Protecting Privacy Rights in the Digital Age

July 2023

Imani Thomas, Harshini Ramesh, Caroline Wilson, Elisa Alloul

MAX BELL SCHOOL *of* PUBLIC POLICY

Acknowledgements

We would like to extend our gratitude to our sponsor organization Interac Corp. for presenting us with this meaningful and pressing policy issue. We sincerely thank the Interac team for the time that they spent with us and their constant support.

We would also like to express our deepest appreciation for our coach, Neil Bouwer, for his expertise and guidance over the past eight months. It has been an insightful experience working with him to shape the direction of this report and to inform our understanding of the policy-making process.

Our report could not have been developed without the support of the Max Bell School of Public Policy community. We thank Nathalie Duchesnay for her leadership as the Policy Lab Coordinator at the Max Bell School. We also thank our professors Dr. Taylor Owen and Pearl Eliadis for their assistance in helping us contextualize the technological and human rights considerations of this Policy Lab. Thank you also to Dr. Scott Janzwood, John Stewart, and Louis Levesque, for their assistance in either reviewing our work or providing advice on policy implementation. We deeply appreciate the dedication the resourceful Max Bell administration has demonstrated to this cohort. We also recognize the efforts of the Director of the Max Bell School, Dr. Christopher Ragan, in creating a community of people passionate about the role of policy in shaping our world.

Thank you to all stakeholders who took the time to speak with us. For a comprehensive list of stakeholder interviewees, please refer to Appendix A.

This document was produced by students at McGill University's Max Bell School of Public Policy as part of the requirements of the Policy Lab, a capstone project of the Master of Public Policy. The contents within do not necessarily represent the views of McGill University, the Max Bell School, Interac Corp., our coach, or stakeholders consulted throughout the process.

Table of Contents

Executive Summary

Economic activity has been transformed by the ability to turn ubiquitous data into valuable insights. One category of this abundant data is personal information, which provides insights into people's characteristics, preferences, and behaviours. No matter the type or sector, every organization in society can use this information to their benefit, whether it be to improve their operations, boost fundraising, gauge voting intentions, or sell services and products. Individuals also gain value from data-driven innovations — 67% of Canadians are willing to share their data for new products or better customer experiences.

However, as more data are collected, people's private spheres continue to shrink. Renowned Harvard professor Shoshana Zuboff coined the term "surveillance capitalism" to describe the phenomenon of collecting excessive amounts of information from and generating insights on groups and individuals.

Balancing the protection of people's privacy with data-driven economic growth is the central challenge of the Digital Age. This Policy Lab report, sponsored by Interac Corp., examines this tension in Canada and how Canadians' privacy protections can be strengthened in the Digital Age. Specifically, it answers the following question:

"With a complex environment of digital privacy protections across various jurisdictions in Canada, what regulatory and legislative changes are needed to recognize digital privacy as a basic human right for all, and how do we ensure digital inclusion and control of data are considered as part of the solution?"

The main objectives of this report:

1. To provide an understanding of Canada's digital privacy challenges by outlining how digital transformation impacts privacy and trust in the digital economy
2. To outline Canada's current privacy policy landscape and proposed legislative changes to the federal regime
3. To propose a human rights-based approach to digital privacy

Interac is a financial technology company navigating the digital privacy policy landscape in Canada. As an organization dealing with sensitive financial information, Interac emphasizes the pre-eminence of privacy and has put forward public education and innovative regulatory initiatives supporting privacy protections. The current federal legal landscape in Canada is changing with the proposed legislation, Bill C-27, the Digital Charter Implementation Act. Interac can play a positive role in changing the trajectory of digital privacy conversations in Canada.

A Snapshot of the Digital Age

Data is a key driver of economic growth in Canada. The digital economy has seen a significant increase in its nominal GDP, outpacing the growth rate of the overall economy at 40% between 2010 and 2017.

In 2019, the industry was worth $118 billion, making it nearly as valuable as Canada's lucrative mining, oil, and gas industries ($119 billion). Both public and private organizations are investing considerably to leverage innovations in advanced analytics, algorithms, and artificial intelligence (AI) to understand how best to collect and process data. This prospecting in the digital economy has led to data being described as "the new oil".

Canadian Digital Privacy Challenges

Privacy in the Context of Private Sector Operations

Data analytics and other new technologies have and will continue to drive economic value and competitive advantages in business and politics. This has major implications for the protection of personal information and by extension, people's privacy. A fundamental tenet of Canada's commercial privacy law is respecting privacy by obtaining consent. Despite federal and provincial privacy laws outlining responsibilities around consent and safeguarding of personal information, businesses are not always compliant with their privacy obligations. Small and medium-sized enterprises (SMEs) in particular face challenges in balancing innovation with complying with privacy law.

Role of Trust in the Digital Era

Trust is critical to growth in the digital economy. People generally expect that information they share about themselves will be used for the purposes that they have identified and that any other information that is discerned about them will be used in a fair and appropriate manner. However, this has not always been the case. In a 2023 survey conducted on behalf of the Office of the Privacy Commissioner of Canada, 39% of individuals believed that businesses respect their privacy rights, a decline from 45% in 2020. Additionally, in a survey commissioned by Interac earlier this year, 74% of Canadians expressed that they would like more control of their online information. Unlike data, trust is not ubiquitous in the digital economy.

Privacy Harms in the Digital Era

A breakdown of trust is not the only kind of harm that can arise in the digital era. The digital space recreates systems of oppression that have harmful impacts on marginalized communities by infringing upon their privacy rights. For example, overcollection of data increases surveillance of traditionally marginalized groups, while data processing can cause discrimination against entire groups, ultimately putting civil and political rights at risk.

Global Policy Shifts

Recognizing that there is a myriad of harms associated with violations of digital privacy, jurisdictions such as the European Union (EU), California and Quebec have moved towards updating their privacy protection legislations. Canada risks falling behind its trading partners, namely, the EU which requires other countries to have privacy legislation comparable to its own to facilitate cross-border data transfers. To ensure that trade can continue uninterrupted, Canada has an imperative to update its privacy laws.

Canada's Policy Landscape

There are three privacy protections to consider under federal law:

1. The Personal Information and Protection of Electronic Documents Act (PIPEDA) is Canada's privacy law governing the use of personal information in commercial contexts.
2. The Office of the Privacy Commissioner of Canada (OPC) is Canada's federal privacy oversight body, responsible for overseeing compliance with the Privacy Act (privacy law applicable to the federal public sector) and PIPEDA.
3. Privacy law outside of commercial use largely concerns the Canada Elections Act which governs the use of personal information in the electoral process as it relates to the maintenance of the Register of Electors.

The federal government is in the midst of updating its privacy regime with Bill C-27, The Digital Charter Implementation Act, which comprises three parts: The Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act.

Existing privacy laws and the current iteration of Bill C-27 are limited in their ability to protect privacy. First, the legislation and bill do not adequately recognize or provide special requirements for sensitive information. Second, despite all sectors being involved in data collection and processing, much of the activities conducted by political parties and not-for-profits are not covered by the law. Third, there are gaps in governing data processing, specifically for the de-identification and anonymization of data. Fourth, current privacy supports are not fully equipped to support SMEs and not-for-profit organizations (NPOs). Finally, the OPC does not have the enforcement powers to fully encourage adherence to privacy laws.

Towards a Human-Rights Based Approach to Privacy Policy

Rapid developments in technology are putting people's privacy at risk. Canada's current regime views privacy through a commercial lens, which does not fully account for the human rights impacts of privacy infringements. Canada needs a human rights-based approach (HRBA) to privacy to strengthen protections. Taking an HRBA to privacy means recognizing two key pillars: 1) information is inherent to personhood and 2) accountability and inclusion foster trust. This approach forms the foundation for two key recommendations to bolster Canada's privacy regime:

Recommendation 1: Raise the Level of Responsibility for Private Actors

Interac should advocate for an HRBA to protect personal information. This begins with recognizing that there is an inherent "humanness" to data – personal information is inalienable from a person and by extension, their personhood. As such, legislative and regulatory changes should include stricter governance around the processing of people's information.

1.1 Safeguarding Sensitive Information

Effectively safeguarding sensitive information begins with a clear definition within the legislation and acknowledging that not all sensitive personal information has the same level of sensitivity and potential for harm. In addition to defining sensitive information, a tiered system of sensitive information should be implemented to ensure that private actors are treating and protecting the most sensitive information with the highest security possible.

1.2.1 Filling in the Governance Gaps

Bill C-27 should extend its scope and include not-for-profits, political organizations, and other similar actors who are not commercial operators but collect and process significant amounts of personal information for their operation.

1.2.2 Governing Data Processing

Bill C-27 should include the “processing” of data, expanding its focus from collection, use, and disclosure. A new set of regulations should be established to provide uniform guidance on managing personal and sensitive information when it is de-identified and/or anonymized.

Recommendation 2: Engineer an Environment of Trust

To build trust in the digital privacy environment, Interac should advocate for elevating community voices in a national conversation on privacy and ensuring the OPC has the ability to effectively promote compliance.

Recommendation 2: Engineer an Environment of Trust

To build trust in the digital privacy environment, Interac should advocate for elevating community voices in a national conversation on privacy and ensuring the OPC has the ability to effectively promote compliance.

2.1 Digital Privacy Dialogues Initiative

Businesses such as Interac should adopt a Digital Privacy Dialogues corporate social responsibility initiative. Such an initiative would convene community members to enable them to discuss their priorities and vision for an HRBA to digital privacy protections.

2.2 Establishing an SME and NPO Advisory Directorate

Such a directorate could support SMEs and NPOs in accessing resources regarding best practices for compliance. This dedicated support would help organizations adapt, and comply with new and amended laws, regulations, and policies, and reduce the risk of investigations, fines, and privacy breaches.

2.3 Enforcing Privacy Law

Bill C-27 should empower the OPC to enforce privacy with adequate regulatory tools including the power to issue monetary penalties.

Introduction

Data are ubiquitous and comprise of any economic activity taking place online.[1] The digital economy is more than 15% of global GDP and is growing twice as fast as the physical world's GDP.[2] As the COVID-19 pandemic swept the globe, more people interacted online, causing digital customer interactions to jump from 36% in December 2019 to 58% in July 2020.[3]

The ability to derive value from data is transforming economic activity, causing countries to compete to leverage data for economic growth and take the lead in technological developments.[4] Data from personal information provides insights on people's characteristics, preferences and behaviours, providing a wealth of knowledge for all sectors. Organizations can use this information to improve fundraising, gauge voting intentions, and sell services and products. People also gain value from data-driven innovations, with over two-thirds of Canadian consumers willing to provide their personal data in exchange for an improved product or customer experience.[5]

However, ubiquitous access to data is shrinking people's private spheres. From the use of social media, to banking and exercising, massive amounts of data can be harvested from a person, tracing anything from their health and interests, to their location.[6] Renowned Harvard professor Shoshana Zuboff pioneered the term "surveillance capitalism", a phenomenon which describes the collection of excessive amounts of data that is then sold or used to generate insights about individuals and groups.[7] She argues that "privacy is not private" because public and private systems of surveillance are dependent on people giving up information about themselves.[8]

Additionally, infringing on people's privacy rights creates severe risks for discrimination and the violation of civil and political rights, especially for traditionally marginalized and vulnerable communities.[9] As such, the United Nations Human Rights Council adopted a resolution in 2019, emphasizing that people have a right to privacy in the Digital Age and that this right must be protected.[10]

Balancing the protection of people's privacy with data-driven economic growth is the central challenge of the Digital Age. People are more willing to share their data, but the pandemic has made them more cautious of their privacy, with trust and transparency becoming key considerations.[11] In fact, 44% of consumers are willing to "switch companies or service providers over their data policies or data sharing practices".[12] The following Policy Lab report critically analyzes this tension in Canada and how Canadians' privacy protections can be strengthened in the Digital Age. Specifically, it answers the question posed by Interac, the Lab's Sponsor:

"With a complex environment of digital privacy protections across various jurisdictions in Canada, what regulatory and legislative changes are needed to recognize digital privacy as a basic human right for all, and how do we ensure digital inclusion and control of data are considered as part of the solution?"

The report will examine Canada's digital privacy challenges by outlining how digital transformation impacts privacy and trust in the digital economy, and Canada's position in the world. It then

presents an analysis of Canada's federal privacy landscape to outline the current policy landscape and proposed legislative changes to the federal privacy regime and highlights the limitations of both. The report applies a new lens to viewing privacy – a human rights-based approach to privacy protections. This forms the basis for two key recommendations. The first recommendation presents legislative changes to raise the level of responsibilities private actors have in protecting Canadians. The second recommendation aims to build trust in the Digital Age through policy initiatives, by elevating Canadians' voices in digital privacy conversations, and by strengthening accountability.

This policy question is especially pertinent for Interac, a private sector actor that is navigating the digital privacy policy landscape in Canada. As a financial technology company regularly dealing with sensitive financial information, Interac has acknowledged the role all actors in society have in "understanding the wide (and wild) world of data privacy".[13] It has targeted its public education efforts at helping consumers understand the intricacies of personal data privacy and security.[14] The policy analysis and impacts of privacy infringements presented in this document provide critical information for new educational opportunities for the public.

Further, Interac thinks critically about ways to innovate on building trust beyond regulatory compliance, as evidenced by the work of its Emerging Regulation and Innovation team.[15] This report provides innovative legislative and regulatory ideas and methods for guaranteeing people's privacy to inform this team's activities. Most importantly, Interac can play a positive role in changing the trajectory of digital privacy conversations in Canada. Last year, the federal government introduced Bill C-27, the *Digital Charter Implementation Act*, to update the federal commercial sector privacy law.[16] The bill targets consumer protections, enforcement capabilities of the Office of the Privacy Commissioner of Canada (OPC), and artificial intelligence governance.[17] This report serves as a starting point for sparking nation-wide conversations on taking a human rights-based approach to digital privacy.

Research Methodology

Part 1: Literature Research

To define the problem, analyze the policy landscape, and create policy recommendations, the research process focused on addressing the following questions:

- What does it mean to recognize privacy and digital privacy as a human right?
- What impacts does the digital space have on privacy infringements for people, especially from traditionally marginalized communities?
- What are the existing Canadian federal and provincial privacy legislation and regulations? What are these protections in jurisdictions comparable to Canada?
- What are the gaps in existing Canadian federal and provincial legislation and regulations?
- What are the impacts of privacy policies on private organizations?

Sources include but are not limited to academic literature, Canadian, American, and European legislation and regulations, insights and recommendations published by the OPC and other

privacy experts in various sectors, government and non-governmental organization reports, articles and reports about the approach to digital privacy as a human right, studies conducted on digital privacy experiences harms, publications from Interac, and books focused on data privacy.

Part 2: Stakeholder Interviews
Stakeholders were selected based on expertise in four key areas: public sector, for-profit sector, academia, and human rights advocacy (for a comprehensive list of stakeholders, see Appendix A). The first stage of conversations conducted from January to March focused on understanding the privacy challenges and Canadian policy landscape in the Digital Age. From April to June, the conversations shifted to testing recommendations and understanding feasibility, strengths, and limitations. These conversations were largely conducted with stakeholders who were consulted in the first round.

