Ontario Private Sector Privacy Reform

Improving private sector privacy for Ontarians in a digital age

DISCUSSION PAPER

1 Hearing from Ontarians

Protecting Privacy and Supporting Ontario's Innovation Economy

To continue the mandate of digital innovation, the Ministry of Government and Consumer Services (MGCS) is seeking to address the gaps in the Ontario's legislative privacy framework, and to establish comprehensive, up-to-date rules that will protect privacy rights and increase confidence in digital services. By exploring key topics in privacy regulation, and considering feedback from Ontarians, we are committed to creating a unique, made-in-Ontario solution to today's privacy challenges, one that suits Ontario's size and complexion, and will nurture innovation for Ontario businesses, associations and other organizations.

To help initiate the conversation with Ontarians, we have identified a series of topics that have influenced privacy regulations around the world. Your feedback will help us to consider how these may apply to Ontario's private sector. We want Ontarians to have more access to and control over their own data when interacting with private businesses and organizations: to be better informed about how their personal information is used and what they are agreeing to when providing it; to be able to withdraw consent and retrieve their data more easily; to be certain that Ontario's businesses will uphold their privacy even in the use of new technologies and digital business models. In addition to protecting the personal information of individual Ontarians, we also want to ensure that any new privacy protections do not pose unnecessary burden to businesses, or inhibit the growth and prosperity of Ontario's innovation ecosystem.

HOW TO PARTICIPATE.

Formal response
If you are an organization, legal or technical expert and wish to submit a formal response to us, you may submit the response to access.privacy@ontario.ca.

Survey
You can also submit your feedback and thoughts through our online survey.
Complete the survey.

Outreach to industries, technical experts, and impacted stakeholders
We will also consult with industries, experts, and other impacted stakeholders regarding legal, technical, and operational elements of modernizing privacy for a digital world.

The consultation period for this proposal will end on **October 16, 2020**.

2 Privacy in Ontario: 2020

Data in a Digital Age: The Need for Privacy

Digital technologies and services have enabled innovation but have also presented new risks such as data breaches, identity theft, surveillance, and commercial data brokerage. Organizations are now collecting more varieties of information from their customers, including physical locations, personal communications and consumer preferences. These developments have made it more difficult for Ontarians to exercise control over the collection, use and disclosure of their personal information. We must ensure that digital transformation takes place in a way which enables the benefits of data-driven innovation but minimizes the risks to impacting Ontarians privacy.

These changes in the digital landscape have generally diminished public confidence in privacy. The current Privacy Commissioner of Canada and author of the 2018-19 Survey of Canadians on Privacy, found that 92% of respondents had some level of concern about the protection of their personal information. Through the recent Consumer Protection Survey and 2019 Data Strategy Consultations, Ontarians have expressed similar concerns. The COVID-19 pandemic has exposed the importance of and urgent need for, digital services for which trust and confidence in the collection, processing, and storage of data remains a barrier to adoption and effective use.

Privacy Laws and Trends: Ontario, Canada and International Jurisdictions

The Province of Ontario does not currently have regulations for privacy in the private sector. The current provincial laws[1] only govern the collection, use and disclosure of personal information by government institutions, and specific health care providers. For the private sector, Ontario instead relies on the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The provinces of Alberta, Quebec and British Columbia however, have chosen to have tailored private sector privacy laws. In early

[1] *Freedom of Information and Protection or Privacy Act (FIPPA), Municipal Freedom of Information and Protection of Privacy Act (MFIPPA),* and *Personal Health Information Protection Act* (*PHIPA)*

2020, Quebec for example, has recently introduced Bill 64, which also strengthens privacy rights and requirements for both public and private organizations.

In 2018, the European Commission introduced the General Data Protection Regulation (GDPR), which significantly strengthened privacy protections in the European Union by introducing more robust requirements for consent, transparency and enforcement, and provided individuals with greater control over their personal data. Many countries and jurisdictions around the world have since updated their statutory frameworks to align with this new global standard. Canada's federal government has indicated its intent to modernize PIPEDA, however to date there have not been any substantial changes.

