Modernizing Privacy in Ontario

Empowering Ontarians and Enabling the Digital Economy

WHITE PAPER

Caution:

The provisions included in this white paper are intended to facilitate dialogue concerning its contents. Note that it will not become law unless a bill is passed by the Legislative Assembly of Ontario. Should the decision be made to introduce a bill in the Legislative Assembly, the comments received during consultation will be considered during the preparation of the bill. The content, structure, form and wording of both language versions of the consultation draft are subject to change as a result of the consultation process and as a result of review, editing and correction by the Office of Legislative Counsel.

1 Introduction

The Government of Ontario's vision is to make Ontario the world's most advanced digital jurisdiction. As outlined in the government's recently announced Digital and Data Strategy, this goal supports Ontarians with the skills, rights, and opportunities to fully participate, work, and thrive in the digital world. Businesses will benefit from new investments in broadband and public data infrastructure, while people will benefit from increased access to reliable, user-designed online government services.

Paramount to this work is digital privacy, and ensuring Ontarians have the power to control what personal data they share, when they share it, and with whom they share it. This is a priority of the Ontario government. Especially with the COVID-19 pandemic requiring millions of Ontarians to live their lives almost fully online, it is essential for the future of our economy and the well-being of our people to update our privacy laws.

In Ontario, privacy in the private sector is governed by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Last year, the Government of Canada introduced Bill C-11, *The Digital Charter Implementation Act,* to replace PIPEDA and modernize the federal privacy regime. While it includes some welcomed new developments, the proposed law has several points of weakness: its consent framework could allow organizations to collect and use citizens' data for commercial interests without their knowledge; it does not provide special protections for children and youth; and its digital rights do not go far enough to protect individuals from new risks

such as surveillance. As Daniel Therrien, the Privacy Commissioner of Canada, recently stated, “I believe that C-11 represents a step back overall from our current law and needs significant changes if confidence in the digital economy is to be restored.”

The Government of Ontario is committed to addressing these gaps. After carefully considering the feedback received during our 2020 privacy reform consultation[1], including from the Information and Privacy Commissioner of Ontario (IPC), as well as commentary from privacy experts on Bill C-11, Ontario is considering proposals that would implement a fundamental right to privacy for Ontarians, introduce more safeguards for artificial intelligence (AI) technologies, introduce dedicated protections for children, update consent rules to reflect the modern data economy, promote responsible innovation and correct the systemic power imbalances that have emerged between individuals and organizations that collect and use their data.

Ontario’s Information and Privacy Commissioner’s thoughtful submission applauds the government for initiating dialogue on these important questions. In her submission, Commissioner Patricia Kosseim identifies the need for a modern privacy regulatory regime that is principles-based, fair and well-balanced, pragmatic, flexible, and proportionate, noting that, “Consumers, businesses, and government have all come to the shared realization that privacy protection, far from impeding innovative solutions, is key to enabling their success.”

This white paper outlines Ontario’s proposals and provides examples of legislative language that demonstrate how these protections could be reflected in law. These proposals are aligned with the government’s Digital and Data Strategy and build on recent efforts to improve health privacy in the *Personal Health Information Protection Act* (PHIPA). These proposals, if introduced, would harmonize with Ontario’s other privacy laws, and minimize regulatory burden for Ontario organizations.

In brief, the proposals in this paper are organized by the following themes:

- rights-based approach to privacy;
- safe use of automated decision-making;
- enhanced consent and lawful uses of personal data;
- data transparency for Ontarians;
- protecting children and youth;
- a fair, proportionate and supportive regulatory regime; and
- support for Ontario innovators.

[1] We received a wide range of feedback and participation in the consultation: 175 organizations consulted, 14 sectoral roundtable meetings, 97 written submissions, 20 interviews with academic and legal privacy experts, 929 online survey responses, and 2 virtual townhall meetings.

These proposals will only be meaningful if their protections are comprehensive. The scope of the federal privacy regime is limited to commercial activities. This means that many private sector organizations, including charities, unions, associations and other non-profits, are not covered under the proposed bill, despite the collection and use of Ontarians' personal information by these organizations. To close this gap, the province is considering expanding the scope of privacy requirements under each of these themes to include non-commercial organizations, ensuring that Ontarians' personal information receives adequate coverage and protection in every aspect of life.

During the development of this white paper, the Office of the Privacy Commissioner of Canada (OPC) independently brought forward thoughtful feedback to the federal government on Bill C-11 via a public submission. While this submission does not directly address Ontario's privacy proposals, we encourage you consider the OPC's report and recommendations as well when responding to this white paper. For well-considered commentary from Ontario's Information and Privacy Commissioner on Ontario's privacy proposals, please see its public submission.

2 Key Areas of Reform

Rights-based approach to privacy

Problem:

With rapid advances in technology that vastly expand the ability of organizations to collect, use, and share personal information, new rules and rights are needed to protect Ontarians from potentially unfair practices and maintain a high level of trust and confidence in the digital economy.

Goal:

Consistent with the recommendations of the OPC, Ontario could establish a fundamental right to privacy as the underpinning principle for a provincial privacy law, ensuring that Ontarians are protected, regardless of commercial interests.

*

In the 2020 provincial consultation on privacy reform, Ontarians expressed a reasonable level of concern that their data is not protected when privacy competes with the interests of organizations. This concern has resulted in mistrust and uncertainty about data practices across the province. Privacy is not merely an individual concern; rather, it is part of the social capital of a democratic society, interrelated with freedoms of speech, expression and association. Many experts have advocated that the value of privacy is

therefore best expressed as a fundamental right, rather than as a balance of competing interests.

Privacy is recognized under *the Universal Declaration of Human Rights*, and Europe's *General Data Protection Regulation* (GDPR) is based on a framework of individual data rights. However, the federal system is limited to commercial activities, and Canada's laws have generally fallen short of taking an overtly rights-based approach. Quebec is an exception, as its private sector privacy law recognizes and implements the right to privacy explicitly set out in the Quebec *Charter of Human Rights and Freedoms* and *Civil Code.*

Ontario is considering whether to recognize a fundamental right to privacy in Ontario. This approach could take the form of a preamble that would outline this fundamental right in the following manner:

> **Preamble**
> Privacy is a foundational value in society. Every individual is entitled to a fundamental right to privacy and the protection of their personal information.
>
> Changes in technology have allowed organizations to easily collect vast amounts of personal information about individuals, often undermining the control that an individual has over their personal information.
>
> To establish the trust and confidence of individuals, organizations must be subject to rules, guided by principles of proportionality, fairness and appropriateness with respect to the collection, use or disclosure of personal information.

A key factor in establishing public trust and confidence in the right to privacy will be the provision of genuine transparency requirements and strong, independent oversight for Ontarians. These features will be outlined in forthcoming sections. It will also require a clear definition of personal information that addresses the highly variable forms in which data is found and used. In today's landscape, organizations often use information that has been de-identified from its original state (see Supporting Ontario Innovators), or information that has been derived or inferred from personal information by evidentiary reasoning or other analytical processes. While there may some utility in keeping a definition of personal information that is simple, clear and distinct from these derivations, a modern privacy regime nevertheless must decide how to address data appearing in different forms. We welcome feedback from Ontarians as to how best to strike this balance if these terms were contemplated by a forthcoming privacy law.

Fair and Appropriate Purposes

One protection for individuals in modern privacy laws is a requirement that organizations only collect, use and disclose individuals' personal information for purposes that are objectively fair and appropriate in the circumstances. The concept of "fair and appropriate" is an overarching protection that sets the parameters of permissible activity. It provides that information can only be collected, used and disclosed for purposes that an individual would reasonably expect, regardless of which lawful grounds for collecting, using and disclosing personal information may apply. This means that an organization would need to satisfy this criterion whether the organization has obtained consent, or another legal authority is relied upon. Ontario is considering setting out these provisions in the following manner, to have a similar limitation for the collection, use or disclosure of personal information as in federal Bill C-11 and other existing Canadian privacy laws:

Appropriate purposes

(1) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider fair and appropriate in the circumstances.

Factors to consider

(2) The following factors must be considered in determining whether the purposes referred to in subsection (1) are fair and appropriate:

1. The volume, nature and sensitivity of the personal information, including whether the organization has taken steps to de-identify the personal information.