Limitations

This Policy Lab focuses on legislative and policy analyses, and recommendations at the federal level. The introduction of Bill C-27, the *Digital Charter Implementation Act*, which is being discussed in the House of Commons, presents an opportunity to insert new ideas and dialogue into the privacy policy landscape during an imminent shift in Canada's privacy regime. Provincial legislative and policy changes are not discussed as they fall outside the scope of Bill C-27. The report does not extensively address the *Artificial Intelligence and Data Act* (AIDA) component of Bill C-27. Platform governance is not covered in this report as it is more relevant to analyses of competition law and policy. Cybersecurity is not addressed in this project. Additionally, the implications and impacts of privacy legislation on trade are acknowledged but not significantly analyzed.

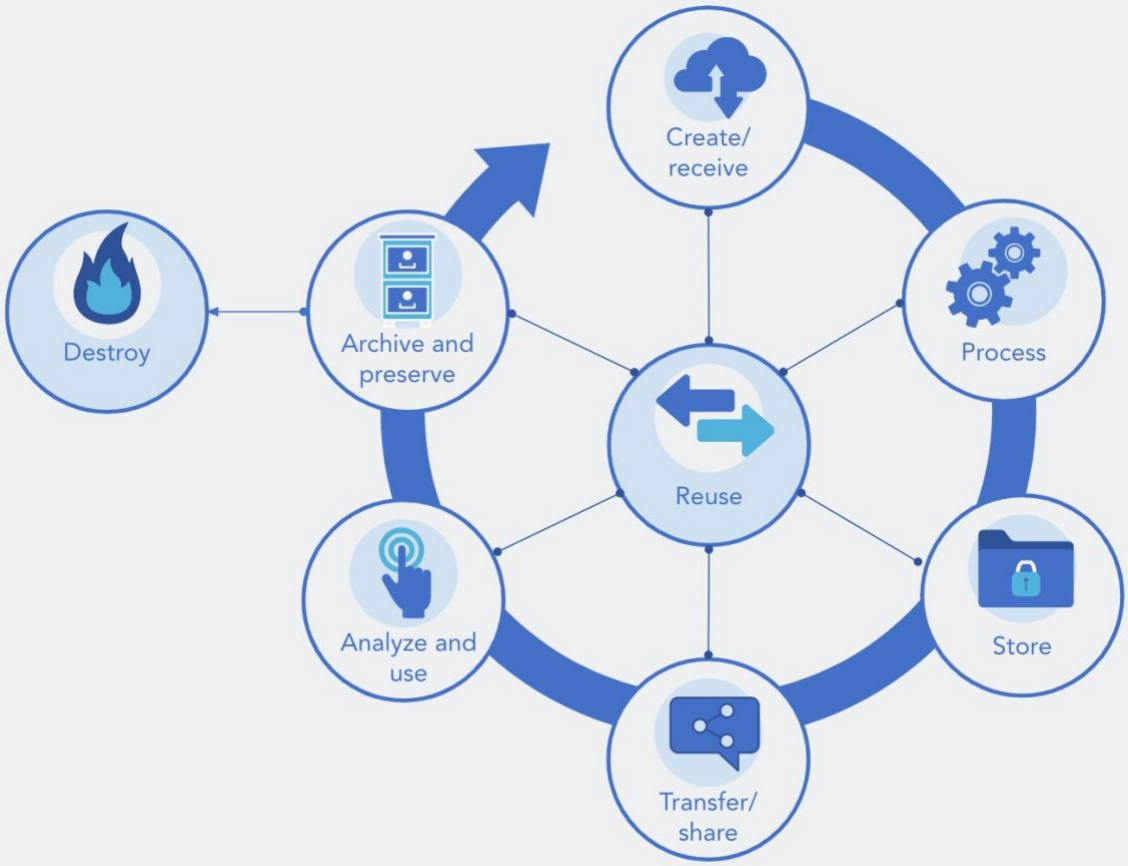
This Policy Lab does not reflect lived experiences from traditionally marginalized communities. Time and resource limitations presented constraints for conducting meaningful engagements with traditionally marginalized communities. This Policy Lab does not cover Indigenous law and issues of data sovereignty. Meaningful and culturally appropriate consultation is necessary with Indigenous rights holders to reflect legal interpretation, policy challenges, and recommendations in a respectful and impactful manner.

A Snapshot of the Digital Age

Opportunity abounds in the Canadian digital economy. The size of the industry has ramped up considerably in the past decade, with nominal GDP for the digital economy outpacing the growth rate of the overall economy at 40% between 2010 and 2017.[18] In 2019, the industry was worth $118 billion, making it nearly as valuable as Canada's lucrative mining, oil, and gas industries ($119 billion).[19] A key driver of this growth is data. Both public and private organizations are investing considerably in technology research and products that leverage innovations in advanced analytics, algorithms, and artificial intelligence (AI) to understand how best to collect and process data. This prospecting in the digital economy has led to data being described as "the new oil".[20]

However, unlike oil, data are limitless. Every observable aspect of the world, including those observable aspects of a person's life, can be assigned a data point. A data point makes its way through the data lifecycle where it is created or received, processed, used, and transferred, among other stages (See Figure 1).[21] Organizations derive value from this lifecycle by recording those observable data points, structuring them for analysis, and then inferring insights to inform outputs. This information value chain can constantly be fed new information, as people produce new data every moment of their lives. Moreover, the sum of data is of greater value than their parts, leading to strong incentives for all actors to use and aggregate data intensively.[22]

Figure 1 - The Data Lifecycle



Source: World Bank, 2021

Another positive attribute of data is their excludability. Organizations can process and store information about people, places, and things in ways that are inaccessible to others, giving them a unique advantage in competitive environments. While current markets for data are underdeveloped, making the value of data assets difficult to ascertain, data's ubiquity, combined with its excludability, and known and unknown potential explain the global rush for data across the public, private, and even not-for-profit sectors.[23]

The most prominent examples of the known potential of data come from developments in big data analytics and AI. Big data analytics is the process of pooling and cleaning massive amounts of data, often from disparate sources, to extract actionable insights about people.[24] E-commerce companies such as Amazon use big data analytics to process information on names, addresses, purchase history, and user activity to provide targeted recommendations for products to consumers and they also use this information in concert with data from their warehouse operations to ship orders efficiently.[25] AI takes analytics further by contextualizing data, supporting decision-making about people based on patterns, and generating content.[26] Popular language models such as ChatGPT generate text based on training from vast amounts of text data from the Internet, while AI image generators such as Midjourney create original images based on training from existing image data.[27]

As with technological advancements of the past, political agents have also taken advantage of the benefits of analytics and AI, using personal information to improve fundraising campaigns and influence voting intentions.[28] Nonprofits can also benefit from these tools by using data to drive fundraising efforts, transform reporting, and improve program administration.[29]

Canadian Digital Privacy Challenges

While innovation in the digital economy has and will continue to drive economic value and competitive advantages in business and politics, it also deals with personal information. Personal information does not only have economic value, it also has value inherent to a person's privacy. Canada's digital privacy challenges as they concern personal information include the use of personal information in the private sector, diminishing levels of trust in the digital space, privacy harms faced by individuals, and shifting global policies.

Privacy in the Context of Private Sector Operations

Canada's commercial privacy law includes basic tenets of respecting privacy such as obtaining consent, minimizing data collection, and safeguarding personal information.[30] In recognition of people's desire for privacy, some organizations have attempted to go beyond the basic legal requirements for privacy protections. Some have deployed privacy-enhancing technologies such as data de-identification and synthetic data and have employed strategies such as "Privacy by Design", a concept developed by Ontario's former Information and Privacy Commissioner, Dr. Ann Cavoukian.[31] Nevertheless, these practices are not universal, and some privacy-enhancing technologies have proved fallible in effectively protecting personal information.[32]

Despite provincial and federal privacy laws that uphold the role of consent and the safeguard of personal information, a 2023 survey of business leaders conducted by PricewaterhouseCoopers revealed that 46% of Canadian respondents sometimes use customer data without express consent and 49% do not always vet the third parties with whom they share their customer's data.[33] Another survey conducted by Canada's privacy ombuds, the Office of the Privacy Commissioner of Canada (OPC), showed that business awareness of responsibilities under Canada's federal

privacy law has decreased since 2019, with only 52% of businesses highly aware of their duties under the law. Additionally, the likelihood of having a privacy policy increases the larger a business is – 79% of large businesses surveyed noted having such a policy, compared to 60% of small businesses.[34]

Stakeholders noted that small and medium-sized enterprises (SMEs) in particular face challenges in balancing innovation with complying with privacy law. They shared that SMEs tend to find that there is a lack of clarity around which jurisdiction's privacy law applies to them and they do not understand how to take advantage of the promise of data analytics without breaking the law. Further, many stakeholders perceived the OPC as lacking in the requisite technical expertise to understand changes in the digital space and as being unresponsive to developing a dialogue with businesses, indicating opportunities for increased stakeholder engagement.

Role of Trust in the Digital Economy

A key challenge for organizations in the Digital Age is building trust. Trust plays a crucial role in the economy as it reduces transaction costs, increases efficiency gains, and is a determinant of economic development and wellbeing. In the digital economy, one of the main components of trust is privacy. People generally expect that information they share about themselves will be used for the purposes that they have identified and that any other information that is discerned about them will be used in a fair and appropriate manner.[35] However, Canadians do not necessarily trust organizations to respect their privacy and they remain concerned about their lack of control over their data. In a 2023 survey conducted on behalf of the OPC, 39% of individuals believed that businesses respect their privacy rights, a decline from 45% in 2020. This mistrust is further characterized by most Canadians who are uncomfortable with having their face scanned to verify their age online (65%) or their voice used to verify their identity (61%).[36] In a survey commissioned by Interac earlier this year, 74% of Canadians expressed that they would like more control of their online information.[37] Unlike data, trust is not ubiquitous in the digital economy.

One example of the central role of trust in the digital economy is the development of smart cities, particularly in liberal democracies. Smart cities rely on data to provide a better quality of life for inhabitants and include benefits such as the reduction of crime rates, shortening of commutes, and reduction of carbon emissions.[38] When Barcelona sought to become a smart city, it empowered residents to design methodologies for the collection and sharing of data from sensors in their neighbourhoods, allowing residents to realize a key aspect of privacy rights: control of one's data.[39]

By contrast, Toronto's own smart city pilot project, a collaboration between Sidewalk Labs (a subsidiary of Google) and a Canadian Crown Corporation, was plagued with concerns from citizen interest groups, technology advocacy groups, and former partners of the project for a multitude of reasons. Some of these concerns centered around the creation of a new class of data called "urban data". This classification referred to images or information from public and semi-private spaces and its definition attempted to distinguish it from personal information, leaving the data unaddressed by Canadian privacy laws.[40] Additionally, while the company initially emphasized

the role of de-identification of data at the source, its position evolved to state that while Sidewalk Labs would strip personal identifiers of individuals, it would not guarantee that third-party organizations participating in the project would do the same.[41] While Sidewalk Labs cites the pandemic as the cause for its cancellation of the project, the company has not since attempted to launch another smart city project.[42] The project is widely understood to have failed in developing social acceptance and trust, crucial components of a data-enabled city.[43]

Privacy Harms in the Digital Age

A breakdown of trust is not the only kind of harm that can arise in the Digital Age. The digital space can recreate systems of oppression with a disproportionately harmful effect on marginalized groups. For example, contact tracing through digital apps, while intended to guarantee public health safety during the pandemic, sparked fears among traditionally marginalized communities.[44] These groups have historically faced discrimination and stigma in the face of epidemics, as evidenced by authorities' targeted criminal sanctions of marginalized communities during the HIV epidemic. Similarly, the collection and publication of the location of COVID-19 outbreaks sparked racial, religious, and xenophobic tensions, creating a lack of safety for these groups.[45] To understand how privacy harms in the Digital Age manifest, it is important to analyze how the information value chain replicates current structures of oppression, starting with the collection of data.

Overcollection of data increases surveillance of traditionally marginalized groups

Racialized communities are disproportionately surveilled and data-driven technologies exacerbate this experience.[46] In the United States, private companies partner with local and state police and intelligence agencies to share data and surveil residents.[47] Canada has started to explore similar surveillance partnerships. The Royal Mounted Canadian Police (RCMP) was caught using Clearview AI's facial recognition technologies for surveillance.[48] Clearview AI had contravened privacy law by collecting biometric data without consent.[49] By using Clearview's technology, the RCMP was also in contravention of the law because it collected more information than was necessary to carry out its operations.[50] This kind of overcollection of data can lead to "big data discrimination", a phenomenon composed of increased surveillance, over-policing, and discrimination by design.[51] Activists have raised concerns that technologies such as those from Clearview AI will contribute to the overpolicing of Black and Indigenous people, given that they are built from data focused on people from these communities.[52] Furthermore, these technologies are often inaccurate as they concern racialized people, creating additional risks wherein people are misidentified for crimes.[53]

Data processing can cause discrimination against entire groups

Using data to enhance products and services has several unintended consequences. For years, Facebook had allowed users to be targeted by ads according to their interests which inadvertently revealed information such as race, ethnicity, and sexual orientation. Advertisers had used this information to intentionally exclude people from receiving targeted housing ads based on their race.[54] Additionally, a case study on "data mining", a process for identifying patterns in data, showed that the process can identify features of individuals and groups that they did not

specifically disclose about themselves. Inferences and labels, which are not always accurate, can be drawn from behaviour online, such as location data or spending habits.[55] Consequences of inaccurate inferences include losing jobs, government benefits, and loans.[56] Certain data analysis software labelled low-income welfare applicants as "lazy" and identified them as high-risk candidates for welfare benefits, leading to the eventual denial of benefits.[57] Likewise, an investigation conducted by ProPublica found that algorithmic software used by American courts were nearly twice as likely to inaccurately label Black defendants as likely to commit a future crime, compared to White defendants.[58]

Data collection and processing can put civil and political rights at risk

In 2018, the New York Times broke the story of the Cambridge Analytica-Facebook scandal. When Facebook users gave permission to an app to access their Facebook profiles to fill out a quiz, the app harvested the information of the users and their friends. In total, the app gathered information from 87 million individuals around the world. The company Cambridge Analytica then used the personal information from the quiz and from individuals' Facebook accounts to generate psychological profiles on voters. These insights were sold to political operatives, enabling campaigns to target millions of users using private, personal information and allegedly swinging votes in the Brexit referendum and American presidential election of 2016.[59] Improper data collection and processing can be wielded to manipulate voters, placing democratic rights and institutions at risk.

Global Policy Shifts

To date, 137 countries have adopted data protection and privacy legislation.[60] Jurisdictions similar to Canada have moved swiftly on updating their privacy laws in the face of challenges of the Digital Age. Examples of recently updated laws that are relevant for Canada come from the European Union (EU), California, and Quebec.

