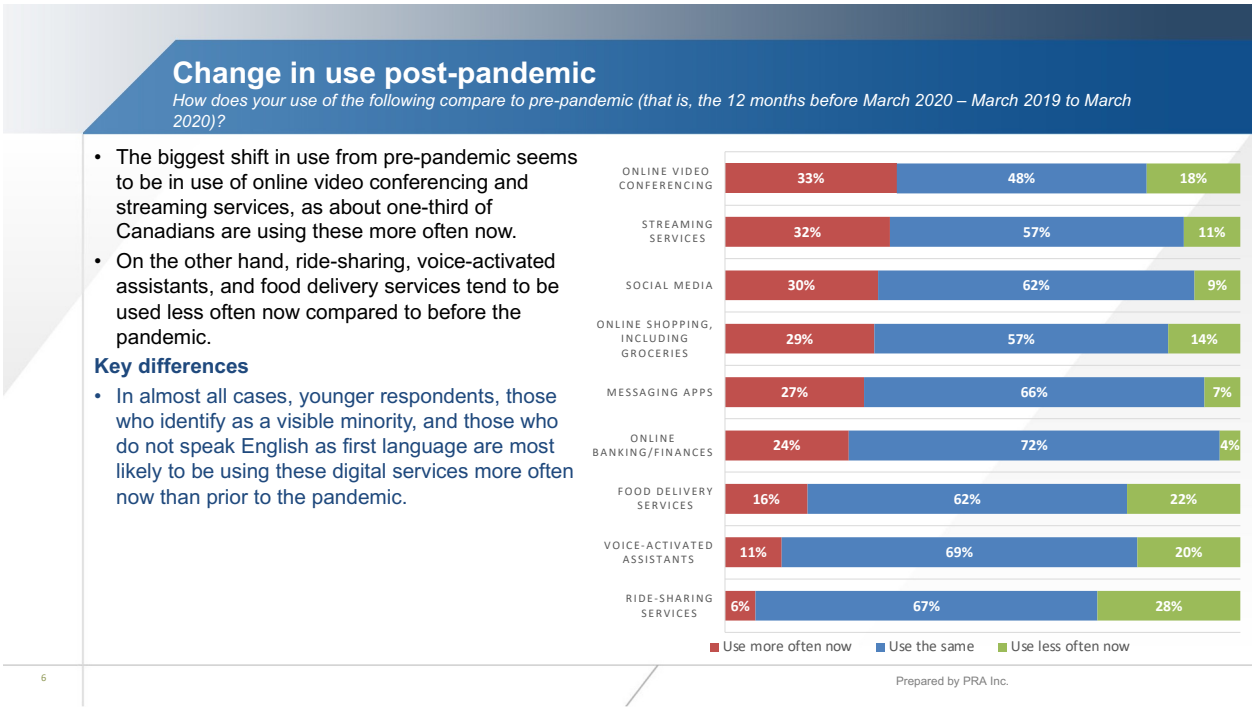
Key Findings

PRA determined several key findings from the survey, support for which arose in a number of the individual questions. These included:

- Concern about use of personal information is high. Almost 3 in 4 respondents are at least somewhat concerned about digital companies using, collecting, and storing their information, with one third being very concerned. This concern is high amongst all demographic groups.
- Awareness is high, but knowledge is lower. Although 9 in 10 respondents are aware that digital companies use their information in some way, substantially fewer are well informed about how digital companies use it.
- Strong support for changes. There is very strong support for changes to better protect digital users, and that support is strong across all demographic groups.
- Younger people may be more at risk. Younger respondents tend to be the heaviest digital users, yet appear to be least likely to take steps to protect their personal information.

Looking at the Details

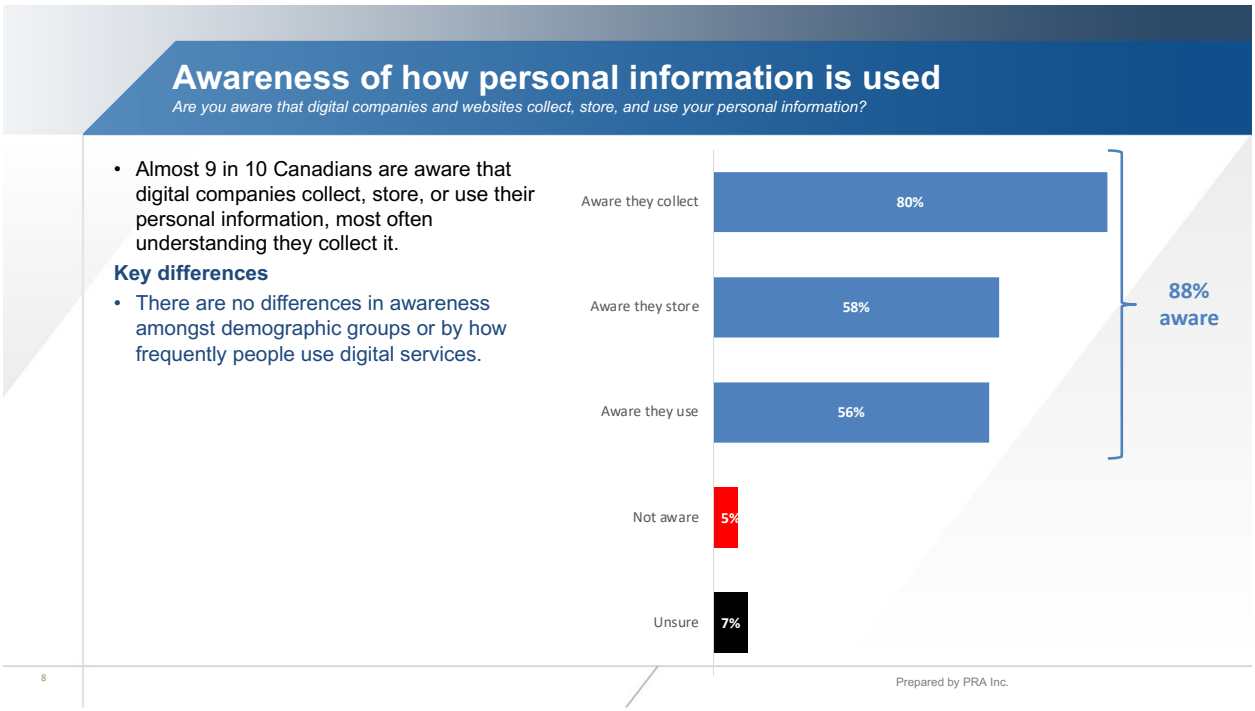
Responses to several of the questions stand out in answer to our initial research questions, or in support of conclusions drawn using other research tools in this project.



Respondents were asked to compare their digital use now to their digital use before the pandemic. The biggest shift in use from pre-pandemic seems to be in use of online video conferencing and streaming services, with about one-third of Canadians using these more often now. More consumers are also engaging on social media platforms and shopping online.

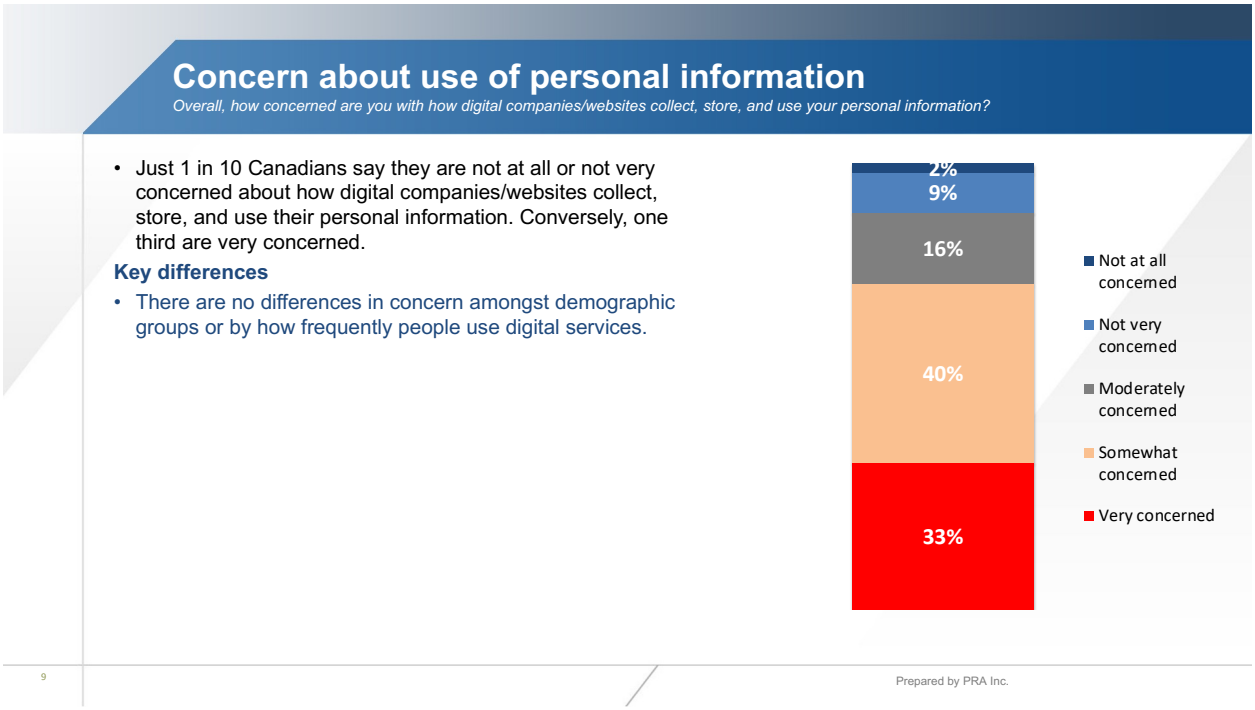
There were some key differences between groups of consumers identified by the research firm:

- In almost all cases, younger respondents, those who identify as a visible minority, and those who do not speak English as first language are most likely to be using these digital services more often now than prior to the pandemic.