2. Whether the collection, use or disclosure is necessary to achieve the legitimate needs of the organization.

3. Whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits.

4. Whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

Purposes

(3) An organization shall determine at or before the time of the collection of any personal information each of the purposes for which the information is to be collected, used or disclosed and record those purposes.

Legitimate needs

(4) For the purpose of paragraph 2 of subsection (2), the legitimate needs of an organization do not include,

(a) the monitoring or profiling of an individual under the age of 16 for the purposes of influencing the individual's behaviour or decisions;

(b) purposes that are known to cause, or are likely to cause, significant harm to the individual or groups of individuals;

(c) any purpose that would contravene a law of Ontario or of Canada; or

(d) any other prescribed purpose.

To complement the concept of fair and appropriate purposes, Ontario is also considering a general requirement for organizations to limit their collection, use and disclosure to only that personal information that is necessary to carry out its intended purpose. This provision of limitation supports a "less is more" principle of data minimization, which could further help to establish a consistent and lawful framework that enshrines Ontarians' right to privacy.

LIMITING COLLECTION, USE AND DISCLOSURE

Limiting collection, use and disclosure

An organization may collect, use or disclose personal information only if,

(a) the personal information is necessary for the purposes determined and recorded under [subsection]; and

(b) the organization obtains the individual's consent in respect of the collection, use or disclosure or the organization is otherwise permitted to collect, use or disclose**,** as the case may be,

While Bill C-11 does require that a collection, use or disclosure of personal information be "appropriate in the circumstances", the fairness requirement could strengthen this foundational component of Ontario's privacy framework. Ontario's Information and Privacy Commissioner noted that the principle of fairness (among others) is conspicuous in its absence from PIPEDA and should be clearly articulated in any modern privacy law. The inclusion of "fairness" would be intended to reinforce a more citizen-oriented interpretation of the law and embed these purposes within the rights-based principles outlined in the preamble. To enhance this aspect of the law as compared to Bill C-11, Ontario could require organizations to consider the volume and

nature of the information in addition to its “sensitivity.” To make the latter more meaningful, Ontario may also consider, like Europe’s GDPR and Quebec’s Bill 64, providing a definition for sensitive information that informs the application of these principles. This definition could be based on risk, or based on specific classes or categories of information. Many privacy experts have recommended a definition combining both approaches.

The requirement to have a “fair and appropriate purpose” could also be formulated to account for other relevant factors. For example, it could also require organizations to consider whether they have taken steps to de-identify the information. Significantly, Ontario could also clarify the concept of “legitimate need” for personal information by introducing specific limitations, such as prohibiting purposes that could cause harm to individuals or groups or contravene other provincial or federal laws. (The possible prohibition related to monitoring and profiling for individuals under 16 years of age, captured by one of the above provisions, will be presented in an upcoming section.)

The proposed provisions outlined above demonstrate a privacy-first approach that establishes clear privacy rights for individuals and limits organizations to collecting, using and disclosing personal information only for legitimate purposes that a reasonable person would find fair and appropriate under the circumstances. By limiting the collection, use or disclosure of personal information to objectively “fair and appropriate” purposes, these proposed provisions would establish principle-based boundaries that organizations must stay within – and would have to meet – if they are to collect, use and disclose Ontarians’ personal information. These boundaries could, consistent with other modern privacy laws, precede all other authorities outlined in the law, and therefore play an integral role in upholding Ontarians’ fundamental right to privacy.

Data Rights of Mobility, Disposal, Access and Correction

The overall right to privacy is supported by affirming important data rights that allow Ontarians to access, correct, transfer and dispose of their own personal information. The right of access to one’s own personal information, and the right to request its correction, are found in modern privacy laws, notably PIPEDA, Alberta’s and British Columbia’s privacy laws, and Quebec’s existing law. The right of individuals to obtain and transfer their own information, known as “data mobility” or “data portability,” is now found in Europe’s GDPR, Canada’s Bill C-11, and Quebec’s Bill 64. All of these rights are now considered to be essential features of modern privacy regimes.

Another right found in more recent laws is the right for individuals to require organizations to, subject to certain limitations, dispose of their personal information. Ontario is also considering a right to disposal, also known in some jurisdictions as the right to erasure or deletion, along these lines:

Disposal at individual's request

(1) If an organization receives a written request from an individual to dispose of personal information that it has collected from the individual, the organization shall, as soon as feasible, dispose of the information, unless,

(a) disposing of the information would result in the disposal of personal information about another individual and the information is not severable;

(b) there are other requirements of this Act, another Act or an Act of Canada or an Act or regulation of Ontario or Canada or of the reasonable terms of a contract that prevent the organization from disposing of the information;

(c) the personal information has been disclosed in the course of a legal proceeding or is otherwise available to a party of a legal proceeding; or

(d) such other circumstance, as may be prescribed, exist.

Ontario welcomes public feedback to inform the appropriate scope and limitations of this right. For instance, the Privacy Commissioner of Canada has recommended that the right of erasure should include all information that an organization holds about an individual, including from third parties such as data brokers, rather than just information that was collected from them directly. The Information and Privacy Commissioner of Ontario has also recommended that minors deserve special consideration with respect to erasure, to support youths' freedom of experimentation and self-discovery at a young age without worrying about the permanence of information they post about themselves online. As part of this right to disposal, Ontario may also consider a requirement for organizations to provide reasons to the individual in instances where a request is refused, and inform the individual of the available recourse. Disposal requirements would also extend to any service providers that may have received the information to help carry out the purposes of the original collection.

Disposal by service provider

If an organization has transferred personal information to a service provider and the organization subsequently disposes of the information, the organization shall, as soon as feasible,

(a) if the organization received a request from an individual, inform the service provider of the individual's request;

(b) ensure that the service provider disposes of the information; and

(c) obtain a confirmation from the service provider that the information has been disposed of.

In addition to the individual's right to request destruction of personal information that they themselves provided, Ontario may also consider the possibility of exceeding the federal right of disposal, enshrining a requirement for organizations to de-index search results that contain personal information about an individual that has been posted by others. This "right to be forgotten," if introduced, would be subject to countervailing freedom of expression concerns and considerations, similar to the equivalent provision included in Quebec's Bill 64 (s.28.1).

Turning to data portability, Ontario is considering a proposal that would allow individuals to request a machine-readable copy of their data from an organization, enabling them to transfer their business to another provider. Notably, this right would need to be informed by sector-specific standards that would help establish consistent technical requirements and expectations for the organizations that would respond to those requests. For instance, the Privacy Commissioner of Canada has recommended, in reference to Bill C-11, that data mobility rights should extend to "inferred information" (described above). Ontario welcomes views on these questions of scope, and on how best to clarify the appropriate limitations of this right to ensure that it meets the intended goal without becoming impracticable for the organizations that would be implementing it.

If this right is introduced, Ontario would work with various sectors across the province to develop these standards – in line with the Information and Privacy Commissioner's recommendations in response to the 2020 privacy reform consultation. Providing individuals with this right could enhance competition among, and innovation by, service providers. A data probability right could be enabled by provisions like this:

Disclosure under data mobility framework

(1) Subject to the regulations, on the written request of an individual, an organization shall as soon as feasible disclose the personal information that it has collected from the individual to an organization designated by the individual, if both organizations are subject to a data mobility framework provided under the regulations.

Requirement to inform re disposal

(2) If an organization receives a request from an individual under subsection (1), the organization shall inform the individual that they may make a request to have the organization dispose of their personal information.

Finally, Ontario is considering providing individuals with a right to access and correction of their personal information which is in the custody of an organization. This right is

similar to that found in other Canadian and international privacy laws, as well as the access and correction rights currently provided by the *Freedom of Information and Protection of Privacy Act.*

> **Information and access**
> (1) On request by an individual, an organization shall inform them of whether it has any personal information about them and about the use or disclosure of the information. It shall also give the individual access to the information.
>
> **Names or types of third parties**
> (2) If the organization has disclosed the information, the organization shall also provide to the individual the names of the third parties or types of third parties to which the disclosure was made, including in cases where the disclosure was made without the consent of the individual.
>
> **Automated decision system**
> (3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization shall, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained.