European Union

The *General Data Protection Regulation* (GDPR) was passed in 2016, replacing the *Data Protection Directive* of 1995.[61] The new regulation established a new set of rights, such as the right to erasure (the ability to ask an organization to delete your personal information) and the right to data portability (the ability to transfer your personal information from one organization to another), created clear rules for businesses (including severe monetary penalties for the violation of privacy laws), and enables the free movement of personal data within the EU.[62] The push for legislative change was sparked by Max Schrems, an Austrian lawyer and data rights activist, who started the Europe v Facebook movement. From 2011 to 2017, the movement built a case for privacy and data rights, which were later articulated in the GDPR.[63]

California

Adopted in 2018, the *California Consumer Privacy Act* (CCPA) was designed to increase data protection obligations for businesses and enshrine new privacy rights for Californian consumers.[64] The CCPA gives consumers greater control over their personal information and establishes a new set of privacy rights, such as the right to opt out of the sale of one's personal information.[65] The

effort for new legislation was spearheaded by Alastair Mactaggart, a San Francisco real estate developer and investor, who funded and championed a similar bill after learning the extent to which Google collects information on its users.[66]

Quebec

The Act to Modernize Legislation Provisions Respecting the Protection of Personal Information, or, Law 25, was adopted in Quebec in 2021. Law 25 updates rules for the protection of personal information.[67] It introduces stricter requirements for privacy, including enhanced transparency, protections, and new consent provisions for Quebec organizations, with significant fines and increased powers for the privacy supervisory authority, the Commission d'accès a l'information.[68] This policy change was heavily inspired by the GDPR and the desire to adopt best practices for personal information protection in Quebec.[69]

Canadian legislation must keep pace with international standards for privacy protection to ensure the uninterrupted flow of trade as it concerns the cross-border transfer of data. Canada has enjoyed limited "adequacy status" from the EU, meaning that the jurisdiction recognizes that Canadian law provides protection equivalent to EU law as it concerns the personal data of Europeans.[70] Granted in 2001 and reaffirmed in 2006, this adequacy status is restricted to organizations governed by Canada's commercial privacy law.[71] The EU Commission is currently reviewing the adequacy of Canada's legislation in the face of the GDPR of 2016.[72] Bill C-27, the federal government's proposed commercial privacy law, presents an opportunity to maintain Canada's adequacy status, ensuring that personal information can continue to flow between Canada and the EU, and aligning Canada with other jurisdictions.[73]

Canada's Policy Landscape

Privacy Protections Under Federal Law

The Personal Information and Protection of Electronic Documents Act

The *Personal Information and Protection of Electronic Documents Act* (PIPEDA*)* is Canada's privacy law governing the use of personal information in commercial contexts. Passed in 2000, PIPEDA was developed to build consumer trust in e-commerce and to allow Canadian businesses to compete in the digital economy.[74] The legislation provides rules around the collection, use, and disclosure of personal information through an emphasis on the role of consent. Pursuant to section 6.1 of the statute, consent is only valid if people can be reasonably expected to understand what they are consenting to.[75]

A core aspect of PIPEDA is Schedule 1 of the legislation. The Schedule describes ten core principles for the protection of information, expanding on the meaning of consent, explaining how organizations should identify the purpose of the use of data, and providing limitations on the indiscriminate collection of data.[76] The inclusion of these principles into the law is reflective of the crucial role that businesses and other organizations played in the development of PIPEDA. The Schedule originated from the Canadian Standards Association, a voluntary standards group composed of representatives from industry, government, and academia, and was incorporated

as a whole into legislation. Its adoption has allowed for a flexible compliance regime that is principles-based and technologically neutral.[77]

The law applies to all private sector organizations across Canada using personal information for commercial purposes, unless a province or territory has a substantially similar privacy law, and the personal information does not cross provincial or national borders. The federal government has deemed the following provinces as having substantially similar privacy laws: Quebec, Alberta, and British Columbia. The law also applies to all federally regulated organizations, irrespective of which province they operate in.

The Office of the Privacy Commissioner of Canada

The OPC is Canada's federal privacy oversight body, responsible for overseeing compliance to the *Privacy Act* (privacy law applicable to the federal public sector) and PIPEDA.[78] In 1983, the federal government established the OPC to address the limitations of legal proceedings against the government under the *Privacy Act*. Namely, the formality and cost of court procedures can make justice inaccessible for many complainants, so the government opted to create an ombuds to resolve issues in an informal manner.[79] The ombuds model is a Swedish institutional concept whereby an ombuds receives and investigates complaints from the public and completes a non-binding review of an organization's practices. An ombuds typically has no enforcement powers.[80] The duties of the OPC were extended to the commercial sector in 2001 when PIPEDA came into force.[81]

Where it concerns the commercial sector, the OPC has a mandate to promote public understanding of privacy law, promote compliance with PIPEDA, investigate privacy complaints from the public, initiate complaints and investigations itself, enter into compliance agreements, and report on its activities annually to the Parliament of Canada.[82] Its public education initiatives include participation in national and international privacy awareness campaigns and online resources for the general public, children, youth, and seniors.[83] Its guidance to businesses includes such online resources as well; however, the OPC also has dedicated staff to a Business Advisory Directorate that conducts outreach and advisory activities. The Directorate provides advice to businesses that seek to understand the privacy risks of their activities and initiated 14 new advisory activities in the 2021-22 reporting year.[84]

The OPC conducts investigations into businesses if it has received a complaint from a member of the public, if it has reason to believe the business has contravened PIPEDA, or if it has identified a high-risk issue. If the Commissioner believes that the case can be resolved without a formal investigation, it will go through an early resolution process where the issue is mediated.[85] If the case remains unresolved, it will go through a formal investigation, whereby the investigator will inform the organization of the substance of the complaint, gather evidence, consult on the issue internally, and provide their findings in a report to the organization and the complainant. If the investigator finds that an organization has contravened PIPEDA, they can make non-binding recommendations to the organization. If the organization does not follow the recommendations, the OPC can file an application with the Federal Court to order the organization to correct its practices. The Court can also award damages to complainants.[86]

Privacy Law Outside of Commercial Use

The *Canada Elections Act* provides guidelines on the use of personal information in the electoral process. It primarily refers to the information collected by Elections Canada to maintain the Register of Electors for the production of lists of electors, their distribution to those involved in the electoral system, and the use of that information by recipients.[87] These recipients are typically political parties that use various kinds of information management systems for voter management. Data collected by political parties often goes beyond voter lists, as the voter list is aggregated with information that the parties document on individuals' past and present political views, demographic and cultural information, and propensity to support or oppose the party.[88]

Addressing Gaps in Current Privacy Law: Bill C-27

The federal government has introduced Bill C-27, the Digital Charter Implementation Act, to replace PIPEDA.[89] Bill C-27 has three parts: The Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act (AIDA).[90] The CPPA aims to enhance privacy protections in the Digital Age. It would repeal and replace the parts of PIPEDA focused on privacy protections with additions that would raise the consequences for non-compliance by instituting new monetary penalties for non-compliance, expand individuals' eligibility for filing claims and requesting compensation, and include provisions for quasi-criminal prosecutions.[91]

The CPPA would also require private actors to provide explanations to individuals regarding how automated decisions concerning the individuals were made. The legislation retains the consent-based model of PIPEDA and seeks to expand rules around consent, as it concerns withdrawal, deletion and anonymization, additional grounds for collection and use without consent, and data transfer requests. Finally, the CPPA will expand the OPC's role with regard to compliance promotion, by enabling it to issue orders to non-compliant organizations. PIPEDA's provisions regarding electronic documents will remain as the *Electronic Documents Act*.[92]

The second part of Bill C-27 is the *Tribunal Act.* The *Act* would add a new administrative tribunal that would hear appeals of OPC orders and it would be the body responsible for issuing monetary penalties as described under the CPPA.[93] AIDA is the third part of Bill C-27 and it focuses on adding measures to regulate interprovincial and international trade and commerce related to AI systems.[94] AIDA would also require common measures for the design, development, and use of AI systems and provisions requiring protections to lower the risk of AI-related harms and encoded bias.[95] Finally, AIDA includes provisions prohibiting AI practices that may result in significant harm.[96]

Limitations of Federal Law and Policy

Sensitive Information

Personal information, and more specifically, sensitive information, is central to the realization of human rights. According to the OPC, "information that will generally be considered sensitive and

require a higher degree of protection includes health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious or philosophical beliefs."[97] The OPC considers this information sensitive because if it is exposed, it poses risks to safety and can cause long-term reputational and emotional harm.[98]

The legislation does not adequately recognize these risks or provide sufficient requirements for this type of information. Section 4.3.4 of PIPEDA states that consent may vary based on the circumstances and type of information.[99] Specifically, organizations are encouraged to take the sensitivity of information into account, depending on the context.[100] Bill C-27 applies retention periods specifically to sensitive information and considers children's personal information sensitive.[101] However, the legislation lacks clarity with regards to what sensitive information is, making it difficult for actors to know what kind of information should be considered sensitive. While the OPC provides an interpretation of sensitive personal information, it is not binding.[102] In a Submission to the House of Commons' Standing Committee on Access to Information, Privacy and Ethics (ETHI) on a previous iteration of the *Digital Charter Implementation Act*, the OPC also recommended that the legislation provide a definition of sensitive personal information that is context-specific and includes an explicit and non-exhaustive list of examples.[103] The OPC has maintained this recommendation in its submission to ETHI for its review of Bill C-27.[104]

PIPEDA recognizes that the level of sensitivity of personal information is context-dependent because there are cases where information can become sensitive.[105] However, it does not specify criteria for data that require a heightened standard of care, such as biometric data.[106] Bill C-27 requires that private actors consider the level of sensitivity when considering various requirements like how long to retain data.[107] However, the legislation does not provide a specific definition of what information should be considered sensitive or guidance as to different levels of sensitivity.[108] Without specification, private actors are left to decide the level of protection they provide.

To ensure clarity in determining what information should be considered sensitive and the level at which it should be protected, other jurisdictions such as the EU and Quebec have defined and tiered sensitive information. The GDPR defines sensitive information as follows: "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[109] The law requires explicit consent for the processing of sensitive information, unless the information is necessary for fulfilling one's employment requirements or it is part of a collective agreement. It also clarifies that sensitive data such as health data requires a higher level of protection, along with limitations on what health data can be used for. Additionally, the law only allows the processing of data related to criminal offenses and convictions to be performed by a relevant authority.[110]

Non-Commercial Actors Responsible for Personal Information Protection

Elections Canada publishes guidance for the use of personal information from the Register of Electors. The guidelines include sample declarations for lists distributed to Members of Parliament, political parties, and candidates. The guidelines also advise on the use, safeguarding,

and disposition of the lists, and include a list of frequent asked questions and best practices.[111] Nevertheless, Elections Canada does not have the legislative authority to verify if political parties applied the guidance while processing the personal information from the Register. Additionally, while most of the fair information principles listed in PIPEDA are also in the Canada Elections Act, the principles apply primarily to information obtained from the Register of Electors. This presents a gap in the regulation of political parties' collection, use and disclosure of personal information from other sources.[112]

Non-profit organizations and charities also collect a large amount of personal information, but their regular activities are not governed under PIPEDA, as they are not engaged in commercial activities. There is increasing stakeholder awareness and expectations around privacy, transparency, and accountability. Donors, clients, and other stakeholders expect charities and nonprofits to safeguard their personal information, protect it from misuse and be transparent and accountable for how it is used.[113] Though charities and not for profits are expected to adhere voluntarily with PIPEDA, they cannot be legally held accountable under the current federal law. Some provinces (e.g., British Columbia and Quebec) have laws that govern non-commercial actors, such as non-profits.[114]

Gaps in Data Processing Governance

PIPEDA does not govern the use of de-identified or anonymized data. Deidentification is the process of removing personal information from a record or data set, while anonymization of data is a process through which data cannot be linked to identifiable information. De-identification and anonymization are promoted as privacy-enhancing technologies that drastically reduce the risk of personal information being used or disclosed for unauthorized or malicious purposes.[115] These methods help data sharing, while preserving privacy and enable data use by third party processors. [116]

In recognition of the role and value of de-identified and anonymized data in the protection of personal information, Bill C-27 seeks to acknowledge these methods of privacy enhancement in the law. The proposed legislation includes and distinguishes between de-identification and anonymization and it generally[*] does not allow for the re-identification of personal data.[117] However, once information is considered de-identified or anonymized, it is no longer considered to be personal information, and is therefore not governed. This allows the information to be shared, sold, and freely used, without regulation.

Leaving de-identified information to be unregulated presents a risk to the protection of personal information because de-identified data can be re-identified using emerging technologies. For example, health records of patients are de-identified to maintain privacy, but they can be re-identified by combining identifiers with other sources such as databases that contain information on car accidents or illnesses.[118] In another case, researchers at Imperial College London were

[*]Except for security safeguards, compliance under federal or provincial law, testing of fairness and accuracy of models, processes and systems developed with de-identified information or any 'other prescribed circumstance'.

able to accurately reidentify 99.98% of Americans in an anonymized dataset using a machine learning model and datasets that included up to 15 identifiable characteristics such as age, gender, and marital status.[119] This re-identification has important implications for commercial data use. Namely, data brokers can obtain de-identified data from pharmacies, private drug insurers or private clinics, for example, without consent from patients. These datasets can be sold and reidentified to identify physicians and enable companies to market directly to physicians, influencing the volume of drugs prescribed, the quality of prescriptions, and cost increases.[120]

Support for Small and Medium-Sized Enterprises and Not-for-Profit Organizations

In a survey conducted for the OPC in 2022, only 66% of medium-sized businesses and 58% of small businesses reported having a privacy policy compared to 79% of large businesses who reported having a privacy policy.[121] Research funded by Public Safety Canada suggests that as it concerns privacy, many SMEs "hope for the best until they have a breach" and the OPC has already expressed concern that SMEs may be underreporting privacy breaches.[122] Smaller not-for-profit organizations (NPOs) are also increasingly becoming vulnerable to digital privacy threats and many work with information that could risk people's safety and wellbeing if revealed. Similar to SMEs, NPOs lack the capacity to employ the level of expertise and resources required to adequately protect personal information, making them vulnerable to data breaches.[123]

In recognition of the supports required to establish an effective compliance promotion regime, the OPC provides privacy advisory services to businesses, albeit with limited capacity. The OPC offers its services to businesses that are already operational and those that are looking to launch. In some cases, the OPC approaches businesses proactively to offer them advisory services.[124] There is no designated advisory directorate providing specialized support to SMEs and NPOs. In the 2021-2022 reporting year, the OPC conducted 18 advisory engagements with businesses, compared to 105 advisory consultations with federal government organizations.[125] Publicly available headcount information suggests that the OPC's Business Advisory Directorate is comprised of approximately 7 employees while the Government Advisory Directorate is comprised of approximately 13 employees.[126]

Outdated Enforcement Model

When PIPEDA was adopted, privacy regulation did not feature highly visible conflicts with non-compliant actors, which, according to former Privacy Commissioner Jennifer Stoddart, likely influenced policymakers' perception that disagreements in personal information management practices were best dealt with in a context that fostered open dialogue and education.[127] The ombuds model has been relatively effective at contributing to this. In the 2021-2022 reporting year, the OPC resolved 85% of its cases through early resolution.[128] However, as organizations seek to derive value from data in more unconventional ways, and as large, global organizations with a reduced incentive to cooperate with the OPC move to Canada, the Commissioner will continue to see an increase in complaints, but without adequate enforcement tools if the law remains the same.