Exploring Areas of Improvement for Ontario

The series of privacy discussion topics are listed below, and each is explained in further detail in the next section. These topics reflect key areas that the government is exploring to consider a made-in-Ontario privacy law.

1. Increased **transparency** for individuals, providing Ontarians with more detail about how their information is being used by businesses and organizations;

2. Clear **consent** provisions allowing individuals to revoke consent at any time, and adopting an "opt-in" model for secondary uses of their information;

3. Right for individuals to request information related to them be **deleted or de-indexed**, subject to limitations (this is otherwise known as "erasure" or "the right to be forgotten");

4. Right for individuals to obtain their data in a standard and **portable** digital format, giving individuals greater freedom to change service providers without losing their data (this is known as "Data Portability");

5. **Oversight, compliance and enforcement** powers for the Information and Privacy Commissioner (IPC) to support compliance with the law, including the ability to impose penalties where necessary;

6. Introducing requirements and opportunities to use data that has been **de-identified and derived** from personal information, to provide clarity of applicability of privacy protections;

7. Expand the **scope and application** of the law to include non-commercial organizations, including not-for-profits, charities, trade unions and political parties; and

8. Create a legislative framework to enable a more modern privacy regime that would allow for a spectrum of compliance support mechanisms such as the establishment of **data trusts** for privacy protective data sharing.

3 Key Areas for Reform

The topics below reflect new areas of consideration for Ontario based on legal requirements introduced in other jurisdictions, and which many Canadian companies already contend with while conducting business globally. While not an exhaustive list or finalized approach, these topics are aimed to guide the conversation.

Increased Consent and Clear Transparency

In Canada, private sector privacy laws rely on the consent of consumers as the primary legal enabler for the collection and use of their personal information. Organizations are required to publish details about their data collection and use practices in service policies and privacy statements. These policies and statements however are written in dense legal jargon that often seem obscure to individuals when signing up for new services, deterring engagement. The frequency of collection often adds to public confusion; personal information is collected so regularly and automatically that customers cannot be expected to consent each time their information is collected.

To respond to these challenges, the government is now re-imagining consent and transparency requirements, and considering alternative models which better equip Ontarians to make informed choices about their service providers, and to exercise greater control over the collection, use and disclosure of their personal information. Ontario is considering the following options:

- Requiring organizations to offer clear and plain language information about the use of personal information: to state what personal information is collected, how it is collected, how it is used, and with which third parties the information will be shared. Through clear transparency requirements, individuals would understand when and how their personal information is collected, and only be required to consent for collections, uses, and disclosures of personal information that are outside the organization's described practices.

- Clarifying consent requirements would include clarifying exceptions to consent. These may be instances where individual consent is not necessary, practicable or appropriate, such as in instances where the collected data has been "de-identified" or "derived" (see below for definitions and discussion on this topic) and

used to benefit the individual or the overall public good (e.g. for purposes of research or innovation). These exceptions would also be contemplated when considering the overall topic of consent and transparency, and its application to Ontario.

- For all other collections, uses, and disclosures of personal information, the organization would need to obtain affirmative, demonstratable, informed, and unambiguous consent. Requiring individuals to "opt-in" to the collection, use, or disclosure would set the default setting as the most privacy protective option. Enhanced consent and transparency provisions would not allow organizations to collect information unconditionally, but enable more explicit agreement and understanding between individuals and their service providers.

Data Rights: Erasure and Portability

The GDPR takes a rights-based approach to privacy protection, and it has introduced new digital rights concepts that other jurisdictions have adopted. Some of these digital rights already exist within Canadian privacy law, such as the ability to access or correct one's own personal information, or the ability to withdraw consent for an organization to use it. Some digital rights, however, are not currently available to Ontarians. Two of the most prominent of these rights relate to "data portability" and "data erasure."

