



INFORMATION TECHNOLOGY  
ASSOCIATION OF CANADA

5090 Explorer Drive  
Suite 801  
Mississauga, Ontario L4W 4T9  
Tel: 905-602-8345  
Fax: 905-602-8346  
www.itac.ca



ASSOCIATION CANADIENNE  
DE LA TECHNOLOGIE DE L'INFORMATION

5090, Explorer Drive  
Bureau 801  
Mississauga (Ontario) L4W 4T9  
Tél. : 905-602-8345  
Fax : 905-602-8346  
www.itac.ca

Edmonton • Toronto • Ottawa • Montréal

August 5, 2016

## **ITAC RESPONSE: Modernizing Consent and Privacy in PIPEDA**

The Information Technology Association of Canada (ITAC) appreciates the opportunity to participate in the Office of the Privacy Commissioner's (OPC) ongoing dialogue on potential opportunities to modernize Canada's privacy framework. 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.

As the OPC consultation paper notes, data has become an increasingly important commodity and driver of innovation in the global economy. Canada's continued prosperity depends on business' ability to leverage all kinds of data, including data about individuals, to develop new products and market solutions. Canadians recognize the benefits of innovation, research, increased convenience, customization, consistency of services, as well as broader economic and social benefits that come with data sharing. Done responsibly, the analysis and use of personal information by business can be highly beneficial to individuals, businesses, governments and society at large.

In this spirit, ITAC welcomes the opportunity to engage in the OPC's consultation on modernizing consent under the *Personal Information Privacy and Electronic Documents Act* (PIPEDA) and related efforts that will better align Canada's privacy framework with how data is and will be used to deliver social and economic benefits for Canadians. ITAC hopes that the OPC's consultation will deliver recommendations to enhance Canada's privacy regime in a way that enables responsible uses of data to solve problems and generate value and benefits for organizations, individuals and society.

As data, including personal information, becomes core to most business activities, PIPEDA's importance as legislation that directly impacts the economy continues to increase. We encourage the OPC to factor into its deliberations the high economic stakes involved as it considers recommending legislative changes to Canada's overall privacy framework. In its current form, PIPEDA is flexible and can accommodate changes in technology and society. However, technology neutral and principles-based law (such as PIPEDA) can only be effective if the interpretation of the law also remains flexible and reflects practical realities.

The OPC consultation paper stresses that the consent model is challenged by emerging technologies and business models. ITAC agrees with this view. However, PIPEDA is not only a

consent-based law. It is a law that offers great flexibility and comes with a range of safeguards that provide a framework for managing many of the challenges associated with data analytics. The need for technological neutrality and an appreciation for technological advancement was considered and understood at PIPEDA's inception. So long as PIPEDA is not interpreted in an overly restrictive manner, it will remain an appropriate principles-based framework whose consent model addresses today's privacy concerns.

It is important to remember that PIPEDA's principle-based approach, which balances privacy and the interests of business in leveraging personal information, has successfully adapted to a range of new technologies since its introduction. If interpreted by the OPC in a manner that is pragmatic, and that balances both privacy and business interest, we believe that PIPEDA can continue to provide the necessary regulatory framework to protect privacy in the age of Big Data and the Internet of Things. For instance, PIPEDA already requires **transparency** around purposes for collecting, using or disclosing personal information and disclosure of policies and practices with respect to an organization's management of personal information. It also demands demonstrable **data governance** through the Accountability Principle, making changes like the formal incorporation of Privacy by Design unnecessary. In addition, PIPEDA provides a framework for leveraging concepts of **implied consent** and **exceptions to the notice and consent principle** and a **comprehensive regulatory oversight** through strong investigative, audit and information sharing powers. Overall, PIPEDA provides a flexible and adaptive framework that is well positioned to continue protecting the privacy of Canadians while allowing for business innovation even as technology continues to evolve.

