

October 1, 2019

**Comments of ITAC and ITI on
ISED's Proposals for Modernizing PIPEDA**

The Information Technology Association of Canada (ITAC) and the Information Technology Industry Council (ITI) welcome the opportunity to provide comments on ISED's proposals to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA). These proposals are set out in ISED's discussion paper entitled "*Strengthening Privacy for the Digital Age*".¹

ITAC is the authoritative national voice for Canada's \$170 billion information and communications technology (ICT) industry. Canada's 36,000 ICT firms generate over 1.1 million jobs directly and indirectly. The ICT industry in Canada also creates and supplies goods and services that contribute to a more productive, competitive and innovative economy and society. ITI is the premier advocacy and policy organization for the world's leading innovation companies.

General Comments

The importance of a balanced approach

It is now well-understood that data is an important driver of innovation in the global economy and that Canada's continued prosperity depends on business' ability to access data, including data about individuals, to develop and deliver new products and market solutions. When done responsibly, the analysis and use of personal information can be highly beneficial to individuals, businesses, governments and society at large.

Responsible use of personal information must be built on a strong foundation of trust and transparency. Individuals need to be informed what data about them is being collected and how it is being used and disclosed. Ultimately, a balanced approach is needed; one that recognizes the right of privacy of individuals and the need for organizations to collect, use or disclose personal information.

We are encouraged that the importance of balance is prominently reflected in ISED's discussion paper. The paper states that the government is considering "*how best to modernize its private-sector policy and regulatory framework in order to protect privacy and support innovation and prosperity.*" ITAC agrees with this approach and offers its comments set out below in furtherance of this goal.

¹ https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

A proposed framework for modernizing PIPEDA

ITAC and ITI are supportive of ISED's efforts to modernize PIPEDA. Enhancements can be made to PIPEDA's regulatory framework that both improve individual privacy rights and enable a strong and vibrant digital economy for Canada.

Before considering possible enhancements, it is important to acknowledge that PIPEDA has proven to be effective and resilient since it was enacted more than 20 years ago. PIPEDA is both protective of privacy and supportive of economic growth and responsible innovation. It can be applied to countless new and unforeseen commercial activities in a rapidly changing data environment, without the need for frequent legislative amendments.

PIPEDA's effectiveness stems from six key foundational features:

1. PIPEDA is principles-based, allowing organizations to implement privacy protections in a flexible and context-specific manner, taking into account actual risks;
2. PIPEDA is technology and business sector neutral, making it largely future-proof;
3. PIPEDA explicitly recognizes the need to balance the interests of individuals and organizations;
4. PIPEDA adopts organizational accountability as a core principle;
5. PIPEDA promotes transparency, including requiring disclosure to individuals about personal information management policies, practices and controls; and
6. PIPEDA empowers individuals through meaningful control of their data and privacy preferences, including through the right to access and correct their information and the right to challenge inappropriate processing.

ITAC and ITI recommend that these features be reaffirmed and reflected in any amendments to PIPEDA. PIPEDA should be modernized through making refinements to its current privacy framework, rather than by adopting a wholesale new approach.

ITAC and ITI also recommend that proposals to modernize PIPEDA be evaluated against a goal of ensuring that PIPEDA is interoperable with privacy frameworks deployed in other leading jurisdictions, including the European Union. Interoperability does not require that the same exact obligations be adopted (for example, by copying legislative requirements). Rather, it can be achieved through a regulatory framework with compatible outcomes without requiring that different operational processes or technological systems be adopted than those that meet the global standard.

Part 1: Enhancing individual's control

A. Consent

ISED's review of PIPEDA presents a timely opportunity to rethink PIPEDA's emphasis on consent as the basis for processing personal information. Currently, PIPEDA requires an organization to obtain, subject

to exceptions, individuals' valid consent before collecting, using or disclosing their personal information. The underlying objective of this consent-model is to put individuals in control of their data. While we fully appreciate the importance of this objective, it is clear that a consent-model has become ineffective in the modern digital economy.

- Human behaviour: It is unrealistic to expect the average person to invest the time required to fully understand the details of every privacy policy they may come across on a daily basis. It is equally challenging for industry to comprehensibly communicate the details of every potential use of personal information to individuals.
- Unanticipated uses: PIPEDA calls for purposes of personal information collection, use and disclosure to be outlined at the time consent is given. However, increasingly, data analytics makes it likely that organizations will have the ability to use information for new purposes that benefit individuals, businesses and society in unanticipated ways from when consent was originally obtained. In these instances, it can be very challenging, if not often impossible, to obtain consent.
- Technological complexity: As online activities and connected technologies become more complex and ubiquitous, it is becoming more difficult for individuals to track which organizations are processing their data and for what purpose given increases in online activity.
- Common business practices and legitimate use cannot be subject to revocable consents if organizations are to operate efficiently and innovate with data responsibly: Many commonly accepted business practices (e.g. using personal information to get to know your own customers or creating new products or services) that utilize personal information but do not in any way harm individuals have emerged over time. These practices are often described in privacy policies, but are not generally subject to a separate, distinct, revocable consent. It is time for PIPEDA to recognize this reality.

