TECHNATION^CA

October 16th, 2020

Ontario Private Sector Privacy Reform

Submission of TECHNATION

TECHNATION welcomes the opportunity to provide its comments on the Province of Ontario's discussion paper regarding private sector privacy reform.

TECHNATION 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.

Introduction

There is a growing consensus that Canadian privacy laws need to be modernized. The emergence of digital technologies and services has transformed data practices, creating both the benefits of data-driven innovation and risks associated with expanded collection, use and disclosure of personal information. Current privacy laws mostly pre-date this transformation, making it important to assess whether they are adequate to address real and significant concerns about the protection of personal information in a data-driven economy.

When done responsibly, the analysis and use of personal information can be highly beneficial to individuals, businesses, governments and society at large. Data-driven technology and products are already empowering science, supporting innovation, and driving economic growth. There are countless examples of data-driven technology and products improving medical care, making our roads safer, reducing energy consumption and keeping us informed. Data-driven businesses in Ontario are creating new jobs and driving new tax revenues.

Responsible use of personal information must be built on a strong foundation of trust and transparency. Individuals need to be informed of, and have appropriate control over, what data about them is being collected and how it is 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.

TECHNATION CA

Is a Made-in-Ontario law needed?

A threshold question for the Province of Ontario is whether a made-in-Ontario private sector privacy law is needed. Currently, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs the collection, use and disclosure of information in the course of commercial activities within the province. This federal legislation, together with active enforcement by the Office of the Privacy Commissioner of Canada, has provided a resilient legal framework for regulating personal information practices of businesses operating in Ontario.

The Government of Canada has indicated that it is committed to modernizing PIPEDA. It has undertaken a formal consultation process in advance of introducing privacy reform legislation, with a bill expected to receive first reading in Parliament at any time.

The Department of Innovation, Science and Economic Development (ISED) has signaled that its package of privacy reforms will be designed to enhance individuals' control over their personal information, enhance data subject rights, and enable responsible innovation. Significantly, it is expected that each of the "Key Areas for Reform" identified in the Ontario discussion paper (i.e., transparency, consent, the right to be forgotten, data portability, oversight, compliance and enforcement powers and use of de-identified data) will be addressed.

With PIPEDA reform on the horizon, TECHNATION questions whether a made-in-Ontario law is needed. Enacting Ontario private sector privacy legislation would add to Canada's patchwork of private sector privacy laws (currently comprised of PIPEDA and provincial legislation in British Columbia, Alberta and Quebec), creating additional compliance challenges and costs for all businesses operating in Ontario without obvious offsetting privacy benefits. Additionally, because multiple enforcement agencies would have overlapping investigative authority for the same privacy violation, Ontario would become less desirable as a place in which to do business.

These negative impacts can be avoided – without compromising privacy protections – through a single national standard created using federal legislation (i.e., PIPEDA). We urge the Province of Ontario to endorse PIPEDA as this national standard and commit to working with the Government of Canada to ensure that PIPEDA is modernized in a way that meets the Province's policy objectives set out in its discussion paper on privacy reform. Additionally, we recommend that the Province consider enacting new privacy rules only as necessary to fill in gaps in the existing regulatory framework by regulating the privacy practices of non-commercial organizations, such as not-for-profits, charities, trade unions and political parties. By adopting this approach, Ontario can be a leader in promoting stronger privacy laws, while minimizing unnecessary regulatory costs and burdens on businesses.

TECHNATION CA

Privacy reform generally

PIPEDA and comparable provincial laws have proven to be effective and resilient. They provide a comprehensive, yet flexible framework for regulating the collection, use and disclosure of personal information. This framework can be applied to new and unforeseen commercial activities in a rapidly changing data environment, without the need for frequent legislative amendments. The effectiveness of the current laws can be attributed to the following foundational features:

1. They are principles-based, allowing organizations to implement privacy protections in a flexible and context-specific manner, taking into account actual risks;
2. They are technology and business sector neutral, making them largely future-proof;
3. They rely on privacy principles that are both non-prescriptive and generally consistent with common-sense business practices, making it possible for most businesses to understand what the law requires;
4. They balance privacy considerations with business requirements – something that is explicitly required by the purpose statement found in section 3 of PIPEDA;
5. They are substantially similar, both in approach and in specific requirements; and
6. They are interoperable with privacy laws elsewhere, including the EU.

As the Province looks to identify how the current regulatory framework can be modernized, it is important to acknowledge the importance of these foundational features. We recommend that they be reflected in any new privacy law enacted by the Province.