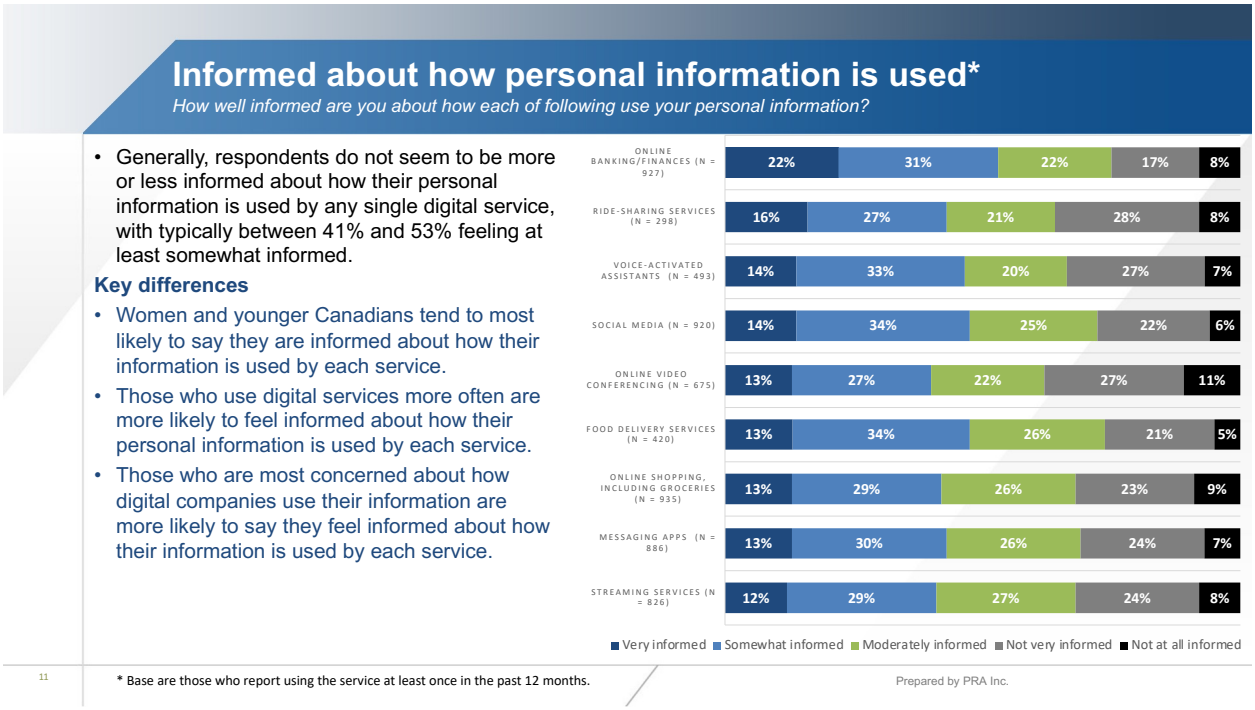
Respondents were asked whether they are aware that digital companies collect, store, or use their personal information, and almost 9 in 10 Canadians responded that they are aware of this.

There are no differences in awareness amongst demographic groups.



Just 1 in 10 Canadians say they are not at all or not very concerned about how digital companies/websites collect, store, and use their personal information. Conversely, one third are very concerned.

There are no differences in concern amongst demographic groups or by how frequently people use digital services.

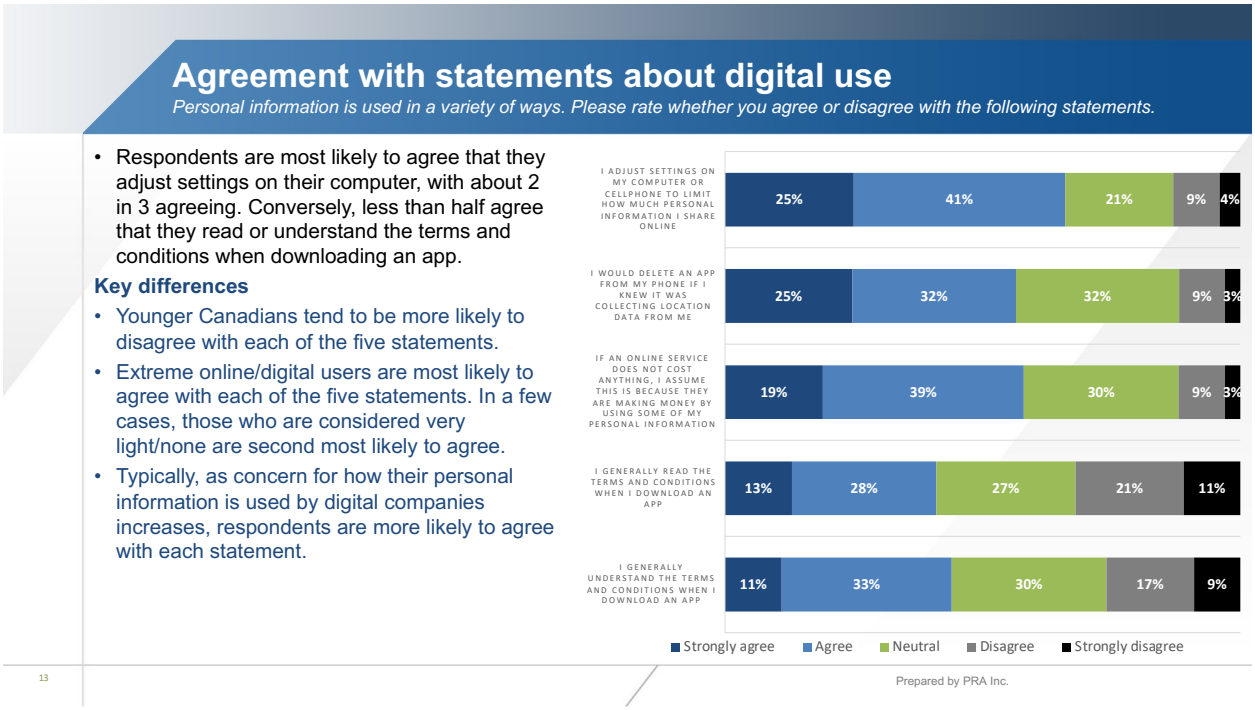


Respondents were asked how informed they are about the use of personal information, with 41% and 53% feeling at least somewhat informed. Interestingly, being more informed about the use of information is generally correlated with a higher level of concern. This is interesting, as the data from the key interviews note that low concern seems to be connected to a low level of awareness about data collection and data use practices.

Once again, there were some key differences between groups of consumers identified by the research firm:

- Women and younger Canadians tend to most likely to say they are informed about how their information is used by each service.

- Those who use digital services more often are more likely to feel informed about how their personal information is used by each service.
- Those who are most concerned about how digital companies use their information are more likely to say they feel informed about how their information is used by each service.