The process to hold non-cooperative organizations accountable is out of the control of the OPC, extensively slowing down compliance enforcement efforts. The average PIPEDA investigation

takes approximately eight months to complete.[129] If the OPC would like to order an organization to comply with its recommendations or issue a penalty for non-compliance, it must file an application with the Federal Court.[130] The Court would hear the case "de novo", meaning that it would consider the issue as new and provide no deference to the recommendation of the Privacy Commissioner.[131] This contrasts with approaches that defer to an administrative body for decisions regarding orders and penalties.

The division of enforcement powers between the OPC and the Federal Court has led to a lengthy and inefficient regulatory process, especially when compared to similar jurisdictions. In the OPC's attempt to hold Facebook accountable for the Cambridge Analytica scandal, the Office took one year to conduct its investigation and the Federal Court took three years to decide on the OPC's application. Overall, the case took over five years from the complainant's notice to the OPC in 2018 to the decision made by the Federal Court in 2023.[132] Comparatively, the United States' Federal Trade Commission also took one year to investigate Facebook for the Cambridge Analytica scandal; however, the Commission issued a US$5 billion penalty shortly thereafter.[133] Other jurisdictions that empower their data protection authorities to make decisions around orders and/or penalties include provinces such as Quebec, Alberta, Ontario, British Columbia, and Prince Edward Island, along with other national common law jurisdictions such as the United Kingdom (UK), New Zealand and Ireland.[134]

Towards a Human-Rights Based Approach to Privacy Policy

PIPEDA currently emphasizes supporting and promoting electronic commerce and does not take impacts on human rights into account. Privacy is a right in and of itself and is a gateway to realizing other rights. Human rights are considered fundamental because they are inherent to all human beings irrespective of one's gender, colour, religion, race, or any other factor. They are intrinsically connected and cannot be viewed in isolation because the enjoyment of one right depends on the enjoyment of the other right. [135] Multiple stakeholders have stated that privacy acts as a gateway for other rights. For example, the right to vote, a democratic right, is connected to the idea of a secret ballot that is based on the core principle of privacy.

Canada's privacy regime requires a human rights-based approach (HRBA) to protect people from the risks and threats privacy infringements pose to their rights. According to the United Nations, an HRBA to policies, plans, and processes are rooted in the protection of "civil, cultural, economic, political and social rights", and human rights principles.[136]

Canada is equipped with international and federal legal instruments which provide a justification for taking an HRBA to privacy. In 1976, Canada ratified the International Covenant of Civil and Political Rights (ICCPR), a legally binding treaty requiring countries to recognize and protect civil and political rights. Article 17 of the ICCPR states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[137] Additionally, Section 8 of the *Canadian Charter of Rights and Freedoms* has been interpreted by the courts as imposing an obligation on political actors to ensure that legislation is enacted to secure the privacy interests of individuals.[138] The federal

Privacy Act, which details the responsibilities the government has to protect the privacy of individuals, has obtained quasi-constitutional status, which allows for a broad interpretation of the law in favour of rights.[139]

An HRBA to privacy policies begins with two key pillars and accompanying recommendations for Canada's privacy policy landscape:

1. *Information as inherent to personhood*

Canada's privacy regime needs to center the person and their rights in data protection policies. This paradigm recognizes that strong protections for data means strong protections for people's rights and their dignity. In its preamble, Bill C-27 acknowledges that protecting privacy is critical to the "individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada".[140] The OPC is keen to recognize privacy as a fundamental right in Bill C-27 and has recommended doing so as recently as May 11, 2023.[141] Now, the federal government needs to take steps to create legislation that moves beyond acknowledgement and towards compelling action. This paradigm shift should also recognize the responsibilities that organizations that handle data have in the Digital Age. The power, knowledge, and control organizations have over people's data creates asymmetries between people and organizations.[142] As people entrust a wider range of actors with their information, a greater onus must be placed on these organizations to develop stronger safeguards for personal information protections.

The first recommendation focuses on raising the level of responsibility for private actors by changing the legislative and regulatory landscape to specify new standards for protecting personal information and by ensuring that all actors handling data have a responsibility to protect information.

2. *Accountability and inclusion foster trust*

An HRBA calls for accountability and respect for the rule of law, especially as it concerns harm to individuals. It also respects the dignity and diversity of individuals by including their perspectives in decisions affecting them.[143] This approach has been central to building trust in situations of conflict, journalistic freedoms, and scientific development.[144] In the case of privacy, the COVID-19 pandemic revealed that a deficit of institutional trust, specifically in how institutions would use personal data, created challenges in increasing people's participation on contact tracing apps.[145] Only 56% of Canadians reported they would use contact tracing apps and 73% cited the invasion of privacy as a reason not to install apps.[146] Engaging with affected Canadians is critical to building trust in organizations and advancing a privacy regime that protects their rights. Canada also needs to create a regulatory environment robust enough to ensure accountability, a critical element of maintaining trust. This includes reasonable supports to enable organizations to fulfil their obligations and ensure they are taking adequate measures to mitigate risks to rights infringements.[147]

The second recommendation introduces three key policy actions: an advocacy initiative from the private sector focused on elevating Canadians' perspectives on digital privacy as a human right,

a government body focused on building capacity for SMEs and NPOs, and a system of penalties for dealing with contraventions with the law.

Recommendation 1: Raise the Level of Responsibility for Private Actors

Interac should advocate for an HRBA to legislation, recognizing that data is inherent to personhood. Treating personal information as an object that can be traded for products and services creates a system which disregards the inherent "humanness" of data. When personal information is described as the "new oil", it renders it "abstract, inert and non-human".[148] Personal data is not something a person possesses; it plays a fundamental role in who they are as a person and who they can become.[149] Protecting that personal information is crucial to preserving human dignity, as recognized by Canada's highest court. In the Supreme Court of Canada case *R. v. Dyment,* a doctor shared a patient's blood sample with the police without the consent of the patient. The Court ruled that informational privacy is included in the right to privacy and specified that **privacy protects individuals' dignity and integrity**.[150] The following recommendations focus on heightening the level of protections to people's information by providing additional protections for sensitive information and improving the governance of data processing.

1.1 Safeguarding Sensitive Information

Defining Sensitive Information

Effectively safeguarding sensitive information begins with a clear definition within the legislation. Some jurisdictions, including Quebec, the UK, and the EU define sensitive information.[151] The OPC has also recommended that the CPPA should establish a general principle of sensitivity with an open-ended list of examples.[152]

The GDPR provides the most prescriptive and robust definition of personal sensitive information, listing all information that is considered sensitive including "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[153] This definition serves as an example of a prescriptive definition that Bill C-27 can draw inspiration from. To ensure that a definition of sensitive personal information is effective and captures the nature of sensitive personal information in a Canadian context, it is recommended that far-reaching consultations and research are conducted to develop a definition that will be helpful and applicable.

Raising the Standard of Sensitive Information Processing

Not all sensitive personal information has the same level of sensitivity or potential for harm. As such, Bill C-27 should specify a tiered approach to sensitive information that would require private actors to take a differential approach to providing protections. Law 25, the GDPR, and the UK's GDPR and Data Protection Act, treat sensitive information with a tiered or specialized approach.[154]

This addition to Bill C-27 should retain flexibility to determine sensitivity of information based on context. However, some information should remain highly sensitive, regardless of context. For example, the GDPR specifically identifies genetic, biometric and health data as special categories of personal data that merit further processing regulations developed by Member States.[155] Similarly, the UK's GDPR and Data Protection Act specifically identifies data which are subject to additional safeguards.[156] It considers identity-based information such as race, ethnicity, religion, biometric data, etc. to be the most sensitive data due to "significant risks to the individual's fundamental rights and freedoms", depending on the use of the data.[157] While financial information is also sensitive, it does not receive a similar carveout in the law because it does not have the same risks to fundamental rights.[158] Quebec's Law 25 requires express consent for the use of sensitive personal information and the law may also apply differently to different cases of sensitive personal information.[159]

By operating according to a tiered system of sensitivity, the standard by which private actors are required to protect digital privacy can be raised. A tiered approach to sensitive personal information places the onus on private actors to ensure the most stringent protections are given to the most sensitive information. It is recommended that far-reaching consultations and research are conducted to develop provisions and consequences for each tier. The recommended tiers are as follows:

1. High level of sensitivity: Biometric and Health Data
    a. Biometric data is any data that uses physical characteristics and biological measurements to identify people digitally. Biometric data includes but is not limited to facial recognition, fingerprints, iris recognition, palm recognition, and any DNA based recognition.[160]
    b. Health data is any information pertaining to an individual's medical records, history, medical conditions, and any other related information.

2. Medium level of sensitivity: Identity-Based Characteristics, Location-Based Information, and Financial Information
    a. Identity-based characteristics include but are not limited to race, ethnicity, religion, sex, gender identity, sexual orientation, age, ability, and socioeconomic status.
    b. Location based information includes but is not limited to location tracking, home address, school, and workplace.
    c. Financial information.

3. Low level of sensitivity: General Personal Information
    a. General personal information includes but is not limited to name, email address, phone number, and social media account names.

To enforce this standard of care, Bill C-27 should introduce a tiered administrative monetary penalty system, which penalizes non-compliance. Further details are outlined in section Recommendation 2.3 Enforcing the Law.

Textbox 1. Treating minors' information as sensitive

Minors' privacy is particularly vulnerable in the Digital Age. Children are often not aware of or privy to knowledge around terms and conditions and research finds that young people have limited knowledge of business practices regarding the use of information for commercial purposes. Additionally, children often lie about their age, exposing them to an unregulated digital media environment.[161] Such an environment can enable the targeting of children with manipulative content that can influence behaviours and the physical, mental, and emotional wellbeing of children.[162]

PIPEDA has no specific provisions for protecting the privacy rights of minors.[163] Bill C-27 makes mention of minors, stating that their personal information is considered sensitive. It specifies that requests can be made to dispose of personal information if they are in relation to a minor.[164] Recognizing the harms faced by children online, the UK and the US have taken legislative action to promote their privacy. The UK Parliament incorporated the Children's Code into the *Data Protection Act* in 2020. The Code provides 15 standards for the use of children's information, including standards around profiling, the use of nudge techniques, and considerations for the best interests of the child.[165] In the United States, the Children's Online Privacy Protection Rule places restrictions on websites and providers that cater to minors under the age of thirteen or websites and providers that are aware they are collecting data from children under the age of thirteen.[166] Further policy analysis should be undertaken to identify measures appropriate for the Canadian context.

1.2 Fill in the Governance Gaps

1.2.1 Non-Commercial Actors

International treaties already recognize that obligations for the respect for human rights are not limited to government and business. Considering the extensive amount of personal information processed in non-commercial contexts, Bill C-27 should extend privacy protections to activities conducted by not-for-profits, political organisations, and other similar non-commercial actors. Such an extension and application of the law would need to be balanced with other rights and freedoms such as the freedom of expression and the freedom of the press, to ensure that other pillars of Canada's democratic society are upheld.

1.2.2 Governing Data Processing and De-identified and Anonymized Data

A. Legislative changes

Specify "processing" of data in Bill C-27

As the use of AI and similar technologies becomes more prevalent, the understanding of the term "processing" becomes increasingly significant, as it forms the basis for data analysis and complex decision making. Processing refers to a collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal).[167] PIPEDA only focuses on the collection, use, and disclosure of data and does not clearly indicate the other activities that comprise processing.[168] Explicitly defining processing would ensure that a comprehensive set of activities are covered within the ambit of the law and leave little room for ambiguity. Other privacy legislation such as the GDPR defines processing, allowing for a broader coverage of activities such as the organization, structuring, storage, adaptation or alteration, alignment or combination, restriction, and erasure or destruction of personal data, among others.[169]

Governance of anonymized and de-identified data

Bill C-27 defines anonymization as a process to "irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means".[170] A set of regulations are needed to provide uniform guidance on managing personal and sensitive information when de-identified and anonymized information.

B. Regulatory Changes

Meet global standards for de-identification

Bill C-27 does not specify standards for de-identification or anonymization. It only states that actors should adhere to "generally accepted best practices", leaving room for interpretation of what constitutes best practice. The Government of Canada should provide regulatory guidance for anonymization and de-identification that are inspired by the latest standards of the EU, the UK and the recently introduced International Standards Organization (ISO) standard on de-identification. The latest standards in ISO/IEC 27559:2022 mitigate de-identification risks associated with the lifecycle of de-identified data that is applicable to all types and sizes of organizations.[171]

Adopting global standards would provide a strong basis for the development of national and international regulation, helping to save time and reduce barriers to do business and other operations and results in an engagement with privacy experts and industry. Given the highly technical nature of the space, Canada should incorporate ISO's new data standard for de-identification into its regulatory framework. The government should conduct this through an ambulatory incorporation by reference. This mechanism would allow a document that may change and that is not in the text of the regulations to be considered a part of the regulations, allowing for faster and more relevant changes to regulatory requirements.[172]

Implementation Considerations

Timeline and Costing

Bill C-27 is currently undergoing study in the House of Commons Standing Committee on Industry and Technology and can be expected to take at least six more months until it is reported in the

House of Commons.[173] Considering the implications and challenges associated with the fast-paced digital space, Parliament is expected to study Bill C-27 further in relation to the online harms bill (Bill C-11). Additionally, the review of Canada's adequacy status in relation to the GDPR could put an accelerated timeline on the passing of the bill. Ultimately, legislative changes could take approximately 2 years to come into force and could take longer if an election is called prior to the fixed election date of October 2025.[174]

If the development of regulations under the *Consumer Privacy Protections Act* follow the same process of the development of regulations under the *Artificial Intelligence and Data Act (*both are components of Bill C-27), the development and assessment timeline of the proposed regulatory changes could require at least six months for consultation on regulations, one year for the development of draft regulations, three months for consultation on draft regulations, and three months for the initial regulations to come into force.[175] This could not be expected to be completed before the Parliament is dissolved in the next federal election.

The cost of studying and implementing the legislative changes around sensitive information and the inclusion of data processing governance provisions would be funded through existing financial resources.

Stakeholder Analysis

Political parties and not-for-profit organizations whose primary activities are largely unregulated may push back on compulsory privacy requirements, arguing that they lack the resources to comply or that they already voluntarily follow existing privacy law. For instance, when the B.C. privacy regulator began its investigation into the personal information management practices of federal political parties operating in B.C., the parties argued that they already follow federal laws concerning privacy and challenged the constitutional authority of the provincial Privacy Commissioner to investigate them. The federal Liberal, Conservative, and New Democrat parties have since filed a petition for judicial review of the provincial law in the B.C. Supreme Court.[176]

Incorporating ISO standards by reference may cause pushbacks from organizations not previously subject to comprehensive privacy law and from small- to medium-sized organizations. ISO standards are currently a premium service and will incur a cost of investment to organizations. Additionally, some Members of Parliament may push back against an ambulatory incorporation by reference, as this may be perceived as legislative powers to a private third party.