In the circumstances, ITAC and ITI recommend that consent be recognized as one of multiple legal bases for processing personal information. Following the approach under the General Data Protection Regulation (GDPR), additional bases for processing should include processing in respect of the performance of a contract, compliance with a legal obligation, vital interest of the data subject, public interest and legitimate interest.²

Additionally, we are supportive of adding the new exceptions to consent described in ISED's discussion paper. These exceptions would allow for the use and disclosure of de-identified information, with penalties for re-identification, and processing for "*standard business practices*" that are reasonably expected and can be legitimized based on documented balancing of interests and impacts. Notwithstanding this support, we recommend that ISED explore alternatives to adding new exceptions to consent.

² GDPR, Article 6

ISED could exclude de-identified data from the definition of personal information and include standard business practices within the new authority for processing described in the preceding paragraph. This could be coupled with appropriate contractual and legal safeguards that ensure an enforceable obligation not to re-identify the information.

Adding these new grounds for processing and exceptions to consent will not diminish privacy protections. Legislative drafting and related guidance can put in place guardrails to ensure that related risks or harms are addressed. For example, processing on the basis of there being a legitimate interest could be made conditional, in certain cases not already blessed by ISED or the OPC, upon an organization conducting a documented risk assessment to ensure that the benefits of processing are not outweighed by potential impacts to an individual's rights and that tailored risk mitigations and controls are in place.

De-emphasizing consent in these ways would achieve many key objectives of modernizing PIPEDA. Specifically, it would:

- Facilitate more meaningful control by individuals through consent requirements that overcome consent fatigue, focusing an individual's attention on the collection, use or disclosure of personal information that is not reasonably expected;
- Bring PIPEDA into closer alignment with other leading global privacy frameworks (including the EU);
- Enable responsible innovation;
- Promote international competitiveness;
- Provide predictability for businesses; and
- Reduce regulatory burdens and compliance costs on businesses.

These outcomes can be achieved while also enhancing privacy protections, primarily through an increased emphasis on transparency and organizational accountability, which will help to reduce the level of responsibility that individuals currently bear to inform themselves of an organization's privacy management practices.

B. Transparency

ISED is seeking comments on specific proposals to enhance transparency. ISED proposes *"requiring organizations to provide individuals with the information they need to make informed decisions, including requiring specific, standardized, plain-language information on the intended use of the information, the third parties with which information will be shared, and prohibiting the bundling of consent into a contract."* As well, ISED is asking whether sensitive personal information should be defined, with specific protections added to PIPEDA.

ITAC and ITI agree that the disclosure of understandable and actionable information is foundational to effective privacy protections. It is critical to keep in mind, however, that legislating how transparency is achieved will undermine one of PIPEDA's core foundational features – that is, a principles-based approach that allows organizations to implement privacy protections in a flexible and context-specific manner, taking into account actual risks.

Prescriptive and inflexible disclosure requirements create material problems – both for businesses and individuals. As we have witnessed following the coming into force of CASL³, prescriptive rules create significant compliance costs, undermine interoperability with laws in other jurisdictions, impair innovation and contribute to consumer fatigue.

A better approach is for PIPEDA to require that meaningful notice be provided to individuals, but allow businesses to determine how best to communicate with individuals in the context of the products and services being offered. It can then fall to the businesses to demonstrate compliance, and in particular that the notice process they have implemented is sufficiently understandable from the general perspective of their target audience.

A contextual, risk-based assessment is also appropriate in the case of sensitive information. We do not recommend that PIPEDA define sensitive information or identify specific protections to be applied to sensitive information. Organizations should be required – as they are today – to undertake an assessment of the specific personal information they process and adopt privacy processes and safeguards that correspond to the sensitivity of the information in the specific context.