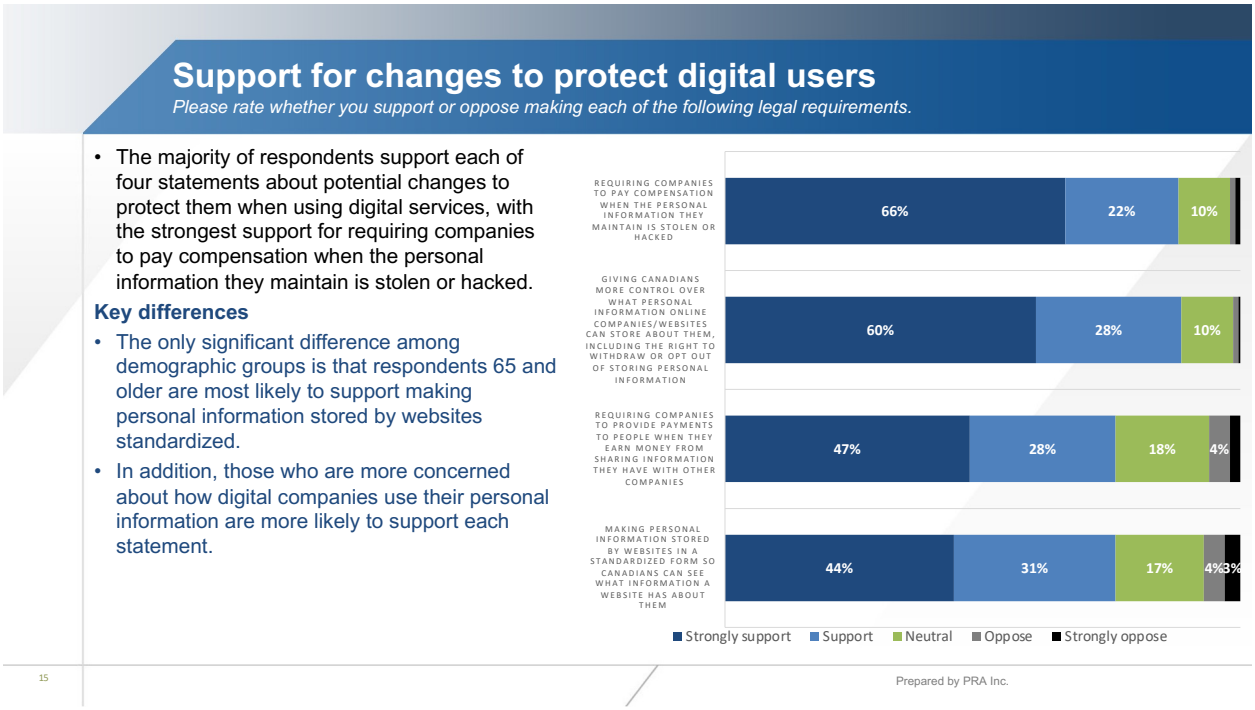


Information is used in a variety of ways. In order to assess their awareness, respondents were asked about whether they agreed or disagree with a series of statements about the use of personal information online. Respondents are most likely to agree that they adjust settings on their computer, with about 2 in 3 agreeing. Conversely, less than half agree that they read or understand the terms and conditions when downloading an app.

Some key differences between groups of consumers identified by the research firm were as follows:

- Younger Canadians tend to be more likely to disagree with each of the five statements.

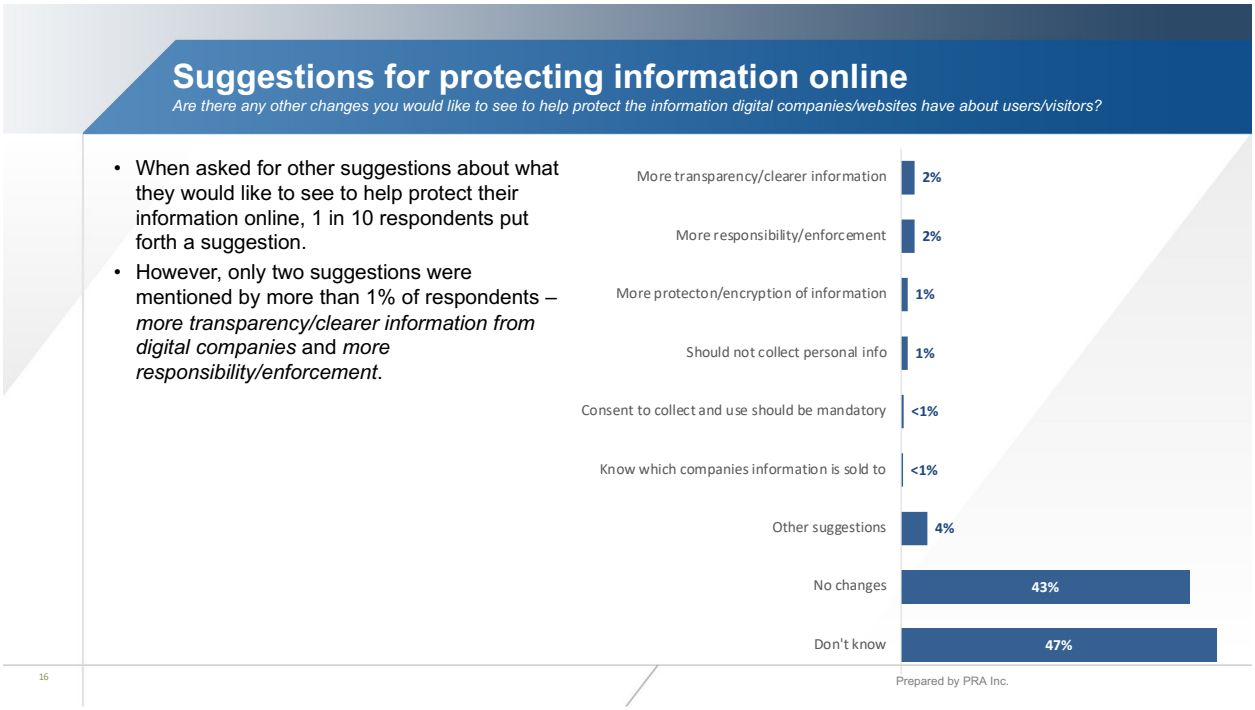
- Extreme online/digital users are most likely to agree with each of the five statements. In a few cases, those who are considered very light/none are second most likely to agree.
- Typically, as concern for how their personal information is used by digital companies increases, respondents are more likely to agree with each statement.



Respondents were asked to rate their support from some proposed legal requirements. The majority of respondents support each of four statements about potential changes to protect them when using digital services, with the strongest support for requiring companies to pay compensation when the personal information they maintain is stolen or hacked.

Key differences between groups of consumers included:

- The only significant difference among demographic groups is that respondents 65 and older are most likely to support making personal information stored by websites standardized.
- In addition, those who are more concerned about how digital companies use their personal information are more likely to support each statement.



Respondents were asked whether there are any other changes they would like to see to help protect the information digital companies/websites have about users/visitors. 1 in 10 respondents put forth a suggestion. However, only two suggestions were mentioned by more than 1% of respondents:

- more transparency/clearer information from digital companies and
- more responsibility/enforcement.

The full Digital Technology Survey Report is found in Appendix C and the question set is found in Appendix D.

Focus Groups

Introduction

Five focus groups were conducted with consumers across Canada (December, 2022 to January 2023). A professional research firm, Prairie Research Associates (PRA), was contracted to conduct the sessions, which took place via video conference. The script for the sessions was developed by the research firm with the advice and input of the project research team.

Methodology

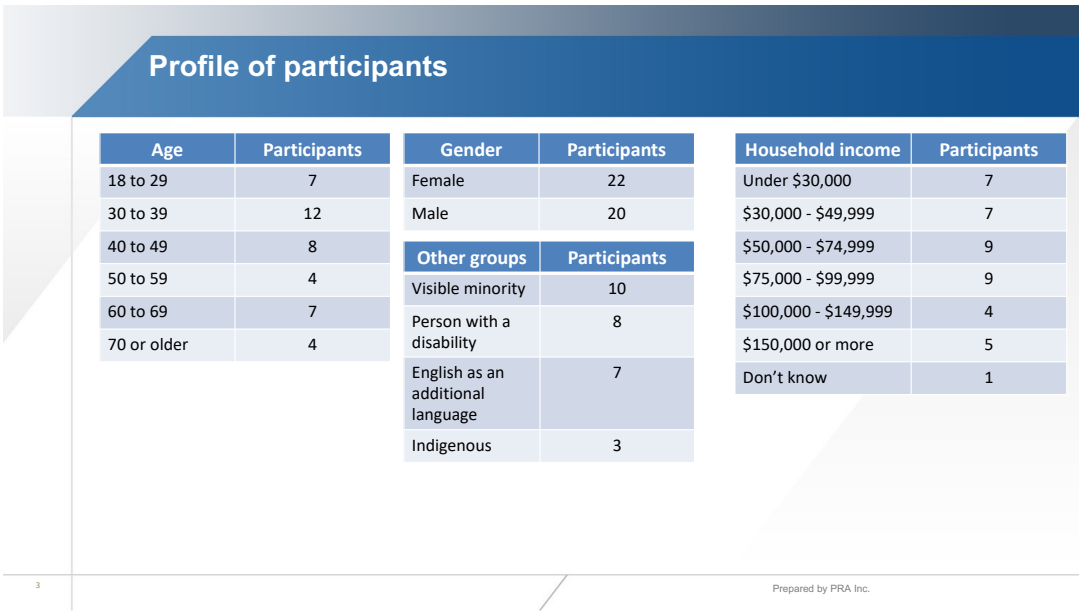
PRA conducted five online focus groups, one with participants in each of the following provinces/regions: Atlantic, Québec (French), Ontario, Manitoba, and northern (Yukon, Northwest Territories, and Nunavut). To qualify for the groups, participants had to be 18 years or older, use at least one online website or service at least weekly, and have equipment (camera and microphone) to be able to participate in the online focus group.