Risks and Risk Mitigation

Defining sensitive information, implementing a tiered system according to level of sensitivity, and governing de-identified and anonymized data could limit Canadian innovation and business expansion to Canada if the same protections do not apply in other jurisdictions. This would make adaptation more complex and costly for Canadian businesses and businesses that would like to operate in Canada. However, several key trading partners have already implemented similar required protections, and international businesses are already adapting.

Additionally, legislative changes requiring a definition for sensitive information, a tiered approach to sensitive information, and de-identified and anonymized data governance may also place more burden on SMEs and NPOs as they adjust to added regulations. However, the dedicated support outlined in Recommendation 2.2 seeks to alleviate this burden. Finally, given the above timeline and the potential for an early federal election in the federal minority Parliament, if an election is called before the Bill has received royal assent and there is an associated dissolution of Parliament, then the Bill may die on the order paper.[177] However, the Bill could be revisited following the opening of Parliament after the election.[178]

Recommendation 2: Engineering an Environment of Trust

To build public trust in the digital privacy environment, Interac should advocate for a human rights-based approach to privacy and take the lead on elevating community voices in a national conversation on privacy. An HRBA would supplement traditional regulatory strategies that the OPC already employs that have been referred to as "responsive regulation". Responsive regulation refers to a regulator's use of "a range of approaches to encourage capacity building", along with escalatory sanctions when earlier steps are unsuccessful.[179] Such a strategy combined with an HRBA would allow the OPC to implement compliance and enforcement strategies that deter unlawful behaviour, encourage and reward compliant actors, and incorporate the perspectives of communities. The following table describes the components of Recommendation 2 by comparing the current state of compliance activities and responsibilities (described above in the section *Privacy Protections Under Federal Law)* to the proposed future state.

Table 1 – Current and Future State of Canada's Privacy Compliance Regime

	Activities and Responsibilities	
Components of Compliance	Current State	**Future State** *(Human Rights-Based Approach)*
Understand Stakeholder and Community Perspectives	OPC • Public opinion research	OPC • Public opinion research Private Sector • **Digital Privacy Dialogues Initiative** ***(Recommendation 2.1)***
Compliance Promotion	OPC • Compliance promotion materials ○ OPC interpretation of PIPEDA ○ Technology-specific guidelines	OPC • Compliance promotion materials ○ OPC interpretation of PIPEDA ○ Technology-specific guidelines **and templates**

	• Reports of PIPEDA Investigations findings • Business advisory services	• Reports of PIPEDA Investigations findings • Business Advisory Directorate advising services • **Anonymous help service** • **Case studies of best practices** • **Dedicated advisory services for SMEs and NPOs *(Recommendation 2.2)***
Compliance Verification (Inspection)	OPC • Intake of complaints from the public • Reports triggered by media reports, whistleblowing, etc. • Risk-based investigations	OPC • Intake of complaints from the public • Reports triggered by media reports, whistleblowing, etc. • Risk-based investigations
Response	OPC • Attempt to resolve cases through mediation • Compliance agreements	OPC • Attempt to resolve through mediation • Compliance agreements
Enforcement	OPC • Application to the Federal Court Federal Court • Hear case as new and make decision (*de novo*) • Issue orders to comply with the law • Issue fines	**OPC** • **Hear facts of investigation** • **Issue orders to comply with the law (*already proposed under Bill C-27*)** • **Issue administrative monetary penalties *(Recommendation 2.3)***
Appeal	Higher Court Authorities • Hear appeals	**Privacy Appeal Tribunal** • **Hear appeals (Recommendation 2.3)** Higher Court Authorities • Hear appeals with **deference to tribunal decision *(Recommendation 2.3)***

An additional future consideration for the OPC's compliance framework could be the inclusion of a regulatory sandbox. This experimental lab would allow organizations to test their ideas with the

OPC and enable the Commissioner to identify the policy implications of emerging technologies as they arise (See Textbox 2 for an example of a privacy regulatory sandbox).

Textbox 2. The UK Information Commissioner's Office Regulatory Sandbox

Jurisdictions similar to Canada have adopted approaches to privacy protections that aim to reduce uncertainty and foster coordination and trust, which facilitates learning and innovation. In the United Kingdom, the Information Commissioner Office has developed a regulatory sandbox for privacy, opening their doors to innovations that are likely to be transformative, those that fall under an emerging technology category, and those related to the use of biometrics (technology that uses an aspect or pattern of physical characteristics).

The service is free of charge and benefits both the regulator and the company through a stronger understanding of technological innovation on the regulator's side and through increasing consumer trust and an understanding of data protection frameworks on the company's side.[180]

2.1 Digital Privacy Dialogues Initiative

Businesses should adopt a Digital Privacy Dialogues corporate social responsibility (CSR) initiative. This initiative would convene community members to discuss their priorities and vision for an HRBA to digital privacy. It would center people, who provide the data that fuel the digital economy, and would provide insights into how individuals perceive an HRBA to privacy. Taking such a co-creation approach with the public through a CSR campaign can increase consumer confidence in a company.[181] Additionally, privacy protections have already formed part of CSR strategies. Apple's 2022 Environmental, Social and Governance Report recognizes the fundamental human right to privacy and includes a commitment to preventing issues surrounding the realization of that right (along with examples of how it is upholding its commitments).[182] Ultimately, the Digital Privacy Dialogues Initiative could provide primary data to guide what additional legislative, policy, and private governance changes should be made to foster trust in the Canadian digital context.

This CSR strategy would improve an existing model for engagement on emerging technology and privacy issues. In 2018, the Canadian Institute for Advanced Research (CIFAR), a non-profit organization focused on AI research and advocacy, received funding from the federal government to conduct the AI Futures Policy Lab project.[183] This initiative ran from 2018 to 2019, convening policymakers, industry experts, and advocates across the country for workshops on AI. Participants would learn about the implications and trajectory of AI and collaborate on generating policy solutions.[184] Education is critical in this context given that 79% of consumers do not understand what companies are doing with their data.[185] The Digital Privacy Dialogues Initiative

could retain the creation of a toolkit to inform and educate Canadians about the advancement of technology and privacy protections. It could also replicate the convening of different voices from different sectors and community spaces. However, CIFAR's process was criticized for excluding everyday Canadians, potentially missing out on valuable insights about the everyday impacts of AI.[186] The proposed CSR program should emphasize engaging with Canadians, especially traditionally marginalized communities, who face disproportionately high impacts as it concerns privacy infringements.

To create this initiative, companies should begin by understanding the internal appetite of employees of taking an HRBA to privacy. Alignment with employee goals can positively influence the success and integration of a CSR strategy.[187] Subsequently, businesses should conduct project risk assessments to outline the impacts on communities in designing engagement strategies. Working with communities and municipalities to co-create objectives and indicators of success is crucial for the successful implementation of the initiative. CSR teams should identify trusted community partners and organizations to contact to better engage traditionally marginalized communities. Partnering with municipal governments could also provide companies with existing infrastructure, resources, and relationships with community members to host these dialogues. One positive example of partnership includes the Community Solutions Network of Infrastructure Canada's Smart Cities Challenge. This program emphasizes engaging communities on the implementation risks and opportunities with regards to data management, privacy, and security.[188]

Implementation Considerations

Timeline and Costing

Implementing the initiative would take three years, including one year for project design, and two years for relationship building and community engagements.[189] Cost estimates for implementation are drawn from Canadian municipal community consultations on integrating technologies to create Smart Cities. Costs could range from $50,000 to $200,000, depending on how widespread consultations are within a locality.[190] Engagement costs for in-person or online engagement would differ based on resource needs.[191] In-person and online engagement could differ by a 1:6 cost ratio per participant.[192] Choosing to engage in-person or online engagements will depend on the effectiveness and preferences of specific communities.

Risks and Risk Mitigation

A key risk includes a lack of meaningful engagement, which tokenizes traditionally marginalized groups and cultivates mistrust in CSR strategies. Actively integrating community leaders in the designing and implementation project to shape priorities and how engagement should take place to mitigate this risk. Barcelona's Smart City consultative process, which led to the successful integration of the smart city project, serves as a positive model. The city recruited from a diverse group of community members to select "Community Champions" that co-designed project governance and management policies.[193] Stakeholders would be likely to welcome this initiative, especially considering that politicians across party lines have verbalized citizens' demands for improved privacy protections under Bill C-27.[194] Additional advice or inputs from communities could also help Members of Parliament to better identify areas of improvement in the Bill.[195]

Understanding people's priorities is the foundation of the development of privacy policies and programs that take an HRBA.

2.2 Establishing an SME and NPO Advisory Directorate

To equip SMEs and NPOs with the awareness, resources, and expertise required to adapt to new privacy requirements, an additional Advisory Directorate for SMEs and NPOs should be established in the OPC. This body would provide resources and information regarding best practices for compliance to help SMEs and NPOs comply with new and amended laws, regulations, and policies, and prevent the possibility of an investigation, fine, or breach.

This Directorate could be modelled off of France's Commission Nationale Informatique et Liberté, described in Textbox 3. It could be staffed by Data Protection Aides (DPAs), privacy specialists to whom SMEs and NPOs could submit privacy-related questions (including anonymous questions) and requests for support via website or phone channels. A DPA could be assigned to a case, review the request, and provide support. The Directorate should prepare a digital privacy guidance toolbox which would detail information regarding data protection compliance, how to safeguard different levels of sensitivity for sensitive personal information, what to do if a breach occurs, and continually improve data protection practices to ease the process of adaptation to Canada's new privacy regime. This guidance toolbox would be tailored to SMEs and NPOs organizations of various sizes and capacities to further support them in their efforts.

Textbox 3. Advisory Role Model: Commission Nationale Informatique et Liberté (CNIL)

France's Data Protection Authority, CNIL, has departments that are dedicated to developing compliance tools and providing support to organizations, and they are separate from the investigative departments.[196] Through these departments, CNIL has developed guidelines based on the needs of small and medium-sized organizations to promote higher levels of compliance.[197] It also established a charter to explain its approach to providing support to data controllers. Individuals and bodies that deal with processing data can submit requests for advice to the CNIL. Depending on the seriousness and difficulty of the question, CNIL provides advice either via letter, email correspondence, phone call, through in person meetings, or an examination of the request during a CNIL plenary session. [198]

Implementation Considerations

Timeline and Costing

The organization would be established in 3 years. It would take 1.5 years to establish the SME and NPO advisory directorate, hire and onboard DPAs with expertise in digital privacy and data protection compliance, and develop and implement the directorate's systems and protocols.

Following the hiring and onboarding of the DPAs, it would take another 1.5 years to develop a digital privacy guidance toolbox, general guidance protocol, and assignments by businesses size and type, area of data protection expertise, and an added page to the OPC website for anonymous question submissions and answer postings.

Based on spending and employment trends in 2021-2022 recorded for a similar program in the government of Canada, the Digital Service Program, it is estimated that the cost of adding and implementing the SME and NPO advisory directorate would amount to approximately $11.8 million.[199]

Stakeholder Analysis
At the end of 2021, there were about 1.21 million small and medium-sized enterprises in Canada, comprising over 99% of all employer businesses in Canada.[200] These businesses employ 84% of Canadians in the workforce, making Canada's economy reliant on the success of its SMEs.[201] This will continue to be the case in the digital realm, as the online space reduces cost barriers to enter markets, causing SME numbers to continue to grow. Considering the significance of SMEs to the economy and that this SME and NPO advisory directorate would be an optional support, this recommendation should receive support across various stakeholder groups.

Not for profit organizations also play an important role in the daily lives of Canadians and Canada's economy. For example, in 2020, non-profit organizations made up $29.9 billion, or 1.4%, of Canada's total economy.[202] Given the important role not for profit organizations play in the lives of Canadians and Canada's economy, and the optional nature of the directorate, this aspect of the recommendation should also receive support from a variety of stakeholders.

Risks and risk mitigation
Some stakeholders have shared that private actors may not want to access this support and open themselves up to more scrutiny from the OPC. To address this risk, an option for actors to submit anonymous questions and requests for advice to the directorate could be established. The OPC could publicly post answers in response to the anonymous questions to promote education and awareness for organizations looking to comply with the law and regulations. Another way to mitigate this risk is for the OPC to provide optional compliance training for lawyers to offer the opportunity for organizations to have their lawyers ask the OPC questions on their behalf to protect their anonymity. Finally, it is recommended that the OPC's compliance guidance remains an independent activity from compliance enforcement just as the Canadian Food Inspection Agency (CFIA) separates compliance and enforcement by keeping inspections and investigations as independent activities.[203]

2.3 Enforcing Privacy Law
While Bill C-27 would give the OPC the power to issue orders and it includes provisions for fines, it would delegate fining authority to a new privacy tribunal.[204] The creation of a new, separate administrative body to issue fines would reduce timeliness, increase the cost of privacy enforcement, and undercut the authority of the OPC by distorting incentives for private actors to work with the Commissioner. Therefore, Interac should advocate for Canada's privacy statute to

enable the OPC to issue administrative monetary penalties (AMPs) for non-compliance with the law and for the tribunal to operate solely as an appeals body.

Penalty Administration

The severity of the AMP should be determined by 1) which aspect of the legislation was broken, 2) the level of sensitivity of the data at risk, and 3) the history of the reporting entity (See Figure 3). The most serious contravention of the law should be a failure to follow an order from the OPC, or processing of data in contravention of the law, followed by other issues such as reporting failures or improper adherence to privacy regulations. Privacy risks or violations concerning sensitive information should be treated with heavier fines. Violations concerning the most sensitive information, as outlined in Recommendation 1.1, would come with the heaviest of AMPs, followed by other sensitive information. Finally, AMPs should account for the history of an organization. If parties have proactively engaged with the OPC in the past on getting advice or leveraging the regulatory sandbox (see Textbox 2), these should be considered mitigating factors, whereas previous penalties and orders should be considered aggravating factors.

The AMPs should be flexible enough to account for the fact that both for-profit and not-for-profit organizations will be subject to enforcement and that not all violations of privacy law pose the same harm to individuals or society. However, the AMPs will need to have a large enough upper bound to have an impact on larger actors who will calculate the cost of negligence to avoid adhering to privacy laws. The existing provisions within Bill C-27 are sufficient in providing for a maximum penalty of $25,000,000 or 5% of a company's global revenue, whichever is higher.[205]

Figure 3 - Considerations for Issuance of Administrative Monetary Penalties

Appealing Decisions

Enabling regulated entities to appeal to the privacy tribunal in the case of penalties ensures that they still have a fair, independent body to review their case. Bill C-27 already enables regulated entities to appeal OPC orders at the tribunal, meaning that the addition of a review of penalties would effectively transform this tribunal into an appeal body. [206] Such specialized appeal tribunals

already exist in the Canadian regulatory ecosystem. The following examples are federal tribunals that are dedicated to hearing appeals of orders and penalties issued by the relevant government body: the Canadian Agricultural Review Tribunal for the Canadian Food Inspection Agency, the Environmental Protection Tribunal of Canada for Environment and Climate Change Canada, and the Transportation Appeal Tribunal of Canada for the Minister of Transport and the Canadian Transportation Agency.[207]

Implementation Considerations

Timeline and Costing

In implementing AMPs, the OPC should start with lower penalties to train actors on the new expectations of the law in the first year of implementation, before moving to higher amounts. The OPC would not be able to administer penalties until the updated privacy legislation comes into force, which, as explained in Recommendation 1, may not take place until 2025.