As an industry, we recognize the value of a strong regulatory framework for privacy. Regulatory oversight and reasonable limitations on how data can be used are important elements in establishing trust between businesses and their customers. We look forward to working with the OPC, and all stakeholders, to enhance this trust in a manner that balances the protection of privacy with business practicalities in a data-driven economy.

### **Current Challenges with PIPEDA**

1. *Express consent is often over-emphasized in interpretations of PIPEDA. This form of consent has practical limits*

As the OPC has highlighted, experience has shown that there are many occasions where it is not practical to obtain express consent, or where consent is unlikely to be meaningful. Specific challenges include:

- i) *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 (PI) to individuals. On some level, trust needs to be at the core of any privacy system. Both industry and the OPC have important roles to play in creating a trustworthy privacy environment.

Over-emphasizing express consent does a disservice to the notion of consent and potentially exposes consumers to harm when they do not differentiate between the more sensitive and more innocuous uses of data. In order to build and foster trust, it is incumbent upon organizations to increase transparency and accountability. This could allow for the increased use of implied consent.

- ii) *Unanticipated Uses*: PIPEDA calls for purposes for PI 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 express consent. There should be more explicit flexibility in interpretations of PIPEDA to allow for responsible new uses after the fact in certain circumstances through existing tools, such as use for a consistent purpose that is reasonable in the circumstances and implied consent.
- iii) *Increasing Technological Complexity*: As noted by the OPC, as connected and sensor enabled technologies become more ubiquitous in our lives, there will be scenarios where “traditional point-to-point transfers of data are being replaced with data flows through distributed systems, making it difficult for individuals to know which organizations are processing their data and for what purposes.” While this complexity may complicate traditional contractual approaches to consent, it should not be viewed as fundamentally undermining the protection of individual privacy. Encryption, de-identification/anonymization and other data approaches or technologies can ensure an individual’s privacy remains protected in these complex systems. Opportunities exist for the OPC, industry and all stakeholders to work together to explore privacy protection in these more complex data scenarios.

## 2. *Data minimization principle in PIPEDA runs contrary to successful analytics*

Data analytics has the potential to deliver far-reaching benefits to our economy and society. However, an overly broad and rigid interpretation of *Principle 5—Limiting Use, Disclosure, and Retention* of personal information—runs contrary to successful analytical approaches. Correlations between data sets are not always obvious and larger sets of data, collected over longer time periods, are the most likely to provide highly impactful results. To realize the economic and social benefits of data analytics, while protecting individual privacy, it is important that the OPC support responsible approaches to analytics that minimize the risk to individuals through anonymization or de-identification. As a result, we recommend that the OPC clarify that the act of de-identifying data is not a “use” that would require consent and take a pragmatic approach to determining adequate safeguards for anonymization and de-identification.

## 3. *Broad view of “personal information”*

Challenges can arise when regulators take a hypothetical or speculative view towards how non-personal information could be re-identified or combined to create personal data. There also can be challenges when regulators provide guidance on uses of all data types, not just PI. It is important that the OPC continue to take a strong, risk-based approach to protecting the privacy of Canadians and be mindful of inadvertently attempting to regulate economic activities outside their purview. While some argue that all data can be re-identified, we urge the OPC to take the more practical approach adopted in the UK, which builds upon a framework of taking all reasonable steps to eliminate the risk of re-identification. The requirement is to use technical and contractual measures to mitigate risk until the risk is remote.

## Framework for identifying forward-looking solutions

Recognizing the importance of Canada's privacy regime in supporting a trustworthy business environment, ITAC has identified several principles that we encourage the OPC to adopt when developing forward-looking solutions:

1. *Aim to achieve a balance between privacy rights and legitimate business interests.* A risk-based approach that focuses on how the collection, use and/or disclosure of PI actually impacts the individual and whether the impacts are fair and proportionate to the benefit is the most likely to give rise to meaningful privacy and allow for other interests to also be protected and enabled. We recommend that the OPC focus more on transparency, reasonable purposes and accountability, and less on maintaining unrealistic models of notice and consent rooted in classical contract theory. We encourage the OPC to partner with all stakeholders to keep interpretations of PIPEDA relevant and current.
2. *Rely on general principles and avoid rules that are unnecessarily prescriptive or narrowly focused.* We suggest maintaining the technology neutral, flexible, context-specific and principles-based approach already reflected in PIPEDA.
3. *Ensure both technology and business paradigm neutrality.* As technology is constantly evolving, it is important that privacy regulations not lock businesses into any particular solution or approach. Likewise, it is important that the OPC not discriminate or create differing requirements based on particular business models or data use-cases (e.g. selling insights gleaned from de-identified user data) or industry sectors. As new, integrated business models emerge, the idea of separating industries into silos is less relevant. Privacy regulation should focus on the privacy-impacting behaviour regardless of industry sector.
4. *Ensure Canada's approach is not more restrictive or prescriptive than other similar jurisdictions and pursue international interoperability where appropriate.* Canada should work with industry and other national governments, through organizations like the Organization for Economic Cooperation and Development (OECD) and the Asia Pacific Economic Cooperation (APEC) to develop interoperable approaches to privacy.<sup>1</sup> In parallel, ensure Canada's approach within its own borders creates consistent and equal treatment among both Canadian and international businesses. Businesses should be treated equally and none should be held to a higher standard than another; especially if the standards are prohibiting Canadian companies from competing with U.S. and international counterparts.
5. *Avoid introducing "no-go zones."* "No-go zones" are unnecessary in the Canadian context. PIPEDA already includes a reasonable purposes restriction in section 5(3) that ensures "responsible use" of PI. For example, because discriminatory uses that violate human rights legislation would not be reasonable, introducing an explicit restriction on such uses is unnecessary. There should be no specific limits on what types of data can or cannot be collected, used or disclosed by an organization, as long as the organization complies with the principles of PIPEDA and Canada's other laws.

---

<sup>1</sup> This should not mean the wholesale adoption of solutions from other jurisdictional contexts. The OPC consultation document highlights a number of proposed elements of the EU's General Data Protection Regulations (GDPR). It is important to note that the GDPR is not yet in force and many of its positions are still highly contentious. While it is important to learn from other jurisdictions, a better understanding of the impacts of the specific EU GDPR case will emerge after it has been finalized and put into force.

## 6. *Utilize the OPC's Mandate to Educate the Public*

While it is important that the OPC partner with industry and academia, the OPC also has an important responsibility to educate the public on privacy issues. Public education needs to remain a core element of the OPC's strategy to protect the privacy of Canadians.

## **Solutions/potential enhancements to PIPEDA**

As previously discussed, PIPEDA provides a flexible and adaptive framework for protecting the privacy of Canadians while allowing for business innovation. This framework has stood the test of time and, as a result, we believe that any amendments to PIPEDA to address data analytics should be limited in scope and focus on reducing uncertainty.

Should the OPC believe that its hands are tied by the current law (e.g. a risk-based approach to consent cannot be leveraged), and/or if the government pursues amendments to PIPEDA, ITAC would recommend the following changes to support achieving the objectives of the legislation (which changes would be subject to PIPEDA's data governance requirements and "reasonable purposes" restrictions):

### 1. *Introduce a New Exemption for Legitimate Business Interest*

PIPEDA's existing exceptions to consent and the principle of implied consent already support an interpretation that allows for processing of PI based upon legitimate business interests within the boundaries of responsible use under PIPEDA (including the reasonable person test under Section 5(3)). To promote clarity on how the current consent rules support responsible use of PI for data analytics, ITAC recommends that the OPC issue related interpretation guidance. Alternatively (or in addition), the OPC could recommend to the government that a new legitimate business interest exception be added to PIPEDA. Industry recognizes that business uses that rely on this exception must be based on demonstrable data governance and transparency. Should the government pursue an amendment to PIPEDA, the legislation should maintain a non-prescriptive, principles-based approach that allows Canada's privacy framework to evolve over time.