In total, 42 people participated across the five groups, as follows:

- Atlantic – 9 (2 New Brunswick, 3 Newfoundland, 2 Nova Scotia, and 2 Prince Edward Island)
- Manitoba – 8
- Ontario – 9
- Northern – 6
- Québec – 10

Demographics

The slide below represents the demographic profile of respondents.



Profile of participants

Age	Participants
18 to 29	7
30 to 39	12
40 to 49	8
50 to 59	4
60 to 69	7
70 or older	4

Gender	Participants
Female	22
Male	20

Other groups	Participants
Visible minority	10
Person with a disability	8
English as an additional language	7
Indigenous	3

Household income	Participants
Under $30,000	7
$30,000 - $49,999	7
$50,000 - $74,999	9
$75,000 - $99,999	9
$100,000 - $149,999	4
$150,000 or more	5
Don't know	1

3

Prepared by PRA Inc.

Key Results

Overview

This report is broken down into four main topic that were covered in each group:

- the impact of the pandemic on participants' use of digital services
- concerns about how their information is used by online/digital companies
- how participants protect themselves when online
- policy/government changes that may better protect their information

Impact of Pandemic on Use of Digital Services

The pandemic seems to have had considerable impact on participants' digital use, with some being impacted more than others. Due to the pandemic restrictions, consumers had fewer options for social connection and entertainment. This spurred an increase in online engagement.

Respondents reported more frequent use of the following:

- use of streaming services
- engagement on social media platforms
- use of messaging apps

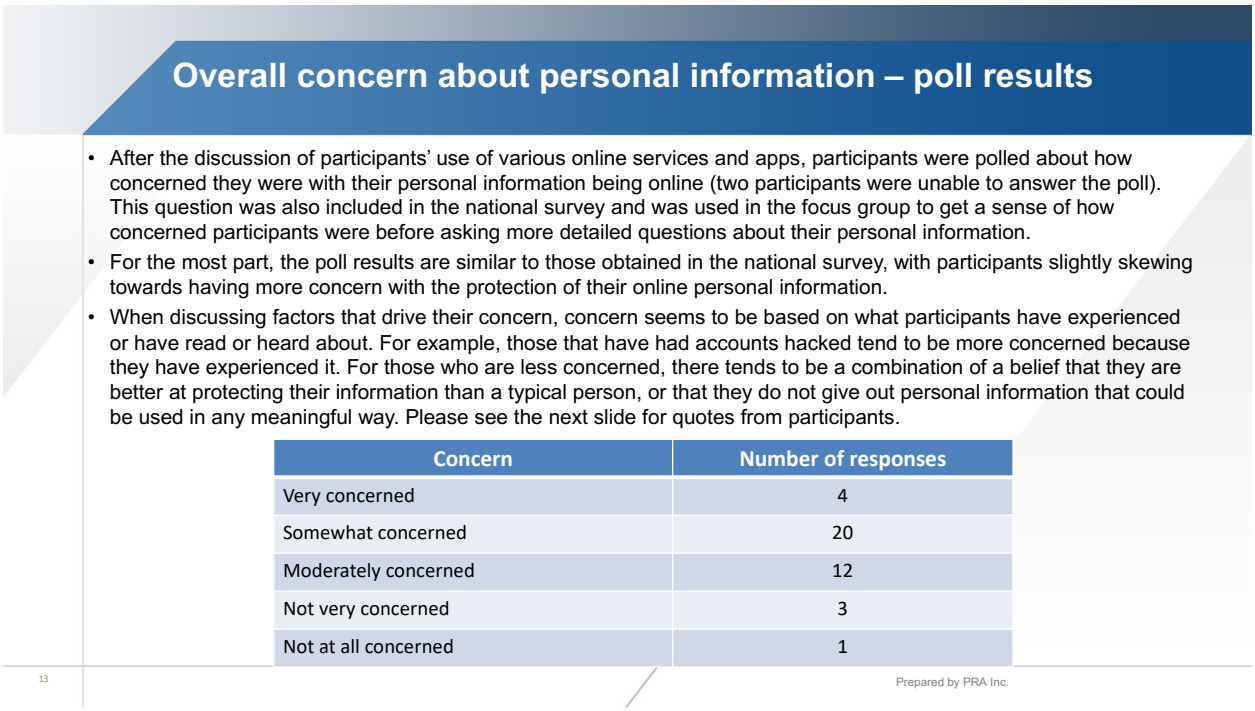
- video conferencing
- online shopping/banking

Because of the pandemic, participants had fewer entertainment and social options available to them. Some say they are watching more TV and movies than prior to pandemic because those behaviours have normalized. Social media use increased for many participants during the pandemic, primarily because of the need to connect or stay connected with people during periods of isolation. Use of messaging apps was often connected to participants' use of social media, since many social media apps also have messaging platforms built in. Therefore, their increased use of social media (both in frequency and variety of use) spilled over into increased use of messaging apps.

Video conferencing use has increased for almost all participants because of the pandemic, as many mentioned they were rarely using or not using these apps at all prior to the pandemic. For the most part, video conferencing was a way to communicate with friends and family for larger groups, and was better than using messaging apps. In addition, many gatherings were converted to video conferencing. Many also continue to use it for work, and have found that its use has not decreased.

Many participants started getting their groceries delivered during the pandemic because it was easier and lowered their risk of exposure to COVID-19. Many have continued to use this service because of its convenience, though less frequently than during the pandemic.

Concerns About the Use of Personal Information



Overall concern about personal information – poll results

- After the discussion of participants' use of various online services and apps, participants were polled about how concerned they were with their personal information being online (two participants were unable to answer the poll). This question was also included in the national survey and was used in the focus group to get a sense of how concerned participants were before asking more detailed questions about their personal information.
- For the most part, the poll results are similar to those obtained in the national survey, with participants slightly skewing towards having more concern with the protection of their online personal information.
- When discussing factors that drive their concern, concern seems to be based on what participants have experienced or have read or heard about. For example, those that have had accounts hacked tend to be more concerned because they have experienced it. For those who are less concerned, there tends to be a combination of a belief that they are better at protecting their information than a typical person, or that they do not give out personal information that could be used in any meaningful way. Please see the next slide for quotes from participants.

Concern	Number of responses
Very concerned	4
Somewhat concerned	20
Moderately concerned	12
Not very concerned	3
Not at all concerned	1

13

Prepared by PRA Inc.

After the discussion of participants' use of various online services and apps, participants were polled about how concerned they were with their personal information being online[7] . This question was also included in the national survey and was used in the focus group to get a sense of how concerned participants were before asking more detailed questions about their personal information. For the most part, the poll results are similar to those obtained in the national survey, with participants slightly skewing towards having more concern with the protection of their online personal information.

When discussing factors that drive their concern, concern seems to be based on what participants have experienced or have read or heard about. For example, those that have had accounts hacked tend to be more concerned because they have experienced it. For those who are less concerned, there tends to be a combination of a belief that they are better at protecting their information than a typical person, or that they do

[7] two participants were unable to answer the poll

not give out personal information that could be used in any meaningful way. The following quotes are a sampling of responses:

> *I am concerned with any personal information, not the companies use themselves because I tend to trust the companies, but I am afraid of leaks. Every now and then I take a look at what class actions are going on. I can see that there are these data leak class action lawsuits. So, I find that concerning because I don't know anything about these other third parties that are receiving information about me.*
>
> *For me I think it is just a little concerning because at least for myself I have no clue what kind of data they are collecting..*
>
> *I almost put 'very concerned' and then I changed it to somewhat because I realized I will do things like specifically when I go to a new website and it asks about cookies I will take the time to go in and not just accept everything. I will actually only accept the minimum of cookies, but then I'll go on some random website. I can understand the hypocrisy that I do in terms of my putting on information so I will be paranoid about one thing and then not necessarily paranoid about the other so that is why I dropped it down a notch.*
>
> *I am careful about what personal information I divulge online so I don't give out anything that I don't want out here, basic principle. I usually don't put my address unless there is a reputable site. I will put my address in something like Amazon because it is fairly reputable.*

Participants expressed concern about the following types of information online:

- financial information
- personal information
- location tracking
- websites visited

Financial information

In terms of concern for their personal information, almost all participants were most concerned about the protection of their financial information, such as credit card and banking information. Participants were most concerned with this information because

if this information is stolen, it is most likely to be used by others and could have a direct, negative impact on their lives.