These changes will require an expansion of the organization, as the directorate that is in charge of issuing the penalty should have a reporting structure separate from that of the directorates that investigate organizations to ensure adherence to legal principles.

Considering that the most recently available public information indicates that the Compliance, Intake and Resolution Directorate (the first body to attempt to resolve complaints) has a headcount of approximately 19 employees and the PIPEDA Compliance Directorate (the body responsible for investigations) has a headcount of approximately 11 employees, the directorate responsible for penalties should consist of approximately 6 employees, or just over half of the size of the investigative unit.[208] This also accounts for the OPC's 85% early resolution rate for PIPEDA cases.[209] Given the OPC spends approximately $0.14 million per FTE on protecting privacy rights, this would require an annual budget increase of approximately $0.84 million.[210] This budget increase should be accompanied with a three-year formative evaluation to examine the costing pressures on the OPC. Given that Bill C-27 already calls for the establishment of an administrative tribunal, and that this recommendation calls for a similar tribunal with less responsibility, there would be no costs additional to Government of Canada estimates for the Bill's proposed tribunal.

Conclusion

The ubiquity of data is quickly transforming Canada's digital economy. All private organizations, including private sector organizations, non-profit organizations, and political parties, are looking to derive value from data. As the enthusiasm for data increases, so do concerns about people's privacy protections. The Digital Age has engendered shrinking privacy spheres, disproportionately affecting traditionally marginalized communities. This creates a key policy challenge of how best to balance the protection of people's privacy rights in a data-driven economy.

This Policy Lab report answers the following questions, sponsored by Interac:

> "With a complex environment of digital privacy protections across various jurisdictions in Canada, what regulatory and legislative changes are needed to recognize digital privacy

as a basic human right for all, and how do we ensure digital inclusion and control of data are considered as part of the solution?"

This report contributes to Interac's public education and regulatory innovation efforts by providing them with a novel and critical analysis of the state of digital privacy in Canada. By outlining how digital transformation impacts privacy and trust in the digital economy, the harms faced by individuals, and the impetus to make policy changes now, the report demonstrates the urgency of the issue and provides recommendations of how Interac can shape meaningful change in the Canadian privacy space. Ultimately, this report calls for an innovative human rights-based approach to privacy protections that raises the level of responsibility for organizations and engineers an environment of trust.

As the digital landscape continues to change in unpredictable ways, the human rights-based approach anchors privacy law in values that retain the dignity and respect of all human beings.

Appendix A – Stakeholder Interviewee List

Organization	Name, *Title*
Calgary Chamber of Commerce	Ruhee Ismail-Teja, *Director, Policy and Communications*
Canadian Chamber of Commerce	Alex Gray, *Senior Director, Fiscal and Financial Services Policy*
Canadian Studies Program, University College, University of Toronto	Siobhan O'Flynn, *Assistant Professor, Teaching Stream*
Center on Privacy and Technology at Georgetown Law	Emily Tucker, *Executive Director*
Centre for Law and Democracy	Toby Mendel, *Executive Director and Founder*
Centre for Media, Technology and Democracy	Helen Hayes, *Research Manager*
Centre for Media, Technology and Democracy	Supriya Dwivedi, *Director of Policy & Engagement*
Digital Governance Council	Tim Bouma, *Director of Verification and Assessments*
Feminism Makes Us Smarter	Françoise Girard, *Founder and CEO*
GEM Consulting	Michelle Gordon
Georgetown University & McGill University	Dr. Guillaume Beaumier, *Post-Doctoral Researcher*
Global Information Governance, Technology	Fuchsia Norwich, *Lawyer, CIPP/C*
Global Privacy & Security by Design Centre	Dr. Ann Cavoukian, *Executive Director* *(former three-term Information and Privacy Commissioner of Ontario)*
Interac	Colette Stewart, *Senior Legal Counsel, Privacy Lead*
Interac	Gabrielle Gallant, *Senior Manager, Public Affairs*
Interac	Scott Cooper, *Senior Legal Counsel*
Interac	Peter Seney, *Corporate Citizenship Manager*
Interac	Phil Pellegrini, *Associate Vice President, Regulation and Innovation, Strategy*
Interac	Scott Cooper, *Senior Legal Counsel*
Leadership Lab	Nour Abdelaal, *Research Associate*
McMillan	Lyndsay A. Wasser, *Partner, Privacy & Data Protection*
Meta	Kevin Chan, *Global Policy Campaigns Strategies Director*
OECD	Michael Donohue, *Data Protection Officer*
Office of the Privacy Commissioner	Daphne Guerrero, *Manager, Research and Guidance, Research and Parliamentary Affairs Directorate*
Self-employed	Marie-Claude Landry, *Consultant*
Shopify	Jarrett Lalonde, *Global Head of Product Policy*
Statistics Canada	Eric Rancourt, *Assistant Chief Statistician*
Statistics Canada	Dr. Pierre Desrochers, *Chief Privacy Officer*

Statistics Canada	Tom Dufour, *Director General, Strategic Data Management Branch*
SunLife	Suzanne Morin, *Enterprise Conduct, Data Ethics and Chief Privacy Officer*
TELUS	Bill Abbott, Director, *Data Policy and Research*
Treasury Board of Canada Secretariat	Ashley Belanger, *Director, Digital Identity*
Treasury Board of Canada Secretariat	Jennifer Schofield, *Executive Director, Privacy and Data Protection Division*
Treasury Board of Canada Secretariat	Michael Goit, *Director of Digital Credentials Policy*
University of British Columbia	Dr. Wendy Wong, *Professor, Political Science*
University of Ottawa	Dr. Teresa Scassa, *Canada Research Chair in Information Law and Policy*
University of Ottawa	Dr. Karen Eltis, *Full Professor, Faculty of Law*
University of Ottawa	Dr. Michael Geist, *Canada Research Chair in Internet and E-Commerce Law*

Endnotes

[1] Heath, Damian, and Ludwig Micallef. 2021. “What Is Digital Economy? | Deloitte Malta | Technology.” Deloitte Malta. 2021. https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

[2] World Economic Forum. 2022. “Why Digital Trust Is Key to Building Thriving Economies.” World Economic Forum. August 17, 2022. https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/.

[3] McKinsey & Company. 2020. “COVID-19 Digital Transformation & Technology | McKinsey.” McKinsey & Company. October 5, 2020. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever.

[4] Ciuriak, Dan. 2022. “Unfree Flow with No Trust: The Implications of Geoeconomics and Geopolitics for Data and Digital Trade.” Centre for International Governance Innovation. February 14, 2022. https://www.cigionline.org/articles/unfree-flow-with-no-trust-the-implications-of-geoeconomics-and-geopolitics-for-data-and-digital-trade/.

[5] Anaya Tessa. 2022. “Consumers Expect Online Privacy, but Can SMEs Deliver It?” GetApp (blog). September 13, 2022. https://www.getapp.ca/blog/3062/online-privacy#When-and-why-are-consumers-happy-to-share-information:~:text=Two%2Dthirds%20(67%25)%20agree%20they%20are%20happy%20to%20share%20their%20personal%20information%20if%20it%20means%20better%2C%20more%20efficient%20products%20or%20services.%20And%2065%25%20are%20happy%20to%20share%20when%20it%20results%20in%20more%20personalized%20products.

[6] Beheshti, Amin, Boualem Benatallah, Quan Z. Sheng, and Francesco Schiliro. 2020. “Intelligent Knowledge Lakes: The Age of Artificial Intelligence and Big Data.” In *Web Information Systems Engineering*, edited by Leong Hou U, Jian Yang, Yi Cai, Kamalakar Karlapalem, An Liu, and Xin Huang, 24–34. Communications in Computer and Information Science. Singapore: Springer. https://doi.org/10.1007/978-981-15-3281-8_3.

[7] Zuboff, Shoshana. “You Are Now Remotely Controlled Capitalists Control the Science and the Scientists, the Secrets and the Truth.” The New York Times, 24 Jan. 2020. https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html.

[8] Zuboff. “You Are Now Remotely Controlled Capitalists Control the Science and the Scientists, the Secrets and the Truth.”

[9] Human Rights Council. 2021. “The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights.” https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement.

[10] Human Rights Council. 2019. “Resolution Adopted by the Human Rights Council on 26 September 2019.” UN Docs. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/297/52/PDF/G1929752.pdf?OpenElement.

[11] EY. 2020. “Has Lockdown Made Consumers More Open to Privacy? EY Global Consumer Privacy Survey 2020.” EY Global Consumer Privacy Survey. EY. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/consulting/ey-global-consumer-privacy-survey/ey-data-privacy-report-v2.pdf.

[12] Cisco. 2022. “Cisco 2022 Consumer Privacy Survey.” Cisco. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf?CCID=cc000160&DTID=esootr000875&OID=wprsc030156.

[13] Interac Corp. “Taking a Look inside Data Privacy.” n.d. *Interac* (blog). Accessed July 5, 2023. https://www.interac.ca/en/content/taking-a-look-inside-data-privacy/.

[14] Interac Corp. “Taking a Look inside Data Privacy.”

[15] Interac Corp. 2023. “How Interac Keeps Pace with Regulation and Innovation, in Canada and Beyond.” *Interac* (blog). 2023. https://www.interac.ca/en/content/ideas/how-interac-keeps-pace-with-regulation-and-innovation-in-canada-and-beyond/.

[16] Minister of Innovation, Science and Industry. 2022. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

[17] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[18] Sinclair, Amanda. 2019. ‘Measuring Digital Economic Activities in Canada: Initial Estimates’. Statistics Canada. https://www150.statcan.gc.ca/n1/pub/13-605-x/2019001/article/00002-eng.htm.

[19] Statistics Canada. 2021. ‘The Daily — Digital Supply and Use Tables, 2017 to 2019’. Statistics Canada. 20 April 2021. https://www150.statcan.gc.ca/n1/daily-quotidien/210420/dq210420a-eng.htm.

[20] *The Economist*. 2017. ‘The World’s Most Valuable Resource Is No Longer Oil, but Data’, 6 May 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[21] The World Bank. 2021. 'Data for Better Lives'. World Development Report. Washington, D.C.: The World Bank. https://www.worldbank.org/en/publication/wdr2021.

[22] Mitchell, John, Molly Lesher, and Marion Barberis. 2022. 'Measuring the Economic Value of Data'. DSTI/CDEP/GD(2021)2/FINAL. Going Digital Toolkit Note. OECD. https://one.oecd.org/document/DSTI/CDEP/GD(2021)2/FINAL/en/pdf#:~:text=Data%20are%20an%20inceasingly%20valuable,2.

[23] Mitchell, Lesher, and Barberis. 'Measuring the Economic Value of Data'.

[24] Beheshti, Benatallah, Sheng, and Schiliro. 'Intelligent Knowledge Lakes: The Age of Artificial Intelligence and Big Data'.

[25] Mrkonjić, Elma. 2022. 'How Amazon Uses Big Data'. *SeedScientific* (blog). 29 August 2022. https://seedscientific.com/how-amazon-uses-big-data/.

[26] Mrkonjić. 'How Amazon Uses Big Data'.; Toner, Helen. 2023. 'What Are Generative AI, Large Language Models, and Foundation Models?' *Center for Security and Emerging Technology* (blog). 12 May 2023. https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models/.

[27] Ramponi, Marco. 2022. 'How ChatGPT Actually Works'. *AssemblyAI* (blog). 23 December 2022. https://www.assemblyai.com/blog/how-chatgpt-actually-works/.; Amina. 2023. 'The Way How Midjourney.Com Can Be Used in Video Production'. *KROCK.IO* (blog). 28 February 2023. https://krock.io/blog/news/how-midjourney-com-can-be-used-in-video-production/.

[28] Markay, Lachlan. 2022. 'AI Becomes a Political "Super-Weapon"'. Axios. 7 October 2022. https://www.axios.com/2022/10/07/ai-becomes-a-political-super-weapon.

[29] First Republic Bank. 2017. "How Nonprofits Can Use Data to Inform Decisions and Drive Performance." First Republic Bank. https://www.firstrepublic.com/~/media/frb/documents/pdfs/content/how-nonprofits-can-use-data-to-inform-decisions.

[30] Statutes of Canada. 2000. *Personal Information Protection and Electronic Documents Act*. Vol. c. 5. https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

[31] OECD. 2015. 'Data-Driven Innovation: Big Data for Growth and Well-Being'. Paris: OECD Publishing. https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en#page4.; Cavoukian, Ann. 2011. 'Privacy by Design: The 7 Foundational Principles'. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[32] OECD. 'Data-Driven Innovation: Big Data for Growth and Well-Being'.

[33] PricewaterhouseCoopers. 2023. '2023 Canadian Digital Trust Insights'. PwC Canada. 6 January 2023. https://www.pwc.com/ca/en/services/consulting/cybersecurity-privacy/digital-trust-insights.html.

[34] Phoenix SPI. 2022. '2021-22 Survey of Canadian Businesses on Privacy-Related Issues'. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2022/por_2021-22_bus/.

[35] OECD. 'Data-Driven Innovation: Big Data for Growth and Well-Being'.

[36] Office of the Privacy Commissioner of Canada. 2023. '2022-23 Survey of Canadians on Privacy-Related Issues'. 14 June 2023. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2023/por_ca_2022-23/.

[37] Interac Corp. 2023. 'Control Is Top of Mind for Canadians When It Comes to Online Personal Information, According to New Data Privacy Week Poll'. *Interac* (blog). 24 January 2023. https://www.interac.ca/en/content/news/control-is-top-of-mind-for-canadians-when-it-comes-to-online-personal-information-according-to-new-data-privacy-week-poll/#:~:text=seven%20in%2010%20(74%20per%20cent)%20want%20more%20control%20over%20their%20online%20information.

[38] Woetzel, Jonathan, Remes, Jaana, Boland, Brodie, Lv, Katrina, Sinha, Suveer, Strube, Gernot, Means, John, Law, Jonathan, Cadena, Andres, and von der Tann, Valerie. 2018. 'Smart Cities: Digital Solutions for a More Livable Future'. McKinsey Global Institute. https://www.mckinsey.com/capabilities/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future.

[39] Mohamed, Suha. 2020. 'Cities & Data Sharing — Part 3: Barcelona'. *The Data Economy Lab* (blog). 10 September 2020. https://thedataeconomylab.com/2020/09/10/cities-data-sharing-part-3-barcelona/.

[40] O'Kane, Josh. 2022. *Sideways: The City Google Couldn't Buy*. New York: Random House of Canada. https://ebookcentral.proquest.com/lib/mcgill/detail.action?docID=7079545.

[41] CBC News. 2018. '"Not Good Enough": Toronto Privacy Expert Resigns from Sidewalk Labs over Data Concerns'. CBC News. 21 October 2018. https://www.cbc.ca/news/canada/toronto/ann-cavoukian-sidewalk-data-privacy-1.4872223.

[42] O'Kane. Sideways: The City Google Couldn't Buy.