The right of access would be an important tool for Ontarians to track the use of their data and ensure its accuracy across organizations and platforms. (The proposed transparency requirement for automated decision-making will be outlined further in the next section.)

Discussion Questions:

- Does the proposed preamble in this section include the right principles, reasons and values to guide the interpretation of a potential privacy bill?
- How should the concepts of personal information, and “sensitive” personal information, be defined in law?
- Do the “fair and appropriate purposes” proposed in this paper provide adequate and clear accountability standards for organizations and service providers?
- How far should the data rights of erasure and mobility extend? Should they include all information an organization has about an individual, or only the information the individual provided?

Safe use of automated decision-making

Problem:

It is clear that AI technologies, such as automated decision systems, offer significant benefits for organizations and the economy. However, new risks such as surveillance and algorithmic bias have emerged that necessitate greater accountability. Bill C-11 improves Ontarians' rights to algorithmic transparency but does not include protections that are available to citizens in other jurisdictions.

Goal:

Building off the Government's public consultations to create a trust framework for AI, Ontario could prohibit the use of AI and automated decision-making systems when they could cause harm to citizens, provide stronger rights to inform Ontarians when and how their data is used by these technologies, and empower them with a right to object to these uses, or at least to contest them.

*

AI has revolutionized the modern data landscape. Many sectors in Ontario have adopted machine-learning technologies to assist or substitute human analysis and decision-making. While these technologies offer valuable innovations, they have also increased the capabilities for surveillance in modern society, and therefore heightened the associated risks for individual rights. Artificial Intelligence allows organizations to link data from different sources to analyze and predict complex patterns of activity, infer highly sensitive information about individuals, monitor their movements and behaviours, and influence their actions – sometimes without the individual's knowledge or control. While surveillance does not always require AI, and not all AI processes amount to surveillance, the intersection of these practices can pose undue risk for citizens. These advanced surveillance capabilities can compromise Ontarians' rights and freedom and create a significant power imbalance between individuals and the organizations that use their data.

Profiling and Automated Decision-Making

Legislators in many jurisdictions, including Europe and Quebec, are responding to AI by giving individuals rights to know about its use, and to comment on, object to, or contest the use of AI. These AI-related rights recognize AI's implications for the fundamental right to privacy and other rights. While AI can, again, yield benefits, Ontario could provide similar rights for individuals. This section will outline these proposed requirements as they relate to profiling and automated decision-making.

The term "profiling" usually refers to the practice of using personal information to create representational descriptions of an individual's features, activities or attributes. Ontario is considering the following definition of profiling:

> "profiling" means any form of automated collection, use or disclosure of personal information to evaluate, analyse or predict aspects relating to an individual;

Although profiling is a long-standing practice, advances in AI now enable organizations to draw from diverse sources to create more comprehensive data sets. Profiles have become essential to the administration of many kinds of commercial activities (mobile app services, online retail) and non-commercial activities (statistical studies, health and social services). However, more insightful profiling comes with proportionate risks to individuals. When profiling is the basis for a decision that significantly affects an individual, a false prediction carries a high risk of harm. As more of Ontarians' everyday lives are shared and managed through online platforms, there is more data available to create profiles, and higher risks to citizens' privacy. When profiled data is used with AI to make decisions about individuals, for example employment decisions, it becomes a form of "automated decision-making," which Ontario is proposing to define as

> "automated decision system" means any technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets;

These automated decision systems (or "ADS") are now used frequently around the world to evaluate eligibility for programs, assess candidates for jobs, and market products based on user preferences. When they are used to automate repetitive, structured processes, ADS technologies help both people and businesses by making decisions involving large volumes of data more efficient. Risk of harm and discrimination increases, however, when these technologies are used to make decisions that involve sensitive personal data or could significantly impact an individual. To date, the use of ADS is obscure; people have limited knowledge of the technology being used, and no

recourse to address any problems that occur when ADS is used without sufficient human supervision.

As already noted, many jurisdictions have already taken steps to balance the use of these technologies with individual rights. Europe's GDPR provides individuals with a right not to be subject to ADS for sensitive categories of data, or where the decisions could produce legal or other significant results. It also empowers individuals to contest ADS decisions in these situations and to request a human review.

Canadian jurisdictions that have recently followed suit include Quebec, as Quebec's Bill 64 would provide individuals with a right to be informed about ADS decisions, including the reasons and the principal factors and parameters that led to the decision, and an opportunity to submit observations to someone in the organization who is in a position to review the decision. Also, Bill C-11 would require businesses to provide an account of their ADS use and, upon request, an explanation of how ADS impacted a particular decision.

These ADS guardrails signal a significant step in protecting individuals and preventing harmful practices, while enabling organizations to continue to use AI responsibly. Ontario is considering building on these protections, beginning with the following provision:

> **Automated decision system**
> (3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization shall, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained.

Clear information about the use of ADS is important; however, explanations are not sufficient to restore control to Ontarians. Individuals must also be protected from these systems when their use could have serious implications, i.e., cause legal or financial injury, reputational damage, or even endanger health and safety. Ontario is considering following the model of the GDPR to prohibit the use of ADS in situations of *significant* impact, subject to some important exceptions:

> **Prohibition re automated decision making**
> (1) An organization shall not use an automated decision system to make a decision about an individual, including profiling, if the decision would significantly affect the individual, unless,

(a) such a decision is necessary for entering into, or the performance of, a contract between the individual and the organization;

(b) such a decision is otherwise authorized by law; or

(c) the organization obtains the individual's express consent to the use of an automated decision system to make a decision that could significantly affect the individual.

This prohibition could provide important safeguards for Ontarians and give consumers confidence that their data cannot be used in unlimited ways. Businesses also would benefit from this greater level of certainty and consumer confidence. However, this protection would be incomplete without the additional right for Ontarians to control and participate in this process, i.e., to understand the meaning and impact of a decision, and to intervene in the decision if it could jeopardize their interests or well-being. In this regard, Ontario is considering giving more control to Ontarians through the following requirements:

Same

(2) If an organization has used an automated decision system to make a decision to which subsection (1) would apply about an individual, the individual may do any of the following:

1. Request the personal information used to render the decision.

2. Request the reasons and principal factors and parameters that led to the decision.

3. Request the correction of personal information used to render the decision.

4. Comment on the decision.

5. Contest the decision.

6. Have the decision reviewed by an individual within the organization with sufficient knowledge to review.

Greater knowledge and control over the use of their data by ADS could allow for a fairer and more proportionate balance of power between individuals and organizations, and ensure that these protections are interoperable with those in other jurisdictions. To enhance organizations' responsiveness to individuals' requests, and to further improve

accountability, Ontario may also consider providing more detailed recordkeeping requirements related to the use of ADS, such as requiring organizations to log and trace the collection and use of personal information in that context. As this recordkeeping requirement would almost certainly add more burden for organizations, the province welcomes feedback to inform its usefulness and practicality, and any other factors – such as the size/scale of organization, or sensitivity of information – that could inform its application and its potential inclusion in the law. Although machine-learning technologies are not limited to profiling and ADS, these rights could provide a foundation upon which Ontario could continue developing a more detailed and comprehensive AI governance regime.

Discussion Questions:

- Do the example provisions provided in this section offer adequate protection for Ontarians whose information is subject to ADS practices?
- Does the proposed regulatory approach for ADS strike the right balance to enhance privacy protections, while enabling new forms of socially beneficial innovation in AI?
- Should there be additional recordkeeping or traceability requirements to ensure that organizations remain accountable for their ADS practices?
- Are there additional requirements or protections that Ontario may consider related to the use of profiling?

Enhancing consent and other lawful uses of personal information

Problem:

While individual consent to collection, use or disclosure of personal information is an essential component of privacy laws, it is widely recognized that the modern data landscape is now too complex to rely upon it as the sole authority for these practices. The complexity of the modern data ecosystem also challenges individuals' understanding of and ability to consent, often leading to consent fatigue, whereby consent is given but is not well-informed. Canada's Bill C-11 and Quebec's Bill 64 both recognize this circumstance. They enhance consent processes while – as existing privacy laws already do – providing exceptions to consent. However, the Bill C-11 proposals may not adequately protect Ontarians; accordingly, Ontario is considering the enhancements set out below.