> *I am mildly concerned about my stored credit card information getting leaked and used fraudulently. I think that is where my concern more so lies.*
>
> *I think if I had to pick the one thing that concerns me the most it would be financial. Like what could make me liable if my bank account got hacked, or my credit card etc. versus if people were to know my location and that is being sold, I can't really do too much about that.*

Personal information

Other aspects, such as their name, phone number, or address, were less concerning than financial information, but still concerning because participants felt that if people were to have this information, they may be able to get access to financial information, and/or this increases the likelihood of identity theft.

> *Social Insurance, banking, possibly my age because seniors are known to be targeted. I don't think my address would be of…well it might be. Possibly my phone number if I start getting harassing phone calls.*

Websites visited

Most participants did not like the idea of apps/websites tracking what other apps/websites they visited, but this was often seen as more of an annoyance or a slight intrusion in terms of what people could do with that information, rather than a major concern.

> *I'm concerned about it because then they start promoting all this stuff to you that you're not even interested in. You might just go on to look at something but then you get 10 emails from them. They've definitely taken your email address and your name so they can say, 'Oh, hi Marg, are you interested in this product?'*
>
> *I find that if you go onto certain websites, you start getting pop ups all the time and I have absolutely no use for that. I don't like other people making the decision,*

'Oh he went to this website so we are going to send you along the information in a related sense.' I find they interfere.

Location tracking

Some participants were unaware that apps on their cellphone or the phone itself may be collecting information related to their location. Regardless, few participants were overly concerned about digital companies having this information on its own, since they did not believe there was much companies could do with it that might harm them directly. However, many said that collecting this information felt intrusive, even if they were not concerned.

There have been some cases like that where the app is tracking your location and it is using that for whatever. I have no idea what it would use that for. I don't really care. I am not going anywhere where I am concerned where somebody knows I am going somewhere right? So, I don't care that someone knows where I am, I care that they are collecting and using data that I haven't consented to providing.

I don't like it at all. It just creeps me out that unless it is necessary and I basically allow it, it is mandatory, for some apps it is mandatory. Some sports betting apps and stuff like that. Without enabling the geo tracker, they are not going to let you on the site so for the mandatory ones that I do want to access but other than that to be honest with you it really disturbs me because I don't feel comfortable being tracked.

Protection of Personal Information Online

Most participants do not take many actions to protect their information online. In fact, the most common way mentioned was by reducing how often they go online or reducing the number of sites or apps they use, which are not forms of protection, but rather just limits exposure. For example, some participants mentioned that they do not post on their social media accounts because they believe that posting is what would increase their exposure.

I don't post very much on Facebook. I watch it to see what my friends are doing because they post a lot, but I rarely post. I think that sort of keeps my privacy where I want it, but I could be wrong."

Otherwise, there was very little consensus about steps that participants consistently take to protect themselves; however, in each group, it was apparent that there was a significant divergence in steps participants take. A few participants would take many steps to protect themselves and seemed to have heightened concern about protecting their information, while others had concerns but took few (if any) steps to protect themselves. Steps participants mentioned to protect themselves included:

- Using complicated passwords
- Using different passwords for each website
- Using two-factor identification (when available)
- Using third-party payment sites/apps rather than providing credit card information (e.g., PayPal, Apple pay)
- Having credit cards that are only used for making online purchases
- Using VPNs when online
- Giving false information when registering to use apps or websites (e.g., incorrect address or birthdate)
- Using different emails for registering on websites/apps that they may not deem reputable

Very rarely did participants mention that they read the terms and conditions for websites or apps. In fact, almost none brought up this behaviour without prompting. When asked directly, almost none of the participants said they read the terms and conditions in any great detail. A few said they may skim the information to see if anything seems concerning to them, but did not mention ever having read something that concerned them.

Like for a lot of apps you do have to create and account and when you create an account you agree to terms and conditions and I can't speak for everybody but I can

speak for myself and say that I have never ever in my life read a single terms and conditions ever, never, ever, ever I don't care what it is, I've never read it.

Some participants mentioned that if they believe the website or app is reputable or well-known, they often just accept the terms and conditions because they assume it is safe and their information is protected.

But if it's a website like Apple or Facebook, I don't really bother to do that because it's kind of like I don't have a choice either way. If it's an app or service that you could easily choose another alternative, then I'll put more effort into it. But with more reputable ones, it's not as much of a concern.

Very few participants mentioned that they take proactive steps to try to protect their information, either on their computers or mobile devices. A few participants mentioned that they do not let apps track them when prompted in their device (primarily Apple devices); however, this seems to be a behaviour associated with the change in Apple's iOS settings that proactively prompts users to indicate if they want the app to track, as participants did not mention doing this manually before the change was made. A few participants say they have gone into the settings on their phone and turned off location services on some apps that they did not think required location services.

I would definitely make adjustments. Like I would, for example the location services thing, how there is the option for 'never,' 'while using,' and 'always using.' Depending on the app, I'll have 'never,' but if it is like McDonalds or something and I'm about to go through the drive through and I'm ordering on my phone, then I'll have it like for 'while using.' So, I definitely do make adjustments based on whatever the app is.

In a few instances, participants say that they allow apps (or certain apps) to track information because it easier than having to manage it every time they use it.

When I install the app I take a look at whether I am going to be using it frequently. If I am, I will give it all the permissions because I can't be bothered to turn it on every time

I am using it, but if I am not, then I am going to turn it off and just keep the app with me until I know I am going to be using it.

When discussing cookies and whether they accept them, behaviours were not consistent, with most participants saying they simply accept them when prompted and others saying they would review and change the settings; however, the primary drivers seem to be a combination of trust in the website and time.

I do see all these things about accepting cookies and stuff but sometimes the websites detail what exactly they are collecting the information for but sometimes they just say necessary cookies or necessary information so they don't elaborate on exactly what they are using it for but because I really want to use the website I just end up clicking accept because I don't have the time to go through all of that.

Potential Policy Changes to Improve Safety Online

When asked for suggestions about what government(s) can do to better protect Canadians' personal information online, participants had few suggestions. Suggestions included:

1. Easier to understand terms of service. In most groups, participants discussed how it is difficult to understand the terms of service associated with using most apps or websites, and they often do not know what they are agreeing to. They would like terms of service to be clearer in terms of the information that is being collected and stored, as well as how it may be used.

   I am assuming that that 75 million paragraph page is telling me everything that they are tracking. I feel like that is something that needs to be transparent and I feel like that is something that, if you are looking for that information to see what these companies are tracking, you'll be able to find it.

   I find with a lot of those terms and conditions, they are so full of legal jargon, you need a law degree to read them right, and people were saying it is pages and pages, so maybe something where the pertinent information, whatever it is that they are trying to store, maybe there is kind of a layman's terms. Something easy

that people can read and understand maybe, as opposed to having everyone read through this huge document that is full of words that I can't spell.

2. Credit monitoring or checks. In one group, a few participants said that there should be a policy that requires companies to provide free credit monitoring when people's information is hacked or stolen from them. This suggestion was raised because a few had received this offer from other organizations in the past, and found it to be something that brought them peace of mind (even if they did not take up the offer).

"We had a privacy breach at Eastern Healthcare and they offered any of their clients free Equifax credit monitoring for two years. I think that's helpful. With that and a credit card of mine that was breached many years ago, I've had credit monitoring in place for a while."

3. Opt-ins rather than opt-outs. In one group, a participant thought that storing personal information or tracking should be something that individuals need to actively opt-into, rather than it being the default and then having to opt-out. Similarly, in another group, it was suggested that people should have the right to indicate that an app or website not store the information that people provided.

I think giving people an easier way to change the cookies or giving them an opt-in instead of an opt-out. They are not automatically that these things are being tracked. You have to opt-in to be tracked instead of opt-out to be tracked.

4. Reducing information required. In one group, participants suggested that apps and websites should be restricted in the amount of information that they can collect. For example, it was suggested that a full birth date should not be allowed to be collected.

5. Although participants struggled to identify suggestions to improve the security of information online, there was fairly strong consensus that governments should be doing more to protect people when online. Primarily, it was ways

for the government to enforce protection laws, but also ways for the public to be able to report and see action when their information has been breached.

There is no place I can inform the authorities for example that this person is a scammer. Of course, they are probably overseas anyway, but there doesn't seem to be a protection system for people doing the scamming, for reporting the bad guys. It is difficult to do.

After being able to put forth suggestions, we discussed four potential policy changes[8] that could be made by the Canadian government to assess participants' reactions:

- Making personal information stored by websites in a standardized form so Canadians can see what information a website has about them
- Requiring companies to provide payments to people when they earn money from sharing information they have with other companies
- Giving Canadians more control over what personal information online companies/websites can store about them, including the right to withdraw or opt out of storing personal information
- Requiring companies to pay compensation when the personal information they maintain is stolen or hacked

Generally, most participants were unenthused or even skeptical about the value of these potential changes, primarily because many saw it as impossible for the Canadian government to enforce them, especially against companies that are not run or owned by Canadians.