Data Erasure

Also known as "the right to be forgotten", the right to data erasure permits individuals to request that organizations permanently de-index (remove from online search results or references) or delete their personal information when it is no longer required to deliver a service. This principle can be applied where the individual has withdrawn consent for the organization to use their information, or where the use of the information was illegal in the first instance. This right has become increasingly relevant in an era of digital services; it empowers individuals to manage their privacy and reputation more directly.

Even where it has been implemented, the right to erasure is not unlimited, and a made-in-Ontario solution would be careful not to overextend this requirement so that it becomes impractical for organizations to follow. In the GDPR, for example, the right to erasure does not apply when the data is necessary for exercising the right of freedom of expression, complying with a legal obligation, performing a task carried out in the public interest, or in the exercise of official authority. The right can also be limited for reasons of public interest, including public health, archiving, scientific, historical or statistical research, or for the establishment, exercise or defense of legal claims.

Data Portability

The right to data portability empowers Ontarians to access one's own personal information. Specifically, this right allows individuals to request that their personal information be provided to them in an open and accessible format. = Data portability will give individuals a greater degree of control over their personal data. An individual would have =the right to extract all of their data from a business or organization (for example, a social media platform) and transfer it in a structured, readily useable and possibly standardized form to a different platform that offers a similar service.

Data portability allows consumers to 'vote with their feet'. An alternative service provider may offer greater privacy protections or better services. This may create greater competition among service providers, foster innovative new goods and services, and allow individuals to switch service providers more easily without losing access to their own data.

Oversight, Enforcement, and Fines

Privacy regulations are only effective if they are followed. There are a variety of tools, that may be employed to assist and encourage organizations to observe the regulations. This may involve including an expanded mandate for the IPC to provide advice and guidance to small organizations. The IPC is in a unique position to work constructively with Ontario's private sector – as they already do with public institutions – to provide best practices for making organizations more privacy protective.

Compliance strategies can range from education, research, guidance, and advisory services, to regulatory sandboxes. The COVID-19 pandemic has required many businesses to digitize services overnight, without building a robust privacy and cybersecurity architecture. An effective privacy regime would not take a "one size fits all" approach, but to set out different strategies for small, medium, and large organizations, and incentivize compliance by setting positive examples, championing best practices and encouraging innovative solutions.

Though this proactive, positive approach to compliance would be preferred, a regulatory toolbox would not be complete without the ability to enforce the law. Penalties are one way of empowering the IPC to enforce compliance. One of the key features of privacy reform in other jurisdictions, is the power for an oversight body to issue orders to organizations found in violation of the law, and to levy fines in severe cases of non-compliance. In Europe, these fines can amount to €20 million, or 4% of a company's annual revenue.

This power to levy orders and fines is generally absent from the Canadian privacy enforcement regime. The Privacy Commissioner of Canada can currently investigate complaints and issue non-binding recommendations and public reports about an organization's privacy practices. Meanwhile, Ontario's IPC can issue binding orders to FIPPA, MFIPPA (only for access) and PHIPA (for access and privacy). In the absence of an Ontario private sector law, these order-making powers do not extend to the collection, use or disclosure of personal information by private sector organizations.

Empowering Ontario's enforcement regime is crucial to modernizing privacy protections. For example, enabling the IPC to issue binding, privacy-related orders to organizations would ensure that these organizations remained compliant in upholding the privacy rights of individuals. Issuing fines under a penalty structure could support the public's confidence that enforcement is meaningful, and therefore encourage good privacy practices among commercial actors. Enhanced oversight and accountability could also enable the IPC to process public complaints, initiate investigations, require organizations to report substantial privacy breaches, or to take public action in response to privacy investigations.

Application to Non-commercial Organizations

The federal privacy law, PIPEDA, applies to organizations that collect, use or disclose personal information in the course of commercial activities. If an organization engages in transactions that relate to selling, bartering or leasing, it must abide by PIPEDA. The federal law does not however apply to other types of personal information – such as employee related personal information, genetic data, biometric data – that do not relate to an organization's commercial activities (some exceptions include federally regulated organizations like banks, airlines, telephone or broadcast companies).