Goal:

Ontario could improve the meaningfulness of consent by making it more informed, while providing alternate authorities for collecting and using personal information to reduce consent fatigue and ensure that organizations cannot use uninformed individual consents as a means to exploit citizens' data.

*

One of the foundational components of a privacy law is the framework of authority permitting organizations to collect, use and disclose the personal data of individuals. Privacy laws typically permit organizations to collect only personal information that is necessary to fulfill legitimate and stated purposes (this was also discussed above in the "Rights-based approach to privacy"). In Canadian privacy law, and in Bill C-11, individual consent is the primary legal basis that organizations may rely upon to process personal data. These laws also provide exceptions to address situations where obtaining consent is not possible or necessary.

Strengthening the authority of consent is an important first step to build out this privacy framework. However, while consent is a significant part of privacy protection, consent-based frameworks also pose their own challenges and limitations. For example, broad consent requirements result in the proliferation of legal notices and dense privacy policies. This leads to "consent fatigue," wherein individuals will click "accept" to any legal notice they receive when signing up for a service without reading or understanding the terms to which they are agreeing. This is exacerbated by the fact that many privacy notices are lengthy, legalistic and complicated. Some organizations may use densely worded notices to conceal permissions for secondary uses and obtain permission for practices that are unfair and inappropriate, and that many Ontarians would not reasonably expect. Ontarians might justifiably object to such terms if they could fully understand the corresponding risks and consequences, but they are not given the information they need to truly understand them.

To countervail these risks of misusing consent, an Ontario privacy law could stipulate certain information for organizations to provide for consent to be considered valid; these potential requirements will be outlined in the next section on transparency. Ontario could also provide the right to withdraw consent, require sensitivity of the personal information to be considered when determining the form of consent, and prohibit organizations from making consent a condition for a service, or obtaining it by deceptive or duplicitous means. These requirements, if introduced, would be consistent with those provided in Canada's proposed Bill C-11.

In today's modern digital landscape, where data is continually collected and information flows are complex, Ontario needs alternative, privacy-protective authorities to collect

and use personal information. In Bill C-11, these alternatives are framed as exceptions to consent, which remains the default central authority. Ontario is considering framing these exceptions as instances in which personal information can be collected, used or disclosed as alternatives to consent.

Before turning to those alternatives, it must be noted that, as is the case under existing Canadian privacy laws, Ontario is considering allowing organizations to rely on implied consent under certain circumstances, taking into account the sensitivity of the personal information involved and the reasonable expectations of the individual. This would also help reduce "consent fatigue" for Ontarians.

In addition, individuals would not be required to provide consent for the collection, use or disclosure of personal information beyond what is necessary to receive a service or product, and also would have the ability to withdraw their consent by giving notice to the applicable organization.

Many of the possible grounds outlined below for collecting, using and disclosing personal information without requiring consent are already common in Canadian privacy laws, although they are now generally framed as 'exceptions to consent'. The grounds proposed below are also generally consistent with those provided in Bill C-11, although as seen later, could improve on Bill C-11.

Business activities

(1) An organization may collect or use an individual's personal information if the collection or use is made for a business activity described in subsection (2) and,

(a) a reasonable person would expect such a collection or use for that activity; and

(b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions.

List of activities

(2) Subject to the regulations, the following activities are business activities for the purpose of subsection (1):

1. An activity that is necessary to provide or deliver a product or service that the individual has requested from the organization.

2. An activity that is carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk.

3. An activity that is necessary for the organization's information, system or network security.

4. An activity that is necessary for the safety of a product or service that the organization provides or delivers.

5. Any other prescribed activity.

The potential list of activities outlined above are very similar to those provided in the proposed Bill C-11. However, Ontario is concerned about addressing provisions that have received criticism in the federal bill. Specifically, Bill C-11 includes the following among its permitted business activities: "an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual." If passed, this provision in Bill C-11 could allow for businesses to collect and use Ontarians' data without consent simply on the basis of convenience or expedience.

Accordingly, the government is considering omitting that particular permitted category of collection, use and disclosure. Similarly, experts have also raised concerns about the possibility of allowing "any other prescribed activity" (see paragraph (2) 5, above) to be added by regulation rather than by statutory amendment, noting that this could also dilute the strength of the protections. The government welcomes feedback on this proposal, and on the list of other activities to make sure that they are scoped properly and do not create unintended consequences that could weaken protections for Ontarians.

The list of permitted categories continues as follows:

Prospective business transaction

(1) Organizations that are parties to a prospective business transaction may use and disclose an individual's personal information if,

(a) the information is de-identified before it is used or disclosed and remains so until the transaction is completed;

(b) the organizations have entered into an agreement that requires the organization that receives the information,

(i) to use and disclose that information solely for purposes related to the transaction,

(ii) to protect the information by security safeguards appropriate to the volume, nature and sensitivity of the information, and

(iii) if the transaction does not proceed, to return the information to the organization that disclosed it, or dispose of it, within a reasonable time;

(c) the organizations comply with the terms of the agreement mentioned in clause (b); and

(d) the information is necessary,

(i) to determine whether to proceed with the transaction, and

(ii) if the determination is made to proceed with the transaction, to complete it.

Completed business transaction

(2) If the business transaction is completed, the organizations that are parties to the transaction may use and disclose the personal information referred to in subsection (1) if,

(a) the organizations have entered into an agreement that requires each of them,

(i) to use and disclose the information under its control solely for the purposes for which the information was collected or permitted to be used or disclosed before the transaction was completed,

(ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and

(iii) to give effect to any withdrawal of consent;

(b) the organizations comply with the terms of the agreement mentioned in clause (a);

(c) the information is necessary for carrying on the business or activity that was the object of the transaction; and

(d) one of the parties notifies the individual, within a reasonable time after the transaction is completed, that the transaction has been completed and that their information has been disclosed under subsection (1).

Exception
(3) Subsections (1) and (2) do not apply to a business transaction of which the primary purpose or result is the purchase, sale or other acquisition or disposition, or lease, of personal information.

Disclosure to service provider
(1) An organization may disclose an individual's personal information to a service provider.

Use by service provider
(2) A service provider to which personal information has been transferred by an organization may use the information only for the same purpose for which it was collected by the organization.

De-identification of personal information
An organization may use an individual's personal information to de-identify the information.

Research and development
An organization may use an individual's personal information for the organization's internal research and development purposes, if the information is de-identified before it is used.

Authorized or required by law
An organization may collect, use or disclose an individual's personal information if the collection, use or disclosure, as the case may be, is authorized or required by an Act or regulation of Ontario or Canada.

Disclosure to law enforcement agency
An organization may disclose an individual's personal information to a law enforcement agency in Canada if there are reasonable grounds to believe that an offence has been committed and the disclosure would enable the law enforcement agency to determine whether to conduct such an investigation.

Investigation or legal proceeding
An organization may collect, use or disclose an individual's personal information if the collection, use or disclosure is reasonable for the purposes of an investigation or legal proceeding.

Collection of employee's personal information
An organization may collect, use or disclose personal information about an employee if the information is collected, used or disclosed solely for the purposes of,

(a) establishing, managing or terminating an employment or volunteer-work relationship between the organization and the individual; or

(b) managing a post-employment or post-volunteer-work relationship between the organization and the individual.

Collection by trade union relating to obligation under a collective agreement
A bargaining organization may collect, use or disclose personal information about an employee if the collection or use or disclosure is necessary,

(a) for the purpose of a campaign to establish bargaining rights;

(b) to comply with an obligation under a collective agreement or to deal with a dispute arising under a collective agreement; or

(c) for the purpose of representing employees in respect of the terms and condition of employment.

Collection by bargaining organization relating to a labour dispute
A bargaining organization may collect, use or disclose personal information about an individual for the purpose of informing or persuading the public about a matter of significant public interest or importance relating to a labour relations dispute involving the bargaining organization.

Individual's interest
An organization may collect or use an individual's personal information if the collection or use is clearly in the interests of the individual, but only if it would be impracticable to obtain consent.