### 2. *New exception to consent for "consistent" purposes*

Recognizing the practical human limits in communicating a comprehensive understanding of every potential data use case, a new exception could be introduced allowing for the use of data for purposes consistent with those for which consent was originally obtained.<sup>2</sup>

### 3. *Updated exception to consent for "publicly available" information*

The understanding of "publicly available" information outlined in PIPEDA's regulations (i.e. phone book details) are outdated and do not reflect the current landscape of personal information shared in public venues.<sup>3</sup> We recommend that the OPC undertake a consultation with all stakeholders to develop a new principles-based, technologically neutral exception for publically available information that is better suited to adapt and evolve over time.

In addition to these possible legislative changes, we recommend that the OPC take the following additional steps:

---

<sup>2</sup> Note: A separate exception for "consistent purposes" would potentially not be necessary if an exception for "legitimate business purposes" is created.

<sup>3</sup> [https://www.priv.gc.ca/leg\\_c/interpretations\\_06\\_pai\\_e.asp](https://www.priv.gc.ca/leg_c/interpretations_06_pai_e.asp)

*4. Recognition from the OPC that the process of anonymizing/de-identifying personal information is not a “use”*

As the OPC consultation paper notes, many international bodies and experts support anonymization and de-identification as a way to enhance privacy and the security of PI. However, there is confusion around whether the act of de-identifying PI constitutes a “use” which requires specific consent. ITAC strongly recommends that the OPC follow the lead of other jurisdictions and clarify that anonymization/de-identification, which ultimately protects the privacy of individuals, does not constitute a “use” under PIPEDA and issue interpretation guidance that identify pragmatic principles to be considered when organizations implement technical and contractual safeguards relating to anonymization/de-identification.

*5. Support voluntary initiatives to control the risk of re-identifying de-identified data through contractual means in appropriate circumstances*

The OPC consultation paper highlights Robert Gelman’s suggestion that technical approaches to de-identification could be complimented with voluntary contracts that formalize an agreement not to attempt re-identification of data sets.<sup>4</sup> In appropriate circumstances, this is a common sense approach to managing and mitigating risk that will protect individuals and create open space for business use of de-identified data. The OPC should work with industry to support voluntary use of this approach in appropriate circumstances.

*6. Support transparency through voluntary industry-led codes of conduct*

In its consultation paper, the OPC raises the possibility of working with industry to develop voluntary codes of conduct to help organizations demonstrate compliance. In general, ITAC supports this self-regulatory approach. We believe that any initiatives should be voluntary and industry-led and recommend that the OPC focus on (i) promoting particular behaviours, rather than mandating practices for particular industries, and (ii) exploring harmonization with international certifications or standards to limit unnecessary duplication. The UK ICO’s Code on de-identification is an example of a practical guidance that balances of privacy and utility.<sup>5</sup>

*7. Support privacy innovation*

As the consultation document notes, a range of new technologies and organizations are being developed to help mitigate privacy risks. These include anonymization techniques with internal control to prevent re-identification as well as the development of trusted data repositories/intermediaries. A number of Canadian firms are already emerging as early leaders in these new fields, with Canada being well-positioned to become a global leader in privacy technology. While maintaining strict technological neutrality as a regulator, ITAC recommends the OPC become a champion for funding the development growth of innovative privacy technologies and organizations in Canada.

---

<sup>4</sup> OPC Consent and Privacy Discussion Paper. Pg. 16

<sup>5</sup> <https://ico.org.uk/media/1061/anonymisation-code.pdf>

## Part B: Answers to specific consultation questions

### **1) Of the solutions identified in this paper, which one(s) has/have the most merit and why?**

ITAC does not believe there is a need to overhaul PIPEDA. PIPEDA's principle and partnership-based approach has been successfully applied to new technologies in the past and there is no evidence to show that potential new scenarios presented by data analytics and the internet of things cannot similarly be addressed within the existing framework. However, it is crucial that the manner in which PIPEDA's principles are interpreted and applied evolve in a practical manner that reflects changes in society's attitudes, technology and business models.