I am just having a tough time understanding how that would be enforced. Like I am just thinking Canadian companies that operate within Canada that have a website; sure, I think we can enact Canadian laws on them, but I'll use TikTok, for example, because it is always in the news about being owned by China, right? So, you know, you have your information on TikTok, there is a data breach and your

[8] The changes were the same as those tested on the national survey.

data is now out in the open. How would the Canadian government force a Chinese entity to reimburse people? I don't see how those two connect.

Standardizing the storage of personal information

Although most participants liked the idea of having information standardized across digital platforms, they did not see a lot of value in terms of what this would provide them. First, many mentioned that they rarely (if ever) actively searched for this information currently. Secondly, knowing what is stored was not deemed to be as valuable as the ability to remove or delete information.

Only if there is an easy way for me to get rid of it if I don't like what I see there. Otherwise, it is like okay you are showing it to me and you have it, I can't get rid of it so what?

Another issue with this policy that a few mentioned was how feasible it would be for an average person to be able to control the information that is stored online about them.

Even if they put in legislation that says these 100,000 websites now have to tell you what they have about you, now I have to go on every single one of these websites and I have to go and pull that back. That doesn't make sense.

Requiring companies to provide compensation when selling/sharing information

At first, almost all participants reacted positively to this policy change, primarily because they did not immediately see a downside to it, since they currently do not receive any remuneration when their personal information is shared or sold.

When asked what they expected in terms of compensation, amounts differed considerably, from suggestions of a few cents to five dollars. With that being said, participants would not want their personal (i.e., name, address, age, etc.) or financial information being sold or shared. However, when participants started to discuss it in depth, they had concerns about the feasibility of implementing this policy, as well as the potential value of the remuneration.

There is like a million-bajillion people online. How many people are they going to pay out and how would you even do that? That is so big and I just feel like it is not very tangible. It is a great idea; I just don't feel like that is something that could be executed well or even in a way that would make sense.

If you look at the size of these lists that they sell, each person would only get pennies, if that. I have seen lists of 10,000 valid email addresses going for like $200. Divide 10,000 by $200; each person wouldn't get very much.

A few participants took this policy a bit further and said digital companies should not be allowed to sell information at all, primarily because they were unaware this was happening.

That shouldn't be allowed. I don't know how you could stop it but I do think they should be made to compensate the people whose information they're using.

Requiring companies to provide compensation when information is stolen/hacked

Reaction to this policy change was similar to requiring companies to compensate for selling information; many thought it was a good idea in principle, but would be difficult to enforce.

That would be cool, but I don't feel like that would ever be a thing. There is like a million-bajillion people online, like how many people are they going to pay out and how would you even do that? That is so big and I just feel like it is not very tangible.

One group mentioned that the compensation could be similar to the suggestion about monitoring people's credit in case their identity or financial information was stolen.

An Equifax set up so we can be alerted. Paying all the costs of us going through identity fraud recapture. Covering all of those things would be adequate. Maybe a class action law suit if there's a large group affected, all the better.

Another group suggested that the compensation would be commensurate with the type of information stolen. For example, financial information is seen as most important to protect, and therefore, compensation for this information would be the highest, whereas compensation for having their name or address stolen would be much lower.

It depends on the information they're taking from us to use. The privacy infraction would determine the weight of the gift.

Having the right to withdraw information

Most participants liked the idea of being able to request that digital companies remove information from their website, but again, did not see how a Canadian law would be applicable to companies that did not reside in Canada.

So, if this got enacted in some way, if that meant that it would force any company that would have any sort of reach within Canada to have the same regulations then, so it could be a Canadian law but then in order for you to have Canadian's eyes on your website then you have to follow these Canadian laws which, again, logistical nightmare. Will that ever actually happen?

Another issue raised was that many participants said they do not give information to digital companies that they do not want them to have, and if it is a requirement to use the platform, they often give false information, so having this ability did not have much value for them.

You have control of what you give the company. Like if I give my name and my email address and that's it, that's it. That is all they have. If that goes out to the

world, who cares? Because my name and my email address exist. In fact, my email address is my name so if a company gets that information I really don't care.

One participant mentioned that rather than having the right to withdraw information, it may be more valuable if people had to opt-in to allow digital companies to store and maintain their information.

It would be nice to have an option to just save it for that website. Depends on the company's reputation ultimately.

The full Focus Group Report is found in Appendix E and the question set is found in Appendix F.

Review and Analysis of Legislative and Policy Frameworks (Canada): Summary

By: Public Interest Law Centre

The Public Interest Law Centre was retained by CAC Manitoba to conduct a review of regulatory and legislative instruments in Canada relevant to consumer protection and risks to consumers associated with digital services and digital service marketplaces.

Compared to literature identifying best practices and examples of consumer protection frameworks in other jurisdictions, Canada has fallen behind but may be catching up.

In response to early developments in internet usage and internet commerce, Canada has created piecemeal protections through statutes such as the *Personal Information Protection and Electronic Documents Act* of 2000, and its 2010 *Anti-Spam Legislation*. These serve to provide consumers with baseline protections for privacy and prohibitions on at least the most egregious of business practices regarding the collection and use of personal data. However, there is much that these statutes do not address.

Another significant missed opportunity for Canadian consumers is seen in the fact that with few exceptions, provinces and territories have not updated otherwise robust consumer protection legislation to reflect risks posed by digital service marketplaces.

Given these shortcomings, the contents of consumer protections in Canada do not measure up to what is now recognized as leading practice in relevant literature and novel approaches implemented internationally.

However, Canada's statutory protections for consumers engaging in digital marketplaces are on the cusp of improving significantly for the benefit of Canadians. Recent policy development and forthcoming legislation stands to substantially improve digital consumer protection for Canadians.

Though not passed at the time of writing, the *Digital Charter Implementation Act 2022* consists of three acts which will govern the relationships between consumers and

organizations regarding the collection, use and disclosure of personal data including the provision of consent, and complementary measures creating means of recourse for consumers harmed by inappropriate use of information.

While the proposed legislative changes contain substantial improvements for Canadians, approaches taken in international jurisdictions may remain more robust in terms of the specificity and clarity of information to be provided to consumers, the standards of adequacy concerning the provision of consent, and the creation of opportunities for data portability may invite further development in Canada following close observation of experience elsewhere.

The full Review of Canadian Legislation and Policy is found in Appendix H.

Review and Analysis of Legislative and Policy Frameworks (International): Summary

By: Public Interest Law Centre

The Public Interest Law Centre has reviewed the statutory frameworks for digital consumer protection in the United States (including a focus on California), Australia, and the European Union and presents examples of diverse approaches to legislating for consumer protection and the protection of privacy of personal data from digital service marketplaces.

The findings suggest that within the variety of approaches to consumer protection reviewed there exist themes and consistencies that highlight the importance of express and explicit consent, consumer education, and potential future opportunities to strengthen consumers' positions in digital service marketplaces. Perhaps most importantly, the field is rapidly developing such that there will be significant value for Canada in closely monitoring developments worldwide.

The United States, and California in particular, represent the legal home of many large digital service providers. This has given rise to leading protections for consumers in terms of the provision of information, the obtaining of express consent, and the expansion of consumers' rights over their information.

Australia, in addition to strengthening requirements for provision of accessible information on risks and vulnerabilities consumers face with respect to their data, is also cautiously exploring data portability as a means of enabling consumers to benefit from the value of their personal data. Introduced on a pilot project basis in certain sectors, the Australian experience with data portability will be one to monitor closely.

Finally, the European Union's recent *General Data Protection Regulation* and complementary *Digital Services* and *Digital Markets Acts* position the EU as a leader in

protecting the private information of consumers as they engage in digital marketplaces.

Following a review of the statutory frameworks in these jurisdictions, the following elements of consumer protection are identified as potentially of value for consideration in Canada:

1. Other jurisdictions are imposing strong requirements that information for consumers about service providers' collection, use, storage and sharing of their personal data be made readily available, both accessible in plain language and detailed, and at minimum available upon request if not expressly provided.
2. There is an appearance of a trend emerging by which consent collected from consumers for the collection, use and sharing of their personal data must be expressly provided, must be fully informed, must be specific, in that blanket consent statements condoning a wide range of activities are not acceptable, and importantly, can be revoked. Revocation of consent should result in immediate stoppage of the activity previously consented to, and in particular, to deletion of information if the withdrawal of consent pertains to information storage and use.
3. Data portability, by which consumers' personal data is collected and stored in a standardized fashion and shared between service providers under the control and direction of the consumer, may be a valuable opportunity for consumers to strengthen their position in the market and benefit, potentially monetarily, from the value of their personal data. Models of data portability are being piloted in both Australia and the European Union, the results of which may invite consideration in Canada.