Emergency
An organization may use or disclose an individual's personal information when necessary to respond to an emergency that threatens the health, safety or security of an individual or the public. If the individual whom the information is about is alive, the organization shall inform that individual in writing without delay of the disclosure.

Identification of individual
An organization may disclose an individual's personal information if the disclosure is necessary to identify the individual who is injured, ill or deceased and is made to a government institution, a part of a government institution or the individual's next of kin or authorized representative. If the individual is alive, the organization must inform them in writing without delay of the disclosure.

Communication with next of kin or authorized representative
An organization may disclose an individual's personal information to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual.

Research in the public interest
An organization may use or disclose an individual's personal information for research purposes if all of the following conditions are satisfied:

1. The research purposes cannot be achieved without using or disclosing, as the case may be, the information.

2. The research purposes relate to a public interest.

3. The use or disclosure is not likely to cause harm to the individual.

4. The purpose of the research is not to make decisions about individuals.

5. The results of the research will be made publicly available, but not in a form that could reasonably enable an individual to be identified.

6. It is impracticable to obtain consent.

7. The organization informs the Commissioner of the use or disclosure before the information is disclosed.

8. Such other conditions as may be prescribed.

Records of historic or archival value
An organization may disclose an individual's personal information to an entity whose functions include the conservation of records of historic or archival value, if the disclosure is made for the purpose of such conservation.

Breach of security safeguards
An organization may disclose an individual's personal information without their knowledge or consent if,

(a) the disclosure is made to the other organization, government institution or part of a government institution that was notified of a breach; and

(b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.

Disclosure after period of time
An organization may disclose an individual's personal information after the earlier of,

(a) 100 years after the record containing the information was created; and

(b) 30 years after the death of the individual.

Publicly available information
An organization may collect and use an individual's personal information if the personal information is publicly available and the collection is consistent with the purposes and context in which the personal information was made publicly available and the reasonable expectations of the individual.

Two of the above grounds require further attention: employee-related personal data; and the collection, use and disclosure of personal information by a trade union.

Employers have legal obligations to collect, use and disclose personal information regarding employees, including for tax purposes. Therefore, requiring consent for the collection, use and disclosure of employee personal information when it relates to the establishment and management of an employer and employee relationship is not feasible. This would not mean that employers would have free rein. As is the case under existing Canadian privacy laws, Ontario could provide that the collection of employee personal information must be necessary for the employment relationship, and that employees must be notified when the collection takes place. Any collection of personal information beyond what is necessary to establish or manage the employer and employee relationship would therefore not be permitted by this lawful authority. For example, if an employer wanted to collect socio-economic information on employees for diversity and inclusion planning purposes, the employer would need to obtain consent from the affected employee.

Similarly, trade unions also have legal obligations with respect to union members that would be greatly hindered if consent were to be required from the individual worker to collect, use and disclose that personal information for legitimate purposes. As the Supreme Court of Canada has affirmed in relation to Alberta's private sector privacy law, trade unions use personal information to fulfil a unique representational role in the workplace and society. The alternative grounds outlined above could allow bargaining organizations, which would be defined to include trade unions and any employee association acting with respect to terms and conditions of employment, to collect, use

and disclose personal information to discharge their legitimate obligations. This definition would allow for organizations seeking to become a certified trade union to also be able to rely on this authority for the collection, use and disclosure of personal information. This authority would allow unions to conduct their lawful activities unimpeded, while providing greater protection for workers' personal information.

While Ontario recognizes consent as a central and meaningful authority, these potential alternate bases could help ensure that individual Ontarians would not need to bear the entire burden of keeping data practices in check and holding organizations to account. This aims to empower Ontarians by ensuring that consent, where necessary, is not simply a box to be checked, but a meaningful and informed authorization by individuals to exercise more control over their data. It is also worth noting that the "fair and appropriate" purpose criterion outlined in the first section of this paper would continue to apply to each permitted instance of collection, use and disclosure, regardless of which other authorities may also apply.

Discussion Questions:

- Does the sample list of "permitted categories" provide a sufficient set of authorities for the collection, use and disclosure of personal information? Are there any categories missing? Are there any categories that are too permissive?
- Consider the sample "business activities" provision provided above. Is it properly balanced to protect personal information while allowing businesses to conduct their operations? How should Ontario define the concept of "commercial risk"? Should "any other prescribed activity" be removed from the list of business activities?
- Are there any additional protections or requirements that Ontario should consider in respect of service providers?

Data transparency for Ontarians

Problem:

Most data practices are now opaque and far too complex for the average Ontarian to track. This obscurity can lead to citizens consenting to practices that create risks of which they are not aware. It can also create mistrust in organizations, and thus risk harming business innovation if individuals believe that their information is being exploited in obscure ways. As Ontario's Information and Privacy Commissioner noted in her response to Ontario's 2020 privacy reform consultation, "transparency is an essential component of any private sector privacy framework and should figure as one of its most important principles". For these reasons, modern privacy laws require meaningful transparency from organizations about their data practices.

Goal:

Stronger transparency requirements could provide citizens with a right to know when and how their data is used by organizations, allowing them to regain control and participate more meaningfully in the decisions that affect their well-being.

*

Transparency is a cornerstone of modern privacy law. Privacy rights cannot be meaningful unless individuals are provided with the knowledge needed to exercise them. The flows and uses of personal information have now become so intricate that it is impossible for most Ontarians to track the multitude of collections and transfers, or to understand how their data is used once it is in the custody of an organization. During the 2020 privacy reform consultation, Ontarians and businesses both indicated that plain-language rules and explanations are crucial to building a privacy-protective culture in this complex data landscape.

Other jurisdictions have made some advances in this area. The GDPR requires organizations to provide concise, intelligible and easily accessible information to individuals throughout the lifecycle of their data process**.** Quebec's Bill 64 enhances transparency requirements, and Bill C-11 provides that organizations must provide plain language policies and practices to individuals. This includes requirements to provide details about use of personal information, with which organizations it is shared, and how long it is retained. Bill C-11, however, permits organizations to collect and use personal information for a number of purposes without having to inform individuals about it.

Ontario is considering how to adapt and improve on the transparency rules found in other jurisdictions. Two proposals are under consideration.

The first proposal would be to require organizations to implement internal privacy policies, practices and procedures. They could be required, in other words, to implement a privacy management program to govern their collection, use and disclosure of personal information, and to make that program available for review. This would ensure that the organization's employees are aware of, and comply with, the program. Among other things, employees would be more responsive to information requests and inquiries from members of the public. These privacy management programs would be informed by resources and templates developed by the province and would also be made available upon request to Ontario's privacy regulator, the Information and Privacy Commissioner of Ontario (IPC).

Privacy management program

(1) Every organization shall implement a privacy management program that includes the organization's policies, practices and procedures put in place to fulfil its obligations under this Act, including policies, practices and procedures respecting,

(a) the protection of personal information;

(b) how requests for information and complaints are received and dealt with;

(c) the training and information provided to the organization's staff respecting its policies, practices and procedures; and

(d) the development of materials to explain the organization's policies, practices and procedures put in place to fulfil its obligations under this Act.

The requirement for organizations to implement a privacy management program will be scalable to the size of the organization. In developing a privacy management program, organizations would take into account the volume, nature and sensitivity of the personal information under their control. This would mean smaller organizations that do not collect highly sensitive personal information will not be required to develop complex privacy policies and procedures. Likewise, larger organizations that collect, use and disclose large amounts of personal information (including highly sensitive information) would need to have a robust privacy management program fit for the scale of data processing they undertake.

In addition to the above requirement, the transparency language proposed below would ensure external transparency through the requirement for organizations to make readily available information about their compliance-related policies, practices and procedures.

The second proposed enhancement for transparency (outlined below) relates to the giving of notices to individuals who are being asked to consent to the collection of their personal information.

Transparency in obtaining consent is significant because it is a key means for individuals to have some control over their own personal information. As indicated above, however, consent notices can overwhelm individuals rather than empower them. Excessively dense and complicated information can therefore erode the validity of consent. It can also undermine the efficacy of other data rights. Feedback from Ontario's 2020 privacy reform consultations emphasized this concern, i.e. that accessibility of, and plain-language requirements for, consent notices are important to ensure that information is meaningful and contributes to Ontarians' ability to make informed decisions.