[43] Shimizu, Yuho, Shin Osaki, Takaaki Hashimoto, and Kaori Karasawa. 2022. "Social Acceptance of Smart City Projects: Focus on the Sidewalk Toronto Case." *Frontiers in Environmental Science* 10. https://www.frontiersin.org/articles/10.3389/fenvs.2022.898922.

[44] Davis, Sarah L.M. 2020. “Contact Tracing Apps: Extra Risks for Women and Marginalized Groups.” *Health and Human Rights Journal* (blog). April 29, 2020. https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups/.

[45] Davis. “Contact Tracing Apps: Extra Risks for Women and Marginalized Groups.”

[46] Ferguson, Andrew Guthrie. 2021. “The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement.” New York University Press. https://altbanking.net/wp-content/uploads/2021/04/Excerpt-from-Andrew-Ferguson-The-Rise-of-Big-Data-Policing.pdf.

[47] Benjamin, Ruha. 2019. *Race after Technology: Abolitionist Tools for the New Jim Code*. Newark, UNITED KINGDOM: Polity Press. http://ebookcentral.proquest.com/lib/mcgill/detail.action?docID=5820427.

[48] Office of the Privacy Commissioner of Canada. 2021. “Police Use of Facial Recognition Technology in Canada and the Way Forward.” June 10, 2021. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1.

[49] Office of the Privacy Commissioner of Canada. 2021. “PIPEDA Findings #2021-001: Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d’accès à l’information Du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta.” February 3, 2021. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

[50] Office of the Privacy Commissioner of Canada. “Police Use of Facial Recognition Technology in Canada and the Way Forward.”

[51] McPhail, Brenda, and Jonathan Obar. “Preventing Big Data Discrimination in Canada: Addressing Design, Consent and Sovereignty Challenges.” Centre for International Governance Innovation, April 12, 2018. https://www.cigionline.org/articles/preventing-big-data-discrimination-canada-addressing-design-consent-and-sovereignty/.

[52] CBC News. 2020. “Clearview AI Facial Recognition Worrisome for Black, Indigenous, Racialized Groups, Expert Says.” CBC. March 5, 2020. https://www.cbc.ca/news/canada/windsor/clearview-ai-worrisome-for-black-indigenous-marginalized-communities-1.5486325.

[53] CBC News. “Clearview AI Facial Recognition Worrisome for Black, Indigenous, Racialized Groups, Expert Says.”

[54] Bond, Shannon. 2021. “Facebook Scraps Ad Targeting Based on Politics, Race and Other ‘sensitive’ Topics.” *NPR*. NPR. November 9. https://www.npr.org/2021/11/09/1054021911/facebook-scraps-ad-targeting-politics-race-sensitive-topics.

[55] Turow, Joseph. 2012. The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth. New Haven: Yale University Press. ProQuest Ebook Central.

[56] Forte, Andrea, and Nora Mcdonald. 2022. “Privacy and Vulnerable Populations.” *Springer, Cham*, February. https://doi.org/10.1007/978-3-030-82786-1_15.

[57] Mañero, J. Review of Virginia Eubanks (2018). *Automating Inequality*: *How High-Tech Tools Profile*, *Police*, *and Punish the Poor*. *Postdigit Sci Educ* 2, 489–493 (2020). https://doi.org/10.1007/s42438-019-00077-4

[58] Angwin, Julia, Jeff Larson, Lauren Kirchner, and Surya Mattu. “Machine Bias.” ProPublica, May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[59] Confessore, Nicholas. 2018. “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.” *The New York Times*, April 4, 2018, sec. U.S. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[60] UNCTAD. 2021. “Data Protection and Privacy Legislation Worldwide | UNCTAD.” UNCTAD. 12 2021. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[61] Publications Office of the European Union. 2016. *General Data Protection Regulation (GDPR)*. *Regulation (EU)*. Vol. 2016/679. https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html.

[62] Publications Office of the European Union. *General Data Protection Regulation (GDPR)*.

[63] Hirsh, Jeanette, and Jesse Hirsh. 2019. “The Peril and Potential of the GDPR.” Centre for International Governance Innovation. July 9, 2019. https://www.cigionline.org/articles/peril-and-potential-gdpr/.

[64] IAPP. 2023. “CCPA and CPRA.” 2023. https://iapp.org/resources/topics/ccpa-and-cpra/.

[65] California Legislative Information. 2018. *California Consumer Privacy Act of 2018*. Vol. 1798.100-1798.199.100. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[66] Amanpour and Company. 2023. “Alastair Mactaggart on Data Privacy Laws | WETA.” 2023. https://weta.org/watch/shows/amanpour-and-company/alastair-mactaggart-data-privacy-laws-l0gcns.

[67] Statutes of Quebec. “Act Respecting the Protection of Personal Information in the Private Sector.” 2023. LegisQuebec. April 1, 2023. https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1?langCont=en#ga:l_i-h1.

[68] PricewaterhouseCoopers. 2023. “Law 25 (Previously Bill 64): Are Businesses Ready for Major Changes in Quebec?” PwC. January 30, 2023. https://www.pwc.com/ca/en/services/consulting/privacy/privacy-canadian-business-hub/bill-64-are-businesses-ready-for-major-changes-in-quebec.html.

[69] Donahue, Yannick. 2020. “Protection des renseignements personnels : jusqu’à 25 M$ d’amende, propose la CAQ.” Radio-Canada.ca. Radio-Canada.ca. Juin 2020. https://ici.radio-canada.ca/nouvelle/1711508/entreprises-amandes-consentement-clients-internet-consommation.

[70] “Adequacy Decisions.” 2023. European Commission. April 11, 2023. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.; Information Commissioner’s Office. 2023. “Adequacy.” Information Commissioner’s Office. May 19, 2023. https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy/.

[71] Innovation, Science and Economic Development. 2020. “Sixth Update Report on Developments in Data Protection Law in Canada.” Annual Reports; Other Reports; Reports; Performance Reports. March 10, 2020. https://ised-isde.canada.ca/site/plans-reports/en/sixth-update-report-developments-data-protection-law-canada.

[72] “Debates (Hansard) No. 136 - November 28, 2022 (44-1) - House of Commons of Canada.” 2022. House of Commons. November 28, 2022. https://www.ourcommons.ca/DocumentViewer/en/44-1/house/sitting-136/hansard#11955659.

[73] “Debates (Hansard) No. 136 - November 28, 2022 (44-1) - House of Commons of Canada.”

[74] Office of the Privacy Commissioner of Canada. 2013. “The Case for Reforming the Personal Information Protection and Electronic Documents Act.” Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_r/pipeda_r_201305/#fn1.

[75] Statutes of Canada. Personal Information Protection and Electronic Documents Act.

[76] Statutes of Canada. Personal Information Protection and Electronic Documents Act

[77] Stoddart, Jennifer. 2005. 'Cherry Picking Among Apples and Oranges : Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA'. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2005/omb_051021/#:~:text=At%20the%20time,section%2029(1).; CSA Group. n.d. "FAQ." CSA Group. https://www.csagroup.org/faq/.

[78] Office of the Privacy Commissioner of Canada. 2023. 'About the OPC'. Office of the Privacy Commissioner of Canada. 23 May 2023. https://www.priv.gc.ca/en/about-the-opc/.

[79] Lavigne v. Canada (Office of the Commissioner of Official Languages). 2002, SCC 53. Supreme Court of Canada.

[80] Groves, Matthew, and Anita Stuhmcke. 2022. 'The Evolution and Future of the Ombuds'. In *The Ombudsman in the Modern State*, edited by Matthew Groves and Anita Stuhmcke, 1st ed., 1–18. Oxford: Hart Publishing. http://www.bloomsburycollections.com/book/the-ombudsman-in-the-modern-state/ch1-the-evolution-and-future-of-the-ombuds/.

[81] Office of the Privacy Commissioner of Canada. 2018. 'Who We Are'. Office of the Privacy Commissioner of Canada. 19 December 2018. https://www.priv.gc.ca/en/about-the-opc/who-we-are/.

[82] Statutes of Canada. Personal Information Protection and Electronic Documents Act.

[83] Office of the Privacy Commissioner of Canada. "Awareness Campaigns and Events." Office of the Privacy Commissioner of Canada, May 5, 2023. https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/.

[84] Office of the Privacy Commissioner of Canada. 2022. 'A Pivotal Time for Privacy: 2021-2022 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act'. Gatineau, Quebec. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202122/ar_202122/.

[85] Office of the Privacy Commissioner of Canada. 2017. 'Enforcement of PIPEDA'. Office of the Privacy Commissioner of Canada. 20 April 2017. https://www.priv.gc.ca/biens-assets/compliance-framework/en/index#.

[86] Office of the Privacy Commissioner of Canada. 2015. 'Annual Report to Parliament 2014 - Report on the Personal Information Protection and Electronic Documents Act'. Gatineau, Quebec: Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201415/2014_pipeda/#heading-0-0-0-8.

[87] Office of the Privacy Commissioner of Canada. 2012. Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis. 17 May 2012, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/.

[88] Open Media. 2023. 'Ensure Political Parties Are Subject to Canadian Privacy Law'. OpenMedia Engagement Network. https://www.ourcommons.ca/Content/Committee/441/FINA/Brief/BR12430848/br-external/OpenMedia-e.pdf.

[89] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[90] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[91] Arai, Maggie. 2023. "Five Things to Know about Bill C-27." *Schwartz Reisman Institute. University of Toronto.* Schwartz Reisman Institute. University of Toronto. April 17. https://srinstitute.utoronto.ca/news/five-things-to-know-about-bill-c-27#:~:text=The%20CPPA%20differs%20from%20PIPEDA,allowances%20for%20who%20can%20seek.

[92] Arai. "Five Things to Know about Bill C-27."; Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[93] Arai. "Five Things to Know about Bill C-27."

[94] Government of Canada, Department of Justice. 2022. "Charter Statement Bill C-27: An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts." *Government of Canada, Department of Justice, Electronic Communications*. November 10. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html#:~:text=on%20the%20Bill.-,Overview,Digital%20Charter%20Implementation%20Act%2C%202022.

[95] Government of Canada, Department of Justice. "Charter Statement Bill C-27: An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts."

[96] Government of Canada, Department of Justice. “Charter Statement Bill C-27: An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.”

[97] Office of the Privacy Commissioner of Canada. 2022. “Interpretation Bulletin: Sensitive Information.” *Office of the Privacy Commissioner of Canada*. May 16. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/#.

[98] Office of the Privacy Commissioner of Canada. “Interpretation Bulletin: Sensitive Information.”

[99] Statutes of Canada. Personal Information Protection and Electronic Documents Act.

[100] Statutes of Canada. Personal Information Protection and Electronic Documents Act.

[101] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[102] Office of the Privacy Commissioner of Canada. “Interpretation Bulletin: Sensitive Information.”

[103] Office of the Privacy Commissioner of Canada. 2021. “Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020.” *Office of the Privacy Commissioner of Canada*. May 11. https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/.

[104] Office of the Privacy Commissioner of Canada. 2023. “Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022.” *Office of the Privacy Commissioner of Canada*. April 26. https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_indu_c27_2304/#fn8.

[105] Office of the Privacy Commissioner of Canada. “Interpretation Bulletin: Sensitive Information.”

[106] Statutes of Canada. Personal Information Protection and Electronic Documents Act.

[107] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[108] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[109] Publications Office of the European Union. *General Data Protection Regulation (GDPR)*.

[110] Publications Office of the European Union. *General Data Protection Regulation (GDPR)*.

[111] Office of the Privacy Commissioner of Canada. Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis.

[112] Office of the Privacy Commissioner of Canada. Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis.

[113] Shainblum, Esther. 2019. 'Why Charities and Not-for-Profits Should Comply with PIPEDA'. *The Canadian Bar Association* (blog). 16 January 2019. https://www.cba.org/Sections/Charities-and-Not-for-Profit-Law/Articles/2019/comply-with-PIPEDA.

[114] Office of the Information and Privacy Commissioner for British Columbia. n.d. 'For Private Organizations'. Office of the Information and Privacy Commissioner for British Columbia. https://www.oipc.bc.ca/for-private-organizations/.; Thompson, Tyler J. 2023. 'Quebec's New Privacy Law 25: Is There a Nonprofit Exception?' *Lexology* (blog). 17 April 2023. https://www.lexology.com/library/detail.aspx?g=1171b8e6-8e8f-4bb5-824e-135dd3583b34.

[115] Information and Privacy Commissioner of Ontario. 2011. "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy." https://www.ipc.on.ca/wp-content/uploads/2016/11/anonymization.pdf.

[116] Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. 2019. "Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models." *Nature Communications* 10 (1): 3069. https://doi.org/10.1038/s41467-019-10933-3.; Cavoukian, Ann, and Daniel Castro. 2014. "Big Data and Innovation, Setting the Record Straight: De-Identification Does Work." Information and Privacy Commissioner Ontario, Canada. https://www2.itif.org/2014-big-data-deidentification.pdf.

[117] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[118] Miller, Katherine. 2021. 'De-Identifying Medical Patient Data Doesn't Protect Our Privacy'. *Stanford University Human-Centered Artificial Intelligence* (blog). 19 July 2021. https://hai.stanford.edu/news/de-identifying-medical-patient-data-doesnt-protect-our-privacy.

[119] Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. "Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models."

[120] Spithoff, Sheryl, Jessica Stockdale, Robyn Rowe, Brenda McPhail, and Nav Persaud. 2022. "The Commercialization of Patient Data in Canada: Ethics, Privacy and Policy." *CMAJ : Canadian Medical Association Journal* 194 (3): E95–97. https://doi.org/10.1503/cmaj.210455.

[121] Office of the Privacy Commissioner of Canada. 2022. "2021-22 Survey of Canadian Businesses on Privacy-Related Issues." *Office of the Privacy Commissioner of Canada*. August 11. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2022/por_2021-22_bus/.

[122] Westin, Fiona, Fyscillia Ream, and Benoît Dupont. 2022. 'Adapting Cybersecurity to the Needs and Capacities of SMEs: A Canadian Perspective'. Montreal: Serene-risc. https://www.serene-risc.ca/public/media/files/prod/page_files/31/Serene_Cybersecurity_Ecosystem_Canada.pdf.; Office of the Privacy Commissioner of Canada. 'A Pivotal Time for Privacy: 2021-2022 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act'.

[123] Giordani, John. 2022. 'Council Post: The Necessity Of Cybersecurity In The Nonprofit Sector'. *Forbes*, 8 November 2022. https://www.forbes.com/sites/forbestechcouncil/2022/11/08/the-necessity-of-cybersecurity-in-the-non-profit-sector/.

[124] Office of the Privacy Commissioner of Canada. "Advisory Services for Businesses".

[125] Office of the Privacy Commissioner of Canada. 'A Pivotal Time for Privacy: 2021-2022 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act'.

[126] Government of Canada, Shared Services Canada. "Browse Organization." Government of Canada, Shared Services Canada, October 10, 2020. https://geds-sage.gc.ca/en/GEDS/?pgid=014&dn=T1U9T1BDLUNQVlAsTz1HQyxDPUNB.

[127] Stoddart. 'Cherry Picking Among Apples and Oranges : Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA'

[128] Office of the Privacy Commissioner of Canada. 'A Pivotal Time for Privacy: 2021-2022 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act'.