Key areas of reform identified in the discussion paper

This section of our submission provides TECHNATION's input on each of the "Key Areas of Reform" identified in the Province's discussion paper.

Increased consent and clear transparency

TECHNATION agrees with the Province's focus on re-imagining consent and considering alternative models. We are supportive of general principles requiring clean and plain language information to explain what information is collected, how it is collected, how it is used, and with whom it is shared. We are also supportive of the Province's proposals to reduce the circumstances when consent is needed (both by requiring consent only for collections, uses, and disclosures of personal information that are outside the organization's described practices and by creating new exceptions

TECHNATION CA

to consent for situations in which individual consent is not necessary, practicable or appropriate, such as when the collected data has been “de-identified” or “derived”).

For the Ontario proposals to be effective, TECHNATION believes that it will be critical for any new privacy law to:

1. Avoid prescriptive rules on what information needs to be disclosed or how disclosure must occur;
2. Be consistent with well-established findings and guidance issued under PIPEDA which allow for organizations to rely on different forms consent (which may include implied and opt-out consent) in appropriate circumstances, rather than mandating the use of opt-in consent in all circumstances or default settings that are always set to the most privacy protective; and
3. Be clear that personal information that has been de-identified is not subject to a consent requirement (see discussion of de-identified information below for a related proposal).

4. Also critical is that alternative authority for processing personal information be added. TECHNATION recommends that the Province look to the General Data Protection Regulations (“GDPR”) in the European Union for an example of how this can be accomplished. Article 6 of the GDPR sets out five grounds for processing in addition to consent:
    - Performance of a contract;
    - Compliance with a legal obligation;
    - Vital interest of the data subject;
    - Public interest; and
    - Legitimate interests.

Data rights: erasure and portability

The introduction of new data rights may create significant costs and compliance challenges for businesses, particularly if they are introduced before international standards have emerged. We recommend that, if introduced, any data rights be made interoperable with laws elsewhere and calibrated so that they do not create barriers to entry for start-ups and other smaller and medium-sized enterprises.

Data erasure

Consistent with the recent recommendation to a British Columbia legislative committee made by the Information and Privacy Commissioner of BC, we recommend that the Province monitor policy and legislative developments in the area, globally and at home, to ensure harmonization with

similar laws in terms of any provision it brings forward.

Any data erasure rights need to take account of legitimate interests to retain data in certain circumstances.

We believe that it will be critical that any new data erasure rights:

1. Avoid requiring a platform or service provider to make a subjective assessment of whether content should be removed;
2. Avoid creating a blanket right to deletion (as doing so would necessitate the creation of many exemptions, which would contribute to complexity and inflexibility);
3. Focus on information that is online and accessible to others where continued availability negatively impacts the individual in a meaningful and inappropriate way; and
4. Enable an organization to retain data that it has a legitimate reason to keep, so that withdrawal from public view (rather than deletion) is sufficient.

Data portability

TECHNATION believes that any data portability right should, if introduced, recognize the need for a consistent international approach aimed at creating workable standards. Some members of TECHNATION are founder members of the Data Transfer Project - https://datatransferproject.dev , an initiative through which open standards for data portability are being developed. We recommend that the Province monitor policy and legislative developments in the area, globally and at home, to ensure interoperability with similar laws.

If the Province decides to enact data portability rights at this time, it will be critical that any new rights:

1. Be narrowly defined so that they apply only when technically and operationally feasible;
2. Focus on requiring that personal information be provided to or made accessible to an individual, rather than a requirement that an an organization directly transfer 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 organization to another);
3. Apply only to personal information that is held electronically;
4. Apply only to personal information that is provided by the individual and transactional data (i.e., exclude derived information and de-identified data);
5. Exclude 3rd party information (at least where it would adversely affect the rights of 3rd parties);

TECHNATION CA

6. Exclude call-notes and complaints;
7. Not prejudice the legal rights of the disclosing parties;
8. 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); and
9. Allow for cost recovery in accommodating transfer requests.

Oversight, enforcement and fines

TECHNATION believes that any enforcement powers must be respectful of administrative laws and the principles of natural justice. Of critical importance, the Information and Privacy Commissioner (IPC) must not be an advocate for a complainant while also serving as the judge and jury. As well, there must be an adequate appeal process, and any self-initiated investigation should be tied to the IPC having reasonable grounds to believe that the organization is non-compliant with the legal standard.