For this reason, instead of inundating citizens with long and unclearly written privacy policies or notifications that are difficult to find, Ontario is considering a requirement for organizations to make information available, in plain language, that explains how the organization is using individuals' data, the lawful basis they are relying on, and how Ontarians can follow up to exercise their data rights.

There are two aspects to this proposal. The first is a requirement, noted above, for organizations to make information about their compliance-related policies, practices and procedures available. A component of this would relate directly to informed consent:

Policies, practices and procedures

(1) An organization shall make readily available, in plain language, information that explains the organization's policies, practices and procedures put in place to fulfil its obligations under this Act.

Additional information

(2) In fulfilling its obligation under subsection (1), an organization shall make the following information readily available:

1. A description of the type of personal information collected by the organization and the particular purpose for its collection.

2. A general account of how the organization uses or discloses personal information.

3. If the organization is not relying on an individual's consent for the use or disclosure, a description of the categories set out in sections xx to xx that the organization is relying on for the use or disclosure.

4. A general account of the organization's use of any automated decision system to make predictions, recommendations or decisions about individuals that could have significant impacts on them and a description of the individual's rights regarding the automated decision system.

5. How an individual may make a request for disposal or access.

6. The contact information of the individual to whom complaints or requests for information may be made.

A key feature of the above proposal is that organizations' transparency about their uses and disclosures of personal information would not be limited to situations where individuals are giving consent. Bill C-11 contains similar transparency requirements, but Ontario's proposal would enhance transparency by requiring more details about the collection, use and disclosure of information.

Related to establishing a privacy management program and policies for protecting personal information, Quebec's Bill 64 also includes a requirement for organizations to conduct an assessment of the privacy-related factors on any information system project or electronic service delivery involving personal information (i.e. a "privacy impact assessment"). Similarly, the federal OPC has called for the federal Bill C-11 to be amended to include requirements for organizations to follow "Privacy by Design" principles and conduct privacy impact assessments on high risk activities. Both Quebec and the OPC's approach aim to increase accountability for privacy protection in organizations. Ontario is interested in gathering input to assess the value of such requirements for enhancing transparency and accountability, and the impacts to organizations should similar requirements be introduced in the province.

The second aspect of the Ontario proposal, set out below, relates directly to what information must be provided by an organization to obtain valid consent, recognizing that, where consent is required, transparency plays an important role in ensuring its validity. The following provisions illustrate the approach that Ontario is considering, and specifies the kind of information that an organization would be required to provide when seeking valid consent from an individual:

Information for consent to be valid

(3) An individual's consent is valid only if the following conditions are satisfied:

1. It is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

2. At or before the time that the organization seeks the individual's consent, it provides the individual with the following information in plain language:

    i. That the individual has the right to give, refuse or withdraw consent in accordance with this Act

    ii. The purposes for the collection, use or disclosure of the personal information determined by the organization and recorded

    iii. The way in which the personal information is to be collected, used or disclosed, including whether the organization will be using an automated decision system with respect to the personal information.

    iv. Any reasonably foreseeable consequences of the collection, use or disclosure of the personal information.

    v. The specific type of personal information that is to be collected, used or disclosed.

    vi. The names of any third parties or types of third parties to which the organization may disclose the personal information.

The principle of transparency is fundamental to the creation of a more privacy-protective society. Ontario's Information and Privacy Commissioner made it clear in her submission that consent will only be informed where it is reasonable to expect that the individual understands the nature, purpose, and consequences of what is being asked. The approach Ontario is considering is intended to give Ontarians more control over the use of their data by empowering them with knowledge. This, in turn, would allow them to participate more meaningfully in the actions, practices and decisions that affect their everyday lives.

Discussion Questions:

- Is the "privacy management program" requirement sufficient to ensure that organizations are accountable for the personal information they collect?
- Are the sample provisions in this section sufficient to ensure that Ontarians understand the nature, purpose and consequences when an organization collects or uses their personal information?

- Should Ontario consider a mandatory requirement for “Privacy by Design” practices or “privacy impact assessments”? What kind of burden would this kind of requirement cause for organizations? How should Ontario balance the value of these requirements with this potential burden?

Protecting children and youth

Problem:

Children are among the most vulnerable groups in the digital economy. Their extensive online activity, combined with the increasing obscurity of data practices, makes them easy targets for unjustified surveillance, invasive monitoring and influence by bad actors.

Goal:

Ontario could provide special protections for children to guard against these heightened dangers by introducing a minimum age of valid consent and prohibiting organizations from monitoring children for the purpose of influencing their decisions or behaviour.

*

The risks associated with modern data practices are significantly higher for vulnerable populations. An individual may be considered vulnerable when circumstances restrict their ability to provide valid consent, to object to the collection, use or disclosure of their data, or when there is a significant power imbalance between that individual and the organization that controls their information.

Children and youth represent an example of this vulnerability, especially when they participate in virtual activities such as online learning or posting to social media. Without adequate protections, children can be easy targets for data-exploitative practices and behavioural influences that can be created by the use of modern information technologies, including AI.

In addition to protections outlined in the rights-based approach to privacy, there are a number of areas in which Ontario is considering additional protections for children and youth. Ontario is contemplating introducing an explicit requirement for parental consent on behalf of a “child” under the age of 16 years. This would signify the age of consent for the collection, use and disclosure of personal information. This requirement, which is similar to a GDPR requirement that relates to children’s online activity, would help to ensure that the consenting individual is able to fully understand and grasp the relevant details, as well as the risks and possible consequences.

Through the following proposal, Ontario could empower parental responsibility, a first essential step when protecting Ontario's children from potentially harmful online practices:

> **Children's personal information**
> (1.1) In the case of the collection, use or disclosure of a child's personal information, the consent must be given on behalf of the child by a person who has lawful custody of the child.
>
> **Verification of identity**
> (1.2) For the purposes of subsection (1.1), an organization shall take reasonable steps to verify the identity of the person purporting to have lawful custody of the child and to verify that the person does have lawful custody of the child.
>
> **Same**
> (1.3) An organization may request an individual purporting to have lawful custody of a child to provide the organization with sufficient information to allow the organization to fulfil its obligations under this section.

This parental (or guardian) authority for consent would also extend to the exercise of the other privacy rights on behalf of the child in their lawful custody. Similar to provisions in the *Freedom of Information and Protection of Privacy Act*, a parent or guardian could request access to the child's personal information. They could also request that it be corrected, be provided in a machine-readable format, be erased, or they could challenge the organization's privacy management practices by submitting a complaint to the organization or to Ontario's IPC.

Many children enjoy a high degree of freedom and discretion when interacting with online platforms. To recognize the capacity of mature minors, Ontario may consider providing youth between the ages of 13 and 16 with a right to object to their parent's (or guardian's) consent to provide their personal information on their behalf, or conversely, to object to their parent's (or guardian's) request to destroy or take down personal information about them.

Just as parental consent may contradict a minor's preference, it also may not always be sufficient to protect children from harmful data practices. To address this issue, Ontario is considering the possibility of explicitly prohibiting organizations from using artificial intelligence technologies to exploit children's data. The intent would be to establish a "no-go zone" to clarify that the legitimate needs of an organization cannot include the monitoring or profiling of an individual under the age of 16 for the purposes of influencing the individual's decisions or behaviour.

In addition to protections for children and youth, it is proposed that, in the case of individuals who are vulnerable for other reasons and cannot exercise their privacy rights, the following rules could apply:

> **Authorized persons**
> (1) Any right conferred on an individual by this Act may be exercised,
>
> (a) where the individual is deceased, by the individual's personal representative if exercise of the right or power relates to the administration of the individual's estate;
>
> (b) by the individual's attorney under a continuing power of attorney, the individual's attorney under a power of attorney for personal care, the individual's guardian of the person, or the individual's guardian of property; and
>
> (c) where the individual is a child, by a person who has lawful custody of the individual.
>
> **Legitimate needs**
> (4) For the purpose of paragraph 2 of subsection (2), the legitimate needs of an organization do not include;
>
> (a) the monitoring or profiling of an individual under the age of 16 for the purposes of influencing the individual's behaviour or decisions;
>
> (b) purposes that are known to cause, or are likely to cause, significant harm to the individual or groups of individuals;
>
> (c) any purpose that would contravene a law of Ontario or of Canada; or
>
> (d) any other prescribed purpose.