The full Review of International Legislation and Policy is found in Appendix I.

Consumer protection fit for the digital age

By: Professor Marina Pavlovic

Professor Marina Pavlovic was retained by CAC Manitoba to conduct research and analysis of the current consumer protection framework and its responsiveness to the digital environment and provide suggestions for reform. This section complements and builds upon the review and analysis of the legislative and policy frameworks conducted by the Public Interest Law Centre.

While the Canadian consumer protection framework provides some basic protections for consumers, it is not fit for the digital age.

Firstly, consumer protection issues now arise in a broader context and straddle both geographical (cross-provincial/territorial and international) and substantive borders (such as consumer protection proper, competition, privacy, etc.). An enhanced and coordinated cooperation between provincial and federal authorities is required in order to create a more robust consumer rights framework fit for the digital age.

Second, the provincial/territorial consumer protection legislation requires significant reform to bring it up to date with the issues arising in the digital society. There are three main areas of concern:

- The provincial/territorial consumer protection framework is rooted in the notion of "commercial" relationships where there is an exchange of goods or services for money. While monetary exchange is still the dominant way in which consumers acquire major goods or services, a growing number of consumer relationships is based on seemingly free relationships, in which consumers exchange personal information for goods or services. These relationships should be brought under the purvey of the provincial/territorial consumer protection statutes to ensure that all aspects of consumers' participation in the digital society are afforded equal protection.
- The current consumer protection framework does not account for and does not protect consumers against online-specific practices, such as dark patterns (interfaces that trick consumers into certain actions). These practices should be

brought under the purview of the legislation. Additionally, the inter-provincial/territorial cooperation should ensure that there are processes in place to monitor for future harmful patterns and proactively address them.

- Most consumer relationships in the digital society are governed by non-negotiated standard-form contracts. While the provincial/territorial consumer protection legislation provides minimum protections (such as that the consumers cannot contract out of the rights in the respective consumer protection act), these contracts have become a dominant regulatory mechanisms of consumer relationship and have expanded the role of private ordering into all realms of digital life. Consumers have no choice but accept the contracts as is. These unilaterally defined contracts implement an online private ordering which allows private actors to effectively work around existing legislation. Commonly used clauses are that the vendors can unilaterally change the terms, restrictions on remedies, restrictions on litigation and class actions, etc. Each of these clauses on its own and, even more so, collectively, further erode an already inadequate protections and often leave consumers without any recourse. Contractual clauses that are harmful to consumers should be prohibited in the legislation. A recently published Discussion Paper by the Ontario Law Commission- *Consumer protection in the digital marketplace* - provides a detailed account of these clauses.[9]
- The provincial/territorial legislative framework does not account that consumers are not a uniform group, rather they come from diverse social locations which makes certain groups (such as youth or elderly) more vulnerable. Any future reform should ensure that there are special protections for vulnerable consumers.

[9] Ontario Law Commission, Consumer Protection in the Digital Marketplace (June 2023), available online: https://www.lco-cdo.org/wp-content/uploads/2023/06/LCO-Consumer-Consultation-Paper-Updated-Final.pdf

Discussion

As this research progressed, a number of themes began to recur in the results of various research tools. Beginning with the review of literature, and reflected in subsequent phases of the research and the data from other research components, the following prominent themes have emerged:

An increasingly digital world

Consumers' reliance on online services worldwide is continuing to grow. This is particularly true in our post-pandemic world. This means that consumers are increasingly exposing themselves to significant risks through their participation in online marketplaces, and are frequently doing so without the benefit of an informed understanding of the nature or extent of the risk, the value of the personal data which they may be giving away, or the protections that may be available to them. These new commercial relationships are materially different from those of the past.

Consumer awareness

Consumers' awareness of how digital service providers and online platforms collect, secure, use and share data is key. Clear disclosure by service providers which provides adequate information about their data collection and use practices is vital to consumers' ability to make informed decisions and exercise meaningful control over personal data that has been collected.

This theme is echoed in the panel survey data, which shows that consumers concerns about and awareness of data collection are high, but actual knowledge about these practices is substantially lower. Experience in international jurisdictions suggests that the importance of well-informed consumers is beginning to be recognized.

Risks to consumers

Consumers face a variety of risks related to privacy and consent, algorithm-based targeted advertising, the transparency and liability of online platforms, and risks

related to possible data theft or leaks. While the risks related to data theft or leaks may present the most obvious consequences (for example, financial consequences flowing from theft and use of payment information), others are more complex. Consumers face significant uncertainty when they expose their personal data to collection and use by digital service providers. Their data may be stored with unknown protections, shared or sold to unknown third parties, and used to manipulate the consumer's digital service experience, potentially all without their knowing.

Meaningful consent

Flowing from the concept of consumer awareness of data collection and use is the related issue of meaningful consent. The review of literature points to the importance meaningful consent with regard to privacy agreements, and this is strongly reinforced in the data arising from the key informant interviews and focus groups. Privacy policies need to be clear, concise, transparent and accessible in order to for consumers to be able to read and understand what they are consenting to, and thus be able to fully appreciate the risks. Additionally, consent that is broken down into options rather than being "bundled" allows consumers to "opt in" (or not) to sharing their information while still being able to access services. Ultimately, consent must be informed, meaningful, and revocable. Data arising from the focus groups reinforces the understanding that consumers need more clarity with regard to terms of service, specifically what information is being collected and stored, and how this information may be used. In particular, the common practice of subjecting consumers to long, non-negotiated standard-form terms of service deprives consumers of the ability to be properly informed and to provide meaningful consent.

Possible regulatory solutions

Legal protections in place today are inadequate relative to the risks consumers face with respect to their personal data. The available protections are also ill-suited to the unique attributes of digital commerce that are distinct from non-digital contractual relationships. A range of regulatory solutions emerge in the literature to counter privacy risks posed to consumers in the digital marketplace, including the right to be forgotten and the concept of data portability. Strong support for regulatory changes

was voiced by key interview respondents, and this is echoed in the panel survey and focus groups. Interestingly, data from the focus groups in and key informant interviews suggests that consumers' awareness of current available protections is low, indicating a need for consumer education.

While there are currently proposed legislative changes in Canada which contain substantially improved protections for Canadians, approaches taken in international jurisdictions are considered to be leading the development of consumer protections. In particular, even after Canada's amended legislative framework is in place, international examples may remain more robust in terms of the specificity and clarity of information to be provided to consumers, the standards of adequacy concerning the provision of consent, and the creation of opportunities for data portability may invite further development in Canada following close observation of experience elsewhere.

The findings in the international review of legislation suggest that within the variety of approaches to consumer protection reviewed there exist themes and consistencies that highlight the importance of express and explicit consent, consumer education, and potential future opportunities to strengthen consumers' positions in digital service marketplaces. Perhaps most importantly, the field is rapidly developing such that there will be significant value for Canada in closely monitoring developments worldwide.

Other themes that emerged through the panel survey, focus groups, and key interviews include:

Digital media literacy and algorithmic literacy

Digital media literacy and algorithmic literacy are key factors in begin able both to understand and to mitigate privacy risks. Educating consumers to be cognizant of the ways in which algorithmic architectures shape their online experiences, including the information, advertising, and opportunities with which they are presented empowers them to discerning about how potentially manipulative or discriminatory algorithms.

Education is especially critical for vulnerable consumers, one such group being children and youth.

Vulnerable groups

An important theme which arises is that consumers engaging in digital marketplaces are not uniform and come from diverse social locations. As a result, some consumer groups are more vulnerable than others, and are therefore at increased risk in the digital marketplace. The panel survey data suggests that younger people may be more at risk; younger respondents tend to be the heaviest digital users, yet appear to be least likely to take steps to protect their personal information. Groups identified as vulnerable in the key informant interviews are: children and youth, seniors; low-income individuals; those living in northern, rural, or remote regions; Indigenous communities, particularly seniors and youth; BIPOC and marginalized or racialized 2slgbtq+ women; newcomers or others with limited English language skills; and persons with disabilities (visible or invisible). Risk increases for those in multiple intersections of vulnerability. Access and opportunities for more vulnerable groups with regard to education on topics such media and algorithmic literacy should be emphasized.

Opportunities for further research

Canadian consumers would benefit from further research looking at ways to improve and implement digital media literacy for youth and other groups identified as being at greater risk, with an emphasis on equipping consumers to understand information-gathering practices in the digital marketplace. Ongoing research and monitoring of jurisdictions implementing more consumer-orientated regulatory solutions that address consumer privacy would be helpful in guiding future regulatory reforms.

Conclusions and Recommendations

What are the consequences of the information gathered online by digital platforms and online companies? How aware are consumers about these impacts? How informed are consumers about the protections available to them and the impacts of not engaging these protections ?