C. Data mobility

ISED is seeking comments with respect to its proposal to provide *“an explicit right for individuals to direct that their personal information be moved from one organization to another in a standardized digital format, where such a format exists.”*

While we recognize that data mobility is an important element of enhancing consumer control, adding such a right to PIPEDA needs to be accomplished in a manner that is consistent with PIPEDA’s foundational features. To accomplish this, we recommend that any provisions addressing data mobility should:

- Be narrowly defined so that they apply to the same or similar product or service and only where technically feasible;
- Require that data be provided to or made accessible to an individual, rather than require an organization to directly move the data to another organization (at least until international standards are developed that settle technical, authentication, security and operational issues created by transferring data from one service to another);
- Apply only to data that is held electronically;
- Apply only to information that is provided by the individual and transactional data (i.e., exclude derived information);

³ An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, SC 2010, c 23

- Exclude 3rd party information at least where it would adversely affect the rights of 3rd parties;
- Exclude de-identified data;
- Exclude call-notes and complaints;
- Provide a safe harbour for disclosing parties (so that they do not face liability for a recipient's or other service provider's acts or omissions);
- Avoid prescriptive rules and rules that are not technology and business sector neutral; and
- Take into account the barriers to entry that data mobility rules could create for start-ups and other small companies.

D. Online reputation

ISED's discussion paper identifies a number of possible options to enhance the ability of individuals to remove their personal information at the source (i.e., websites and online platforms). Specifically, the paper seeks input on:

- Requiring organizations to inform minors about their right to delete or de-identify their personal information that they provided and how to do so, with minimal exceptions;
- Providing all individuals with the explicit right to request deletion of information about them that they provided, with some caveats;
- Ensuring the accuracy and integrity of information about an individual throughout the chain of custody by requiring organizations to communicate changes or deletion of information to any other organization to whom it has been disclosed; and
- Defining retention periods to increase data integrity and decrease the risk of misuse.

While we recognize that enhancing the ability of individuals to protect their online reputation is an important objective, particularly for youth, we once again recommend that any attempt to enhance existing rights (including rights of access, accuracy and consent) be consistent with PIPEDA's foundational features. Our observations can be summarized as follows:

- Implementing the options identified in the discussion paper would introduce prescriptive rules that would create significant compliance challenges for businesses and lack interoperability with other jurisdictions;
- A blanket right to deletion would need many exemptions, contributing to complexity and inflexibility;

- It would be better to focus on information that is online and accessible to others where continued availability negatively impacts the individual in a meaningful and inappropriate way; and
- Where an organization has a legitimate reason to keep the data, withdrawal from public view (rather than deletion) is sufficient.

Part 2: Enabling responsible innovation

A. Possible option: Enabling data trusts for enhanced data sharing

ISED's discussion paper explores the creation of data trusts through which de-identified information could be processed without consent to help enable responsible innovation.

ITAC and ITI view data trusts as a potential innovation-enhancing tool that warrants exploration. Importantly, data trusts provide a framework built on accountability and oversight that enables access to data that otherwise would be siloed. If implemented appropriately, such a framework can help to maximize data usage for innovation, while concurrently enhancing public trust.

While we are supportive of data trusts at the conceptual level, it is clear that there remain significant obstacles that will need to be overcome – including governance, costs and legal liability – if they are to have a material beneficial impact on innovation.

It is our view that data trusts should be seen as only one of many tools that a modernized PIPEDA would include to enable responsible innovation. Permitting the use of de-identified data as described in our submission above, including the pooling of data from multiple sources without establishing a formal trust, is also critical.

B. Self-regulation and technical standards

ISED's discussion paper indicates that *“there is a need to recognize the value and utility of standards, codes and certification as tools to underpin privacy “rules” and try to influence and encourage their development in areas that reflect Canadian requirements, priorities and interests.”* The paper proposes to incentivize the use of standards and codes through formal recognition in PIPEDA as a means of demonstrating due diligence and by providing the Minister of Innovation, Science and Economic Development with broad regulation-making authority related to accreditation/certification schemes. As well, the paper points out that validation of codes or certification mechanisms could be achieved through recognition by the Office of the Privacy Commissioner (OPC) and serve as a mitigating factor in the event of investigations or enforcement action.

ITAC and ITI's perspective is that industry codes of conduct and privacy certifications have an important role to play to strengthen and enforce PIPEDA's accountability principle. They can serve as effective mechanisms to help demonstrate compliance and should be recognized as such within PIPEDA. In keeping with PIPEDA's key foundational features, we recommend that formal recognition of codes and certifications in PIPEDA:

- Be designed so that they are flexible and capable of being calibrated to an organization’s specific information uses and circumstances;
- Ensure that adherence to codes and related certifications are voluntary (rather than a pre-requisite for demonstrating compliance);
- Contemplate certification and complaint-handling by officially recognized and approved third-party certification bodies, with such bodies being subject to oversight by the Standards Council of Canada (making it unnecessary for the OPC to be given new authority in PIPEDA to pro-actively evaluate an organization’s compliance with a code or standard outside of a formal investigation or audit);
- Be drafted to ensure international interoperability; and
- Be incentivized in PIPEDA. Participation in certification schemes should be required to be taken into consideration when deciding on an appropriate remedy following a non-compliance event.