Taken together, these additional protections could be meaningful first steps to ensure that the privacy rights of children and other vulnerable individuals are protected, and that AI cannot be used for invasive marketing, behavioural conditioning or influencing, or in ways that will otherwise have adverse effects on young Ontarians. The protection of children is important for parents and families, and as an investment into a more privacy-protective future. If these protections are introduced, the Government of Ontario could undertake further work with Ontario's Information and Privacy Commissioner to develop supplementary codes of practice and conduct that resemble those introduced in some European jurisdictions.

Discussion Questions:

- What additional considerations are needed in determining appropriate age of consent for the collection, use and disclosure of personal information?
- What operational challenges might organizations face by including age of consent requirements for the collection, use and disclosure of personal information?
- Should Ontario consider other requirements to enhance protections for other vulnerable populations, such as seniors and people with disabilities?

A fair, proportionate and supportive regulatory regime

Problem:

A privacy law would be ineffective without regulatory oversight. An independent oversight body is needed to promote good privacy practices and also to enforce the law, when necessary.

Goal:

Ontario could extend the IPC of Ontario's mandate to include oversight of and compliance with these proposed requirements. This mandate could introduce stronger enforcement powers to hold organizations to account. Alongside these IPC oversight powers; privacy laws should provide for support and guidance to organizations.

*

As an officer of the Legislature, Ontario's IPC has over 30 years of experience in overseeing public body compliance with Ontario's public sector privacy rules. The IPC also has long-standing experience with overseeing compliance with health privacy rules, in both the public and private sectors, under *PHIPA.* The IPC would therefore be the best choice to provide oversight of a made-in-Ontario private sector privacy law.

Bill C-11 introduces a more robust oversight role for the Privacy Commissioner of Canada, and an expanded suite of powers to enforce compliance, including audit, investigative, and order-making powers. However, it also includes more supportive forms of compliance, authorizing the Commissioner to approve certification programs and codes of practice that will provide clear guidelines for organizations, thus reducing risk of contraventions. Bill C-11 also proposes to establish an administrative tribunal to hear appeals in response to Commissioner decisions, and levy monetary penalties.

With the exception of the tribunal proposed in Bill C-11, Ontario is considering adoption of a similar enforcement framework, with emphasis on guidance and support for organizations. Whenever possible, tools and resources should be made available to

assist organizations with understanding their obligations under a privacy law. Provisions could be made to include responsibilities for both the IPC and the Ministry of Government and Consumer Services in developing guidance materials for organizations of all sizes to understand the steps they need to take to become compliant with the law. Guidance and tools can help reduce burden on organizations as they integrate privacy requirements into their policies and procedures. This is a role the IPC has already been fulfilling for many years under Ontario's existing privacy laws.

IPC certification of "codes of practice" is another proactive and supportive tool that could promote compliance. A code of practice is a detailed set of principles and requirements that an organization, or group of organizations (such as a specific sector or industry), develops to meet the requirements under the law. Certification programs, subject to IPC approval, could also build confidence by assuring individuals that the organization's practices both comply with a given code of practice, and proactively manage and protect privacy.

To be an effective oversight body, the IPC also should have the authority and resources to deploy various tools to enforce the law and require organizations to be compliant. In this regard, the IPC should have the authority to initiate and conduct investigations and audits and compel organizations to provide relevant information on how to manage personal information. The IPC also should have the discretion to determine when to investigate a complaint.

Following an investigation, the IPC could have the ability to issue binding orders to organizations that are found to be in non-compliance with the law. Order-making power could include the ability to order an organization to take measures to comply with the law, stop doing something that is in contravention of the law, make public any measures it has taken to fulfil its obligations under the law, and destroy any personal information collected unlawfully.

To strengthen the compliance framework, administrative monetary penalties could serve as a deterrent for organizations that violate any privacy requirements. In the Ontario context, monetary penalties could be administered by the IPC rather than by the independent tribunal proposed at the federal level. The IPC's penalty decisions would be subject to judicial oversight, as is now the case with their other adjudicative decisions pursuant to Ontario's public sector laws.

To ensure effectiveness, the amount of the penalty could take into account the extent of harm, how the organization tried to prevent or mitigate the harm, the number of persons that may have been impacted, and more. Further, the penalty amount could take into account the size of the organization and its annual global revenue. This approach aligns

with Quebec's Bill 64 which proposes different penalties for individuals and organizations and takes into account the size of the organization.

Order

(1) If, in completing an inquiry, the Commissioner finds that an organization has contravened this Act, the Commissioner may by order, impose an administrative penalty on the organization.

Purpose of administrative penalty

(2) The following are the purposes for which a person may be required to pay an administrative penalty under this section:

1. To encourage compliance with this Act and its regulations.

2. Preventing a person from deriving, directly or indirectly, any economic benefit as a result of a contravention of this Act or its regulations.

Factors

(3) In making a determination under this section respecting the amount of an administrative penalty for a contravention, the Commissioner may consider the following criteria and any other criteria that the Commissioner considers relevant:

1. The extent of the harm or potential harm resulting from the contravention.

2. The number of individuals and other persons affected by the contravention.

3. The extent to which the contravention deviates from the requirements of this Act or the regulations.

4. The extent to which the organization could have taken steps to prevent the contravention.

5. The extent to which the organization tried to mitigate any harm or potential harm or to take other remedial action.

6. Whether the organization notified the Commissioner and any individuals whose personal information was affected by the contravention.

7. The extent to which the organization derived or reasonably might have expected to derive, directly or indirectly, any economic benefit from the contravention.

8. Whether the organization has previously contravened this Act or the regulations.

9. Whether the organization has voluntarily paid compensation to a person or any other individual affected by the contravention.

Content of order of administrative penalty

(4) An order requiring an organization to pay an administrative penalty shall,

(a) contain or be accompanied by a description of the contravention; and

(b) set out the amount of the penalty to be paid and specify the time and manner of the payment.

Enforcement measures

(5) The use of an enforcement measure provided for in this Act in respect of a contravention of this Act or its regulations does not prohibit the use, at the same time or different times, of any other enforcement measure or remedy provided for in this Act or otherwise available in law in respect of the same contravention.

Maximum administrative penalty

(6) An administrative penalty shall not exceed,

(a) in the case of an organization that is an individual $50,000; or,

(b) in the case of an organization that is not an individual, the greater of,

(i) $10,000,000; and

(ii) 3 per cent of the organization's gross global revenue in its financial year before the one in which the penalty is imposed.

In considering the maximum amount of administrative monetary penalties, the proposed approach is to have a lower maximum amount of $50,000 apply to individuals (as reflected in part (a) above). The higher maximum penalty of $10 million or 3% of an organization's gross global revenue would be reserved for organizations (as reflected in part (b) above).

Two-year limitation

(7) An order requiring a person to pay an administrative penalty shall not be issued under this section more than two years after the day the most recent contravention on which the order is based first came to the knowledge of the Commissioner.

To ensure procedural fairness, Ontario is considering that orders made by the IPC, including administrative monetary penalties could be appealed to the Divisional Court on a question of law within 30 days.

Right of appeal re compliance orders

(1) A complainant or organization that is affected by a Compliance order may appeal it to the Divisional Court on a question of law in accordance with the rules of court by filing a notice of appeal within 30 days after the complainant or organization receives the order.

Confidentiality of information

(2) In an appeal under this section, the court may take precautions to avoid the disclosure by the court or any person of any personal information about an individual, including, where appropriate, receiving representations without notice, conducting hearings in private or sealing the court files.

Court order

(3) On hearing an appeal under this section, the court may, by order,

(a) direct the Commissioner to make the decisions and to do the acts that the Commissioner is authorized to do under this Act and that the court considers proper; and

(b) if necessary, vary or set aside the Commissioner's order.

Finally, Ontario's proposed approach could include statutory offences that hold organizations liable for violating specified significant provisions of the law, including where an organization fails to: report a breach of security safeguards to the IPC; maintain a record of every breach of security safeguards; retain information subject to an IPC inquiry; abide by an IPC compliance order; or re-identify personal information that has been de-identified or seeks retribution against a whistle-blower.