Based on the contents of its research, CAC Manitoba observes that consumers' reliance on online services and digital service marketplaces worldwide is continuing to grow. As consumers increase their engagement with these marketplaces, they are exposing themselves to potentially significant risks. CAC Manitoba understands consumers' understanding of these risks to be low, the protections available to them in Canada to be developing, and their awareness of the available protections to be inadequate. Consumers frequently do not know what or how much information they are giving away, how it might be used, and how it might do them either good or harm. Importantly, consumers' perceptions of risk and opportunity suggest that the value of their own personal data is not well understood.

The literature shows that consumers are not equipped to fully appreciate the risks involved in engaging with digital service marketplaces, and as a result are vulnerable to activities such as data-harvesting, targeted marketing, or political influences by service providers and digital platforms. Compounding this, they navigate these murky waters in an online architecture that has been constructed to favour the powerful tech companies and platforms that dominate the online marketplace, with long-winded, inaccessible terms of use and statements of consent that are seldom read or difficult to understand, rendering the provision of consent for data collection and use meaningless. The results from the key informant interviews re-enforced these findings, and also emphasized that socio-economic and other barriers to information access and digital literacy compound these risks among members of marginalized communities and groups.

We learned from the digital technology panel survey, key informant interviews and focus groups that consumers are greatly concerned about protecting their personal privacy online. We also heard about the importance of raising awareness through education. Digital and media literacy were identified as key ways to enable consumers to protect their privacy online, and multiple potential sources of information and

education were identified. Key informants noted that burden of privacy protection which now rests too heavily on consumers, and suggested that it needs to be shared by both the business community and government, and that consumer privacy protection needs to be more robustly guided and regulated by policy makers.

From the legislative reviews, we learned about proposed changes to consumer protections in Canada, such as the *Digital Charter Implementation Act 2022*, which at the time of writing had completed First Reading, constitute steps towards improved consumer privacy protection for Canadians. International jurisdictions however, have gained greater strides in terms of specificity and clarity of information to be provided to consumers, the standards of adequacy concerning the provision of consent, and the creation of opportunities for data portability. Canada would benefit from closely following the experiences of these jurisdictions to inform future policy as this sector continues to grow, and further research on the topic of consumer digital protection should remain a priority.

Flowing from the results of the reviews of literature and legislation, the digital technology survey, and key informant interviews, and supported by the focus groups, CAC Manitoba offers the following recommendations to government, regulators, and industry.

1. Responsibility for consumer protection should be shared by all levels of government as well as industry and consumers themselves.
    a. Consumers of all ages should have access to educational resources and opportunities to equip them to take appropriate steps to protect themselves while engaging in digital services marketplaces.
        i. Digital media literacy, algorithmic literacy, principles of information gathering and use, consent, and statutory and regulatory privacy protections should be integrated into school curricula through a variety of subject matters and diverse teaching methods, including the development of an algorithmic literacy "lens" as a teaching tool.
        ii. Digital media literacy, algorithmic literacy, information gathering and use, consent, and statutory and regulatory privacy protections should be the subject of ongoing public education campaigns with varied content and strategy targeting distinct demographics and age categories.

b. Educational resources regarding consumer protection in digital services marketplaces should be designed to effectively reach all consumers, regardless of age, place of residence, levels of experience and digital media literacy, or the preferred usage of and means of accessing the internet.
    i. Educational opportunities should be available both in-person and online in a variety of creative formats.
    ii. Educational resources should include information of practical application, such as step-by-step guides to implementing privacy protections or changing privacy settings on devices or in online accounts.
    iii. Ensure that vulnerable and/or marginalized groups are specifically targeted with educational resources and opportunities, potentially by partnering with and/or funding activities by non-profit organizations already engaged in these communities.

2. Legal and regulatory requirements as well as public pressure should be applied to ensure that businesses do their part to enable consumers to protect themselves.
    a. Information provided to consumers and customers should be accessible, easy to understand and comprehensive.
        i. All information respecting privacy and the treatment and use of personal data should be provided in plain language, should be brief, and must be clear.
        ii. A standard, prescribed form or format for the presentation of this information should be developed to improve consumers' comprehension (for example, standardized nutrition labels contribute to consumers' understanding of the contents of their food).
        iii. All information respecting privacy and the treatment and use of personal data should be provided in a manner accessible to consumers with diverse needs including those using assistive technology such as screen readers.
    b. Consumers' provision of consent regarding the treatment of their personal data should be meaningful, consumer-friendly and guided by best practice.

i. Service providers should be required to obtain consumers' consent before collecting, storing, transferring or otherwise using personal data.
ii. The process of providing consent should be *active* rather than *passive* or *implied*, meaning that consumers should be required to expressly opt-in to allow service providers access to and permission to use their personal data.
iii. The process of providing consent should be *disaggregated* such that consumers can elect to expressly permit the collection and/or use of *certain* personal data and not others, and that consumers can elect to expressly permit certain uses for their data to the exclusion of other uses.

c. Service providers should be obligated to provide support to consumers in the event that their personal data is compromised or misappropriated.
    i. Examples include, for example, paying for credit monitoring services for a period of time following disclosure of personal and/or payment information.
d. Regulators should collect and publicize information relevant to consumers' interests in protecting themselves.
    i. Statutory complaint mechanisms should be well-publicized and accessible to consumers, including through step-by-step procedural guidance and information about options for redress.
    ii. Information gathered through public complaint mechanisms about the conduct of digital service providers should be made public.
e. Federal and/or provincial governments should develop a best-practice guide for digital service providers to serve as an aspirational benchmark. The "Product Safety Pledge" initiatives in Australia and the European Union are examples for consideration.
f. Digital consumer protection should remain a subject of significant interest for Canada's Office of Consumer Affairs for the purpose of funding research.

3. Statutory and Regulatory Reform
    a. The mandatory 5-year review period currently drafted in Canada's *Digital Charter Implementation Act* should be preserved and included in the final version of the Bill and fulfilled on the prescribed timeline. Responses by government to the review process should include a proposed timeline for further legislative amendments.

b. Federal and provincial legislators should continually monitor developments in digital consumer protection in other jurisdictions to ensure that Canada's approach to consumer protection continues to reflect best-practice in a quickly changing environment.
c. Provincial consumer protection legislation should be updated to reflect risks faced by consumers in digital services marketplaces, including when accessing services of local service providers.
d. Consumer protection legislation in general should be accessible, in plain language, and actively communicated to the public to ensure that consumers can benefit from the protections available to them.

4. Data Portability constitutes a fundamental shift in consumers' relationships with digital service providers. should be approached with extreme caution in Canada. The idea may be of value to consumers but should be approached with extreme caution.
    a. The more advanced state of data portability frameworks in Australia and the European Union call for close observation of consumer experiences in those jurisdictions for guidance in the development of Canada's own framework.
    b. Regulations under forthcoming legislation to facilitate Data Portability should not be implemented until extensive public consultation and research is complete.
    c. Should Data Portability proceed in Canada, consumer education about the potential consequences of actively engaging in the collection and sale of personal data should be a high priority.
    d. Should Data Portability proceed in Canada, the above-noted recommendations respecting obtaining consent will be of paramount importance.
    e. Regardless of whether Data Portability proceeds in Canada or the form that it will take, a statutory or regulatory requirement that consumers' personal data be stored in a standardized format may be of value to consumers.

Glossary of Terms and Acronyms

Algorithm. A set of step-by-step instructions for solving a problem or completing a mathematical or computational task. Algorithms sort data to find patterns and make predictions or recommendations. The term is often used to refer specifically to computer programs trained to make predictions. (Media Smarts, Algorithmic Awareness). https://mediasmarts.ca/sites/default/files/publication-report/full/report_algorithmic_awareness.pdf

Algorithmic Literacy. Algorithmic literacy does not only refer "strictly to being able to read and write in code" but also involves "being aware of the presence of algorithms... and the increasing role they play, both for good and for bad. (Media Smarts, p. 19, Algorithmic Awareness). https://mediasmarts.ca/sites/default/files/publication-report/full/report_algorithmic_awareness.pdf

GDPR. GDPR stands for General Data Protection Legislation. It is a European Union (EU) law that came into effect on 25th May 2018. GDPR governs the way in which we can use, process, and store personal data (information about an identifiable, living person). https://gdpr-info.eu

PIPEDA. The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of their commercial activity. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/#

Appendices

The following Appendices are attached to this report:

Appendix A – Review of Literature
Appendix B – Key Informant Interview Report
Appendix C – Digital Technology Panel Survey Report
Appendix D – Digital Technology Panel Survey Questions
Appendix E – Focus Group Report
Appendix F – Focus Group Discussion Guide
Appendix G – Recruiting Guide
Appendix H – Canadian Review of Legislation and Policy
Appendix I – International Review of Legislation and Policy