Should the government consider changes to Canada's approach to consent, ITAC would recommend the following limited changes as a way to reduce confusion and support the objectives of the legislation:

- Clarify and/or codify existing interpretations of PIPEDA by introducing a new exception to consent for "legitimate business interests" and/or a new exception to consent for "consistent" (which changes would be drafted within the general boundaries of responsible use within PIPEDA (including the reasonable person test under Section 5(3)).

Additionally, ITAC is supportive of the OPC:

- Working with industry to promote voluntary contractual means to control the re-identification of data in appropriate situations;
- Promoting voluntary, industry-led approaches to improve transparency and compliance, such as behaviour-based codes of conduct; and
- Recognizing a broader role for implied consent than already exists in PIPEDA, when combined with improved transparency and accountability frameworks.

### **2) What solutions have we not identified that would be helpful in addressing consent challenges and why?**

To reduce uncertainty and to update Canada's consent framework, ITAC recommends that the OPC consider the following solutions which were not included in the paper:

- Convene a consultation with stakeholders to update the exception of consent for "publicly available" information to adopt a principles-based, technology neutral approach that will be better able to adapt to new technologies.
- Issue OPC guidance that recognizes that anonymization/de-identification is not a "use," and is thereby exempt from informed consent requirements.
- While maintaining strict technological neutrality as a regulator, support additional R&D funding for new technological/organizational approaches to mitigate privacy and security risks such as anonymization/de-identification technologies with internal controls to prevent re-identification, and the development of trusted data repositories/intermediaries.

### **3) What roles, responsibilities and authorities should the parties responsible for promoting the development and adoption of solutions have to produce the most effective systems?**

The data governance principles (as reflected in the OPC’s accountability guidelines), together with the reasonable purposes test in section 5(3) of PIPEDA, provide a roadmap for “responsible use” of data. Voluntary codes of conduct can be expected to provide additional visibility of organizations’ activities and provide additional grounds upon which organizations can demonstrate compliance.

Additional OPC enforcement powers are not needed at this time. Enhanced enforcement powers were recently added in 2015 through the *Digital Privacy Act*, and time is needed to test their effectiveness.

ITAC recommends against introducing order-making powers for the OPC, as this would run contrary to the facilitative, information-sharing enforcement framework successfully used to advance compliance with PIPEDA.

### **4) What, if any legislative changes are required?**

As previously discussed, PIPEDA provides a strong and flexible framework for protecting privacy and facilitating responsible data practices. Any changes to the legislative/regulatory framework should be limited in scope and focus on clarifying existing interpretations. Where further clarity is required, the OPC should provide additional details through compliance support materials, business-ready guidelines, etc. as these are better positioned to be updated and revised as new technologies and privacy challenges emerge.

While fundamental changes are not required at this time, especially if the law is interpreted in a pragmatic way which supports both privacy and economic interests, should the government seek to amend PIPEDA’s legislative or regulatory framework, ITAC would recommend:

- Clarifying and/or codifying existing interpretations by introducing an exception to consent for “legitimate business interests” and/or a new exception to consent for “consistent” purposes subject to a reasonable person test of section 5(3).
- Convening a consultation with all stakeholders to update PIPEDA’s *Regulations Specifying Publicly Available Information (SOR/2001-7)* and develop a principles-based, technology neutral approach that will be better suited to evolve with technological change.

---

ITAC would welcome the opportunity to participate in further consultations with the OPC, the Department of Innovation, Science and Economic Development and all other stakeholders to develop practical approaches to modernizing consent and privacy that enhance transparency and trust and that work for all Canadians.

For further information please contact David Messer, Senior Director of Policy, ITAC at [dmesser@itac.ca](mailto:dmesser@itac.ca)