[129] Office of the Privacy Commissioner of Canada. 'A Pivotal Time for Privacy: 2021-2022 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act'.

[130] Office of the Privacy Commissioner of Canada. 'Annual Report to Parliament 2014 - Report on the Personal Information Protection and Electronic Documents Act'.

[131] Office of the Privacy Commissioner of Canada. 2020. 'Announcement: Privacy Commissioner Files Notice of Application with the Federal Court against Facebook, Inc.' *Office of the Privacy Commissioner of Canada* (blog). 6 February 2020. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200206/.

[132] Office of the Privacy Commissioner of Canada. 2023. 'Announcement: Privacy Commissioner Appeals Federal Court Decision Related to Facebook Investigation'. Office of the Privacy Commissioner of Canada. 12 May 2023. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230512-2/.

[133] Federal Trade Commission. 2019. 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook'. *Federal Trade Commission* (blog). 24 July 2019. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

[134] Department of Justice. 2005. "The Offices of the Information and Privacy Commissioners: The Merger and Related Issues." https://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/p7.html.

[135] United Nations High Commissioner for Human Rights. 2018. 'The Right to Privacy in the Digital Age'. A/HRC/39/29. Annual Report of the United Nations High Commissioner for Human Rights and Reports of the Office of the High Commissioner and the Secretary-General. Office of the United Nations High Commissioner for Human Rights. https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.pdf.

[136] United Nations Evaluation Group Human Rights and Gender Equality Task Force. 2014. 'Integrating Human Rights and Gender Equality in Evaluations'. New York: United Nations Evaluation Group. www.unevaluation.org/guidance/HRGE.

[137] "International Covenant on Civil and Political Rights." 1966. OHCHR. December 16, 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[138] Government of Canada, Department of Justice. 1999. "Charterpedia - Section 8 – Search and Seizure." Government of Canada. November 9, 1999. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html.

[139] Office of the Privacy Commissioner of Canada. 2014. "Factum of the Intervener, the Privacy Commissioner of Canada: Elizabeth Bernard and Attorney General of Canada and Professional Institute of the Public Service of Canada." February 19, 2014. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/factum/04_bernard_pa/#fn23.

[140] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[141] Office of the Privacy Commissioner of Canada. "Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022."

[142] Balkin, Jack M. 2020. "The Fiduciary Model of Privacy." SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=3700087.

[143] United Nations Evaluation Group Human Rights and Gender Equality Task Force. 'Integrating Human Rights and Gender Equality in Evaluations'.

[144] United Nations. 2023. 'Human Rights Compliance "Best Antidote to Inequalities", High Commissioner Tells Security Council Debate on Future-Proofing Trust to Sustain Peace'. SC/15273. United Nations. https://press.un.org/en/2023/sc15273.doc.htm.

[145] Teng, Yan, and Yan Song. 2022. "Beyond Legislation and Technological Design: The Importance and Implications of Institutional Trust for Privacy Issues of Digital Contact Tracing." *Frontiers in Digital Health* 4. https://www.frontiersin.org/articles/10.3389/fdgth.2022.916809.

[146] Statistics Canada. 2020. "Willingness of Canadians to Use a Contact Tracing Application." July 31, 2020. https://www150.statcan.gc.ca/n1/pub/45-28-0001/2020001/article/00059-eng.htm.

[147] Global Affairs Canada. 2015. "Advancing Human Rights." Global Affairs Canada. October 16, 2015. https://www.international.gc.ca/world-monde/funding-financement/advancing_human_rights-promouvoir_droits_personne.aspx?lang=eng.

[148] Renieris, Elizabeth M. 2023. *Beyond Data*. The MIT Press. https://mitpress.mit.edu/9780262047821/beyond-data/.

[149] Floridi, Luciano. 2016. "On Human Dignity as a Foundation for the Right to Privacy." *Philosophy & Technology* 29 (4): 307–12. https://doi.org/10.1007/s13347-016-0220-8.

[150] R. v. Dyment. 1988, 2 SCR 417. Supreme Court of Canada.

[151] Publications Office of the European Union. *General Data Protection Regulation (GDPR).*; Government Digital Service. "Data Protection Act." GOV.UK, September 16, 2015. https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK%27s%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently.; Statutes of Quebec. *Act Respecting the Protection of Personal Information in the Private Sector*.

[152] Office of the Privacy Commissioner of Canada. “Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022.”

[153] Publications Office of the European Union. *General Data Protection Regulation (GDPR)*.

[154] Publications Office of the European Union. *General Data Protection Regulation (GDPR)*.; Government Digital Service. “Data Protection Act.”; Statutes of Quebec. *Act Respecting the Protection of Personal Information in the Private Sector.*

[155] Publications Office of the European Union. *General Data Protection Regulation (GDPR)*.

[156] Government Digital Service. “Data Protection Act.”

[157] Information Commissioner’s Office. 2023. ‘What Is Special Category Data?’ Information Commissioner’s Office. ICO. 19 May 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/.

[158] Information Commissioner’s Office. ‘What Is Special Category Data?’

[159] Statutes of Quebec. Act Respecting the Protection of Personal Information in the Private Sector.

[160] Publications Office of the European Union. *General Data Protection Regulation (GDPR).*

[161] Montgomery, Kathryn C., Jeff Chester, and Tijana Milosevic. 2017. “Children’s Privacy in the Big Data Era: Research Opportunities.” *Pediatrics* 140 (Supplement_2): S117–21. https://doi.org/10.1542/peds.2016-1758O.

[162] LaMotte, Sandee. “Marketers Are Gathering Data on Your Kids from the Apps They Use, Study Finds.” CNN, September 16, 2020. https://edition.cnn.com/2020/09/08/health/privacy-violations-kids-apps-wellness-trnd/index.html.

[163] Statutes of Canada. Personal Information Protection and Electronic Documents Act.

[164] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[165] Information Commissioner’s Office. 2023. ‘About This Code’. Information Commissioner’s Office. ICO. 19 May 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/.

[166] National Archives. 2013. *Children's Online Privacy Protection Rule*. Vol. 16 CFR Part 312. https://www.ecfr.gov/current/title-16/part-312.

[167] Computer Security Resource Center. n.d. 'Data Processing - Glossary'. U.S. Department of Commerce National Institute of Standards and Technology. https://csrc.nist.gov/glossary/term/data_processing.

[168] Statutes of Canada. Personal Information Protection and Electronic Documents Act.

[169] Publications Office of the European Union. *General Data Protection Regulation (GDPR).*

[170] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[171] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection. 2022. 'ISO/IEC 27559:2022'. International Standards Organization. November 2022. https://www.iso.org/standard/71677.html.

[172] Government of Canada. 'Incorporation by Reference'. Legislation and Guidelines - Food and Nutrition - Health Canada, n.d. https://www.canada.ca/en/health-canada/services/food-nutrition/legislation-guidelines/acts-regulations/incorporation-reference.html.

[173] "House of Commons Sitting Calendar - 2023." 2023. *Sitting Calendar - House of Commons of Canada*. https://www.ourcommons.ca/en/sitting-calendar.

[174] Statutes of Canada. 2000. *Canada Elections Act*. Vol. c. 9. https://laws-lois.justice.gc.ca/eng/acts/E-2.01/page-6.html#docCont.

[175] Thompson, Kirsten. 'Canadian Government Releases Companion Document to Proposed AI Law'. *Dentons Data*, 17 Mar. 2023, https://www.dentonsdata.com/canadian-government-releases-companion-document-to-proposed-ai-law/.

[176] Boutilier, Alex. 2023. 'Liberals Try to Delay Fight over Privacy Rules for Political Parties'. *Global News*, 8 May 2023. https://globalnews.ca/news/9681510/liberals-fight-privacy-rules/.

[177] "Parliamentary Cycle." 2023. *Parliamentary Cycle - Our Procedure - ProceduralInfo - House of Commons of Canada*. Accessed July 6. https://www.ourcommons.ca/procedure/our-procedure/parliamentaryCycle/c_g_parliamentarycycle-e.html.

[178] "Parliamentary Cycle." Parliamentary Cycle - Our Procedure - ProceduralInfo - House of Commons of Canada.

[179] Gunningham, Neil. 2016. 'Compliance, Enforcement, and Regulatory Excellence'. In *Achieving Regulatory Excellence*, edited by Cary Coglianese, 188–206. Washington: Brookings Institution Press. muse.jhu.edu/book/49139.

[180] Information Commissioner's Office. 2023. 'Regulatory Sandbox'. Information Commissioner's Office. ICO. 19 May 2023. https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/.

[181] Lee, Sun Young, Young Kim, and Yeuseung Kim. 2020. "The Co-Creation of Social Value: What Matters for Public Participation in Corporate Social Responsibility Campaigns." *Journal of Public Relations Research* 32 (5–6): 198–221. https://doi.org/10.1080/1062726X.2021.1888734.

[182] Apple. 2023. "Environmental Social Governance Report - Apple 2022 ESG Report." Apple. https://s2.q4cdn.com/470004039/files/doc_downloads/2022/08/2022_Apple_ESG_Report.pdf.

[183] "Pan-Canadian AI Strategy." 2023. CIFAR. 2023. https://cifar.ca/ai/.; Rasky, Elia. 2023. "Workshopping AI: Who's at the Table?" *Communitas* 3 (1): 103–25. https://doi.org/10.7202/1098933ar.

[184] George, Lianne. 2018. "AI Futures Policy Labs: A Series of Workshops for Emerging Policymakers." *Brookfield Institute for Innovation + Entrepreneurship* (blog). November 13, 2018. https://brookfieldinstitute.ca/ai-futures-policy-labs-a-series-of-workshops-for-emerging-policymakers/.

[185] Cisco. 2022. "Cisco 2022 Consumer Privacy Survey." Cisco. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf?CCID=cc000160&DTID=esootr000875&OID=wprsc030156.

[186] Rasky, Elia. 2023. "Workshopping AI: Who's at the Table?" *Communitas* 3 (1): 103–25. https://doi.org/10.7202/1098933ar.

[187] Lim, Joon Soo, and Cary A. Greenwood. 2017. "Communicating Corporate Social Responsibility (CSR): Stakeholder Responsiveness and Engagement Strategy to Achieve CSR Goals." *Public Relations Review* 43 (4): 768–76. https://doi.org/10.1016/j.pubrev.2017.06.007.

[188] Infrastructure Canada. 2018. "Infrastructure Canada - Smart Cities Challenge." Infrastructure Canada. March 12, 2018. https://www.infrastructure.gc.ca/cities-villes/index-eng.html.

[189] George. "AI Futures Policy Labs: A Series of Workshops for Emerging Policymakers."

[190] City of Toronto. 2018. "Smart Cities Challenge Submission." https://www.toronto.ca/wp-content/uploads/2018/05/9815-Smart-Connected-Communities.pdf.; Cook, Tracey. 2019. "Quayside - Update." City of Toronto. https://www.toronto.ca/legdocs/mmis/2019/ex/bgrd/backgroundfile-133867.pdf.

[191] Savoy, Brandon, and Matthew Crozier. 2020. “Assessing the Value of Digital Community Engagement: Efficiency, Risk, Cost and Trust.” Bang the Table. https://www.bangthetable.com/wp-content/uploads/Business-case-for-online-engagement-2.pdf.

[192] Savoy and Crozier. “Assessing the Value of Digital Community Engagement: Efficiency, Risk, Cost and Trust.”

[193] Soni, Shivam. 2020. “Cities & Data Sharing — Part 3: Barcelona.” *The Data Economy Lab* (blog). September 10, 2020. https://thedataeconomylab.com/2020/09/10/cities-data-sharing-part-3-barcelona/.

[194] “Debates (Hansard) No. 136 - November 28, 2022 (44-1) - House of Commons of Canada.”

[195] “Debates (Hansard) No. 136 - November 28, 2022 (44-1) - House of Commons of Canada.”

[196] Commission Nationale de l’Informatique et des Libertés. 2023. ‘Organization Chart - CNIL’. https://www.cnil.fr/sites/cnil/files/2023-07/organigramme_cnil.pdf.

[197] Commission Nationale de l’Informatique et des Libertés. n.d. ‘RGPD : par où commencer’. https://www.cnil.fr/fr/rgpd-par-ou-commencer.

[198] Commission Nationale de l’Informatique et des Libertés. 2023. ‘Charte d’accompagnement Des Professionnels’. https://www.cnil.fr/sites/cnil/files/2023-02/charte_accompagnement_des_professionnels.pdf.

[199] Treasury Board of Canada Secretariat. 2023. ‘Infographic for Digital Service’. Government of Canada. 28 June 2023. https://www.tbs-sct.canada.ca/ems-sgd/edb-bdd/index-eng.html#infographic/program/ISC-BNP05/financial.

[200] Innovation, Science and Economic Development Canada. 2022. ‘Key Small Business Statistics 2022’. Innovation, Science and Economic Development Canada. 29 November 2022. https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2022.

[201] Delgado, Esteban Pinzon, Robert Fair, and Chris Johnston. 2023. ‘Analysis on Small Businesses in Canada, First Quarter of 2023’. Statistics Canada. https://www150.statcan.gc.ca/n1/pub/11-621-m/11-621-m2023003-eng.htm.

[202] Statistics Canada. 2022. ‘An Overview of the Non-Profit Sector in Canada, 2010 to 2020’. Statistics Canada. https://www150.statcan.gc.ca/n1/pub/13-605-x/2022001/article/00002-eng.htm.

[203] Government of Canada, Canadian Food Inspection Agency. 2020. “Compliance and Enforcement Policy.” *Canadian Food Inspection Agency*. / Gouvernement du Canada. October 30. https://inspection.canada.ca/about-cfia/transparency/regulatory-transparency-and-openness/compliance-and-enforcement/eng/1299846323019/1299846384123.

[204] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[205] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[206] Minister of Innovation, Science and Industry. An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts.

[207] Canadian Agricultural Review Tribunal. 2023. ‘Jurisdiction and Mandate’. 5 June 2023. https://cart-crac.gc.ca/about/about-us-en.html; Environmental Protection Tribunal of Canada. 2023. ‘About the Tribunal’. Environmental Protection Tribunal of Canada. 1 May 2023. https://eptc-tpec.gc.ca/en/about/about-eptc.html; Transportation Appeal Tribunal of Canada. 2023. ‘Transportation Appeal Tribunal of Canada’. Transportation Appeal Tribunal of Canada. 1 May 2023. https://www.tatc.gc.ca/en/home.html.

[208] Government of Canada. 2020. ‘Browse Organization’. Government Electronic Directory Services. 2020. https://geds-sage.gc.ca/en/GEDS/?pgid=014&dn=T1U9T1BDLUNQVlAsTz1HQyxDPUNB.

[209] Office of the Privacy Commissioner of Canada. ‘A Pivotal Time for Privacy: 2021-2022 Annual Report to Parliament on the Privacy Act and the Personal Information Protection and Electronic Documents Act’.

[210] Office of the Privacy Commissioner of Canada. 2023. ‘2023-24 Departmental Plan’. https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2023-2024/dp_2023-24/#heading-0-3-1.