Part 3: Enhancing enforcement and oversight

ISED’s discussion paper includes a range of proposals to enhance enforcement and oversight, including:

- Providing the OPC with increased discretion on whether to investigate;
- Providing the OPC with increased flexibility for auditing organizations;
- Providing the OPC with limited order-making authority (i.e., cessation orders where “*non-compliance has caused or is likely to cause a risk of harm or significant distress to an individual*” [emphasis added] and records preservation orders);
- Expanding the existing fine regime and significantly increasing the range of fines, with the OPC referring matters of concern to the Attorney General for investigation; and
- Statutory damages, with minimum and maximum damages.

As a preliminary matter, ITAC believes the role of the Privacy Commissioner of Canada (and the Office of the Privacy Commissioner) needs to be more explicitly identified in PIPEDA. It should be clear that the Commissioner has a dual responsibility – consistent with the purposes of PIPEDA – for promoting adherence to PIPEDA and enabling beneficial uses of data. Additionally, any enforcement powers within PIPEDA must be respectful of administrative laws and the principles of natural justice. This means that the OPC (or any other regulator) must not be an advocate for a complainant while also serving as the judge and jury. As well, there needs to be an adequate appeal process and proportionality between the violation, the size and capabilities of the organization that committed the violation, and any penalty.

In respect of ISED's specific proposals, ITAC agrees that the Commissioner needs increased discretion as to whether to investigate a complaint or discontinue an investigation (so that it can devote its resources to more important complaints). In exercising this discretion, the Commissioner should have latitude to consider all of the circumstances of the complaint.

Our industry does not agree that the Commissioner requires additional authority to commence audits. The Commissioner currently has broad audit rights – it needs only to have reasonable grounds to believe that the organization has contravened PIPEDA. As well, given the breadth of the Commissioner's powers when undertaking an audit, including compelling the giving of evidence and entering any business premise, providing more expansive audit rights may be contrary to the Charter of Rights and Freedoms or other fundamental principles of Canadian law.

Our industry is not in favour of the Commissioner having order-making power. Officers of Parliament generally do not have the power to make orders in respect of private sector organizations. Additionally, due to the Commissioner increasingly positioning the OPC as a champion for privacy rights, it has become reasonable to ask whether the Commissioner lacks the perception of bias that is critical to any enforcement model.

Should cessation orders be added to PIPEDA, they should be issued by the court and should be restricted to egregious cases when material harm exists or is imminent. The standard for issuance of a cessation order proposed in the discussion paper (*"likely to cause a risk of harm"*) is too low.

Finally, ITAC and ITI do not support adding statutory damages to PIPEDA. Adding them would create conditions that promote opportunistic class actions and undermine efforts to enable responsible use of data and innovation. An enforcement model that promotes compliance through education, with offences being used to address egregious behaviour, is better aligned with the dual purposes of PIPEDA identified by ISED in its discussion paper.

Part 4: Areas of ongoing assessment

ITAC and ITI do not object to ISED's proposal to simplify the structure and drafting of PIPEDA by incorporating the principles in Schedule 1 within Part 1, although the rationale for doing so is not evident. However, if it is redrafted, care must be taken to ensure that PIPEDA remains fully aligned to the six key foundational features described above. From a drafting standpoint, the most critical elements of these features are principles-based, technology neutral and business sector neutral.

Regardless of whether PIPEDA is redrafted, amendments to PIPEDA should clarify how PIPEDA applies to transfers of data to service providers and, more broadly, transborder data flows. ITAC is strongly of the view that PIPEDA does not (and should not) require consent to transfer data for processing by service providers – inside or outside Canada. In response to its recent public consultation, ITAC urged the Commissioner against reading into PIPEDA a consent requirement for these transfers for the following reasons: (i) the OPC's 2009 guidelines on transborder data flows set out an effective approach, (ii) adding a consent requirement does not enhance privacy protections and will increase consent fatigue, (iii) unwarranted, material costs for businesses, (iv) lack of interoperability with global standards, (v) non-compliance with Canada's international trade obligations, and (vi) material negative repercussions

for the economy. Accountability principles provide the best approach to regulating domestic or trans-border transfers of data.

Again regardless of whether PIPEDA is redrafted, amendments to PIPEDA should strengthen the accountability principle within PIPEDA. Organizational accountability should be embraced as key building block for ensuring corporate digital responsibility. This could include adding an accountability framework that includes:

- Comprehensive privacy management programs;
- Documented risk assessments that are made available to the OPC upon request;
- Verification of effectiveness; and
- Demonstration of effectiveness (both internal and external).

We greatly appreciate the opportunity to provide ITAC's views to ISED and would welcome the opportunity discuss our comments with you.