As a result, many types of organizations operating in Ontario are currently not subject to any privacy laws. These organizations include not-for-profits, charities, professional associations, trade unions and political parties. This is a significant gap in Canada's privacy framework. Alberta, British Columbia's and Quebec have all introduced private sector privacy laws that have broader applications, and include all organizations that collect, use and disclose personal information.

When considering privacy reform for Ontario's private sector, the scope and application of protections is a significant consideration. It seems essential to any modern privacy regime that sensitive personal information be protected regardless of whether it is held by a commercial business, or by a not-for-profit. Consistent rules for all types of private sector organizations would help ensure Ontarian's privacy is consistently protected.

Deidentified Personal Information, Data Derived from Personal Information

The modern innovation economy is fueled by de-identified data, not too dissimilar from the way oil fueled the economy of the 20th century. “Deidentified” data is personal information that has been pooled in a manner that would prevent the identification of any individuals’ personal data in the mix. Methods of deidentification include the removal of “identifiers” (e.g. removing names, identifying numbers), obscuring information (e.g. giving an age range in place of exact age), and removing or aggregating information about outliers or small cell size data subjects (e.g. where fewer than five people have the same postal code).

Data that is “derived” from personal information is data that companies may have about customers that was not directly supplied by the customer. This kind of data (such as assessments or evaluations) repurposes personal information that has been previously supplied, as well as other recorded behaviour (such as web-browsing habits). For example, companies may categorize customers based on observed shopping habits, or develop other insights about an individual’s routine actions.

In Canada, this kind of data does not fit neatly into the privacy protection framework. There is no clear set of rules on how deidentified personal information, or data derived from personal information, must be managed by organizations. To bring clarity to organizations, and confidence to Ontarians, the Province of Ontario may consider defining these concepts more clearly in law and setting clear guidelines for how privacy rules apply to these types of data. Since the use of de-identified data reduces the risk of privacy breaches, we will consider ways of encouraging organizations to improve and develop these practices within the private sector, such as offering incentives for companies to design privacy protective applications, or supporting the creation of new technical standards.

Enabling Data-sharing for Innovation, while Protecting Privacy

Privacy laws set limits on how organizations can share personal information. Though these limits are important, they often pose challenges to research and innovation. Data silos can hinder innovation by reducing the number of groups or sectors who can use the data to develop new insights or enhance services.

Emerging data governance models – where personal information, deidentified personal information, or aggregate data, can be shared among different actors or sectors – could help to drive innovation for the public good, or for a common interest among specific organizations. By bringing together data from different sectors and actors, the value of the data can be unlocked for new purposes in the public interest.

Sometimes referred to as “data trusts,” these emerging data governance models allow organizations to assign an individual as the custodian or steward for the data, agree on a standard set of rules for how data would be shared, and ensure that whoever has access to the trust uses the data in accordance with these rules. While data trusts are still a relatively new concept, establishing guidelines, principles or standards for the use of these trusts may open new models for privacy protective data sharing, promoting collaboration, economic development, and innovative solutions to societal issues.

Your privacy matters

We are requesting your feedback in order to help us understand the privacy concerns of Ontarians and how to best address these concerns through either policy, law or regulation.

This feedback will be used by the Ministry of Government and Consumer Services to help us develop a privacy protection framework for Ontario that meets your needs.

If you provide your email address, it will not be associated with your feedback and will only be used to update you on this initiative and notify you about future consultations. Your email address will not be placed on mailing lists or released to any third party, except as may be authorized by law.

For questions on how information collected on this page will be used, please contact us:

Manager of Access and Privacy Strategy and Policy Unit
Ministry of Government and Consumer Services
Enterprise Recordkeeping, Access and Privacy Branch
134 Ian Macdonald Blvd.
Toronto, Ontario
M7A 2C5