Offence

(1) An organization is guilty of an offence if the organization,

(a) knowingly contravenes [Report to Commissioner], [Records], [Prohibition against re-identification of personal information] or [Retention of information], [Compliance order] or [Whistleblowing]; or

(b) obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint, in conducting an inquiry or in carrying out an audit.

> **Penalty**
> (2) An organization who is guilty of an offence under subsection (1) is liable, on conviction, to a fine of not more than the higher of $25,000,000 or 5 per cent of the organization's gross global revenue in its financial year before the one in which the organization is sentenced.

Another option to help individuals receive quicker access to resolutions is to include provisions that would allow the IPC to issue orders to organizations compelling them to take measures to allow individuals to be compensated in the event of a privacy breach. As raised in the OPC's submission on Bill C-11, this may be a helpful tool to require organizations to offer assistance or compensate individuals for losses, financial or otherwise, in the event of a failure of security safeguards involving personal information. Ontario welcomes feedback on this topic.

The proposed enforcement framework could support and assist organizations that are trying to be compliant, while also addressing egregious non-compliance and thus deterring bad actors. Strong oversight and enforcement would further build public trust in digital platforms and technologies, as Ontarians could be safe in the knowledge that bad actors would be subject to investigation and consequences for violating the law.

Discussion Questions:

- Would certification programs and codes of practices be effective in proactively and collaboratively encouraging best practices in privacy protection?
- Are administrative monetary penalties effective in encouraging compliance with privacy laws? Are the financial penalties set at an appropriate level?
- Would the ability for the IPC to issue orders requiring organizations to offer assistance or compensate individuals be an effective tool to give individuals quicker resolutions to issues?

Supporting Ontario innovators

Problem:

Organizations may wish to use de-identified personal information for research and innovation purposes. They may wish to improve their existing technologies, services or products or develop new ones. Such uses of de-identified information can enhance digital economic activity while protecting Ontarians' privacy. To do this safely, however, organizations must be confident that, in using de-identified data, they are not contravening the privacy rules.

Goal:

Ontario could take this opportunity to provide clear definitions, requirements and standards to guide organizations in the use of de-identified data, encouraging safe and responsible research and innovation without compromising the privacy of Ontarians.

*

With the growth of big data and data analytic techniques, organizations and researchers can derive new insights from data to find innovative solutions to issues or problems. However, with the acceleration of data analytics and AI, there is a need to protect individuals from potential privacy harms resulting from using large data sets of personal information.

As previously outlined, Ontario is considering rules regarding the use of automated decision systems that have a significant impact on individuals (see Safe use of automated decision-making). These proposed restrictions are in alignment with work Ontario has been leading to build a framework for trustworthy AI. Please see the consultation page for Ontario's Trustworthy AI Framework for more information. In addition, Ontario is considering a framework that would encourage and, in some cases, require organizations to use de-identified information, whenever possible, to reduce the risks of harm to the individual, while also providing clarity on the obligations that organizations would have with respect to de-identified information.

> "de-identified information" means information about an individual that no longer allows the individual to be directly or indirectly identified without the use of additional information.

There is often confusion around where de-identified information fits within privacy laws, as privacy laws typically only govern "personal information," and are silent on the topic of de-identified information. In today's age, de-identified information has been transformed in such a manner that it is no longer identifiable, which would seem to indicate it is no longer subject to privacy rules; however, it is derived from personal

information and some risks of harm to individuals may still exist, particularly the potential for re-identification.

For this reason, Ontario is considering an approach that would extend certain requirements to de-identified information. This could include requirements related to the implementation of a privacy management program, ensuring that there are security safeguards in place to protect the de-identified information, and providing an opportunity to make a complaint or request information with respect to compliance.

The intent of this proposed approach is to ensure that organizations are transparent and accountable for their use of de-identified information. It would also recognize that certain features of a privacy framework are neither desirable nor practicable when dealing with de-identified personal information. For example, if information has been de-identified, organizations would not be required to respond to an individual's request to access, append, port, or delete personal information.

Ontario is considering a framework for de-identification premised on a risk-based approach, which would require organizations to employ de-identification protocols that are proportional to the sensitivity of the personal information. Ontario is also considering prohibiting the re-identification of personal information, except in accordance with stipulated technical and administrative measures, including privacy protections.

> **Proportionality of technical and administrative measures**
> An organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information.
>
> **Prohibition**
> Except as required by law and subject to such exceptions and additional requirements as may be prescribed, no person or organization shall use or attempt to use de-identified information to identify an individual, either alone or with other information, for any purpose other than to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information except in accordance with stipulated technical and administrative protocols including the protection of an individual's privacy.

These recommendations reflect those put forward by the Information and Privacy Commissioner of Ontario in her submission to the government's 2020 privacy reform consultation. The IPC is a leading voice with respect to de-identification, having issued its well-respected De-Identification Guidelines for Structured Data in 2016.

Finally, the concept of “anonymized data” – personal information that has been altered in such a way that it is no longer identifiable in relation to an individual – is also being considered. This concept would further expand the risk-based approaches to data use and incentivize the use of anonymized data by removing it from privacy rules altogether.

> **Anonymized information**
> (3) For clarity, this Act does not apply to information has been altered irreversibly, according to generally accepted best practices, in such a way that no individual could be identified from the information, whether directly or indirectly by any means or by any person.

The proposed approach to de-identified information could promote innovation through data analysis in a privacy-protective manner. Organizations would be incentivized to manage privacy risks by employing de-identification and anonymization techniques when conducting privacy analysis. These techniques could help reduce the residual risks of harm to individuals without preventing organizations from realizing the value of data.

The responsible use of de-identified information has great potential to benefit the public good. Thereby, these proposed requirements could help to lay the foundation for Ontario to explore models of data stewardship and governance, and systems of safe information-sharing that could advance the collection, use and disclosure of data for socially beneficial purposes. The government is considering these options carefully and will welcome feedback from Ontarians to inform this important next phase of policy work as the province continues to implement its Digital and Data Strategy and explore data authorities for providing safe, shared access to information. Although the digital world poses risks, a more privacy-protective regime can help unlock new benefits and innovations for the future of the province.

Discussion Questions:

- Would the clearer articulation of which privacy rules apply to de-identified information, as discussed in this section, encourage organizations to use de-identified information, and therefore reduce privacy risk?
- Would the inclusion of the concept of anonymized information, and clarifying that the privacy law would not apply to this information, encourage organizations to use anonymized information?
- For sharing information for socially beneficial purposes, what additional safeguards or governance would be needed in addition to de-identification of information, in order to protect privacy?

Conclusion

Public trust and confidence in the digital economy are key to the future prosperity of Ontario and the well-being of Ontarians. Ontario's proposed approach would lay the groundwork for this by implementing a rights-based approach to privacy to empower Ontarians and give Ontario's organizations a competitive advantage in a data-driven world.

While many organizations in Ontario are already observing a high standard of privacy in their activities, others may face some challenges when adapting their practices and services to new requirements. Regulatory change can be challenging, and data protection requires time to improve. Ontario recognizes that the proposed approach outlined in this paper would require a transitional period and is considering a minimum of two years, if any legislation is introduced, for the law to come into effect.

The proposed approach would require sequenced implementation, the provision of resources – including in the form of user-friendly guidance materials, certification programs and codes of practice to familiarize organizations with any new obligations – and the establishment of consistent, interoperable standards. The province would also continue to engage stakeholders from different sectors to seek feedback about guidance and implementation to ensure that their sectors are appropriately supported in the transition.

As a leader in data protection, Ontario could also become one of the leading digital jurisdictions in the world – and establish a foundation of privacy that will empower Ontarians, protect their personal information, and promote responsible innovation and data uses for the public good.

HOW TO PARTICIPATE

Formal response

We welcome your feedback on the details and draft provisions outlined in this paper. If you are an organization, legal or technical expert, or a member of the public and wish to submit a formal response to this paper, you may submit to the following address: access.privacy@ontario.ca.

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
Telephone: 416-327-1600 or 1-800-668-9933 (Toll-Free Number - Ontario only)