Additionally, we recommend that:

1. Any order-making powers granted to the IPC be limited to egregious cases when material harm exists or is imminent;
2. There be proportionality between a violation, the size and capabilities of the organization that committed the violation, and any fine;
3. Maximum fines take into account the relatively small size of the Ontario market – for example, the maximum fines under the GDPR are an inappropriate point of comparison, given that the population of the EU is 30 times the population of Ontario; and
4. The IPC not have jurisdiction to investigate or enforce the Ontario law if PIPEDA applies to the collection, use or disclosure of the personal information in question.

In respect of our last recommendation, section 3(2)(c) of the Personal Information Protection Act in British Columbia provides an important precedent. Adopting the same approach will help to prevent conflicting jurisdiction among the Privacy Commissioner of Canada and the Ontario Information and Privacy Commissioner. Overlapping enforcement may increase compliance costs for companies that operate across the country, while also creating the risk of uneven levels of privacy enforcement for citizens. The GDPR's one-stop-shop mechanism for regulatory oversight also serves as an important reference point.

De-identified personal information and data derived from personal information

TECHNATION believes that permitting the use of de-identified data is critical to enabling responsible use of data, including for commercial purposes. Any related rules, including definitions

TECHNATION CA

of key concepts, should be aligned with what we have identified above as the foundational features of privacy laws in Canada. Specifically, they should be:

1. Principles-based;
2. Technology and business sector neutral;
3. Balanced (as between privacy considerations and business needs);
4. Substantially similar, both in approach and in specific requirements, to other privacy laws in Canada; and
5. Interoperable with privacy laws elsewhere.

TECHNATION supports the proposal by the Canadian Anonymization Network ("CANON") in its comments to ISED regarding PIPEDA modernization. CANON has recommended the adoption of a risk-based framework for de-identification based on a "spectrum of identifiability", where information that poses no serious risk of re-identification could remain outside of the application of privacy law, while information with a low risk of re-identification could be covered by privacy law, but with certain exemptions such as consent.[1] The Information and Privacy Commissioner of Ontario has also expressed support for this approach in the past.[2]

Enabling data-sharing for innovation, while protecting privacy

TECHNATION is encouraged that the Province is looking to identify strategies for enabling data-sharing for innovation, while protecting privacy. We agree that data trusts warrant exploration, as they can maximize data usage for innovation, while concurrently enhancing public trust. However, it is clear that there remain significant obstacles to the use of data trusts that will need to be overcome – including governance, costs and legal liability. As well, we believe that data trusts should be seen as only one of many tools to enable responsible innovation. Other tools include adding new grounds for processing personal information (including public interest and legitimate purposes) and permitting both the use of de-identified data and the pooling of data from multiple sources through the implementation of appropriate data governance, de-identification and accountability frameworks.

Additional issues

The final section of our submission sets out recommendations of TECHNATION in respect of issues not explicitly addressed in the Province's discussion paper.

[1] CANON's submission to ISED can be found at: https://deidentify.ca/wp-content/uploads/2019/10/CANON-Submission-ISED-Strengthening-Privacy-for-the-Digital-Age.pdf.

[2] See Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacyfound, which can be found at: https://www.ipc.on.ca/wp-content/uploads/2016/11/anonymization.pdf.

TECHNATION CA

Transborder data flows

Taking into account the importance in the digital and traditional economies of cloud computing and hosted services, privacy laws need to permit and even facilitate the transfers of personal information outside the province and Canada. TECHNATION strongly believes that the framework for transfers of data outside Canada developed under PIPEDA is both effective and appropriate to achieve this outcome. If the Province decides to enact private sector privacy laws, we recommend that it adopt a similar approach to PIPEDA, and consistent with the framework under PIPEDA, view transfers of information as a "use" by an organization and not a disclosure for which additional consent is required.

Employee privacy

Consent is not the appropriate legal authority for the collection, use or disclosure of employee personal information. An employee is generally unable to provide free consent given the imbalance of power between an employee and employer. The collection, use or disclosure of personal information about an individual that is collected, used or disclosed to establish, manage or terminate an employment relationship should be excluded from consent requirements. It should be adequate for the employer to notify the data subject that it will be collecting this information and inform them of the purposes for the collection.

This recommendation is consistent with employee privacy provisions in private sector privacy laws in British Columbia and Alberta. It is also in line with the concept in the GDPR that there are multiple legal bases that may be relied upon to authorize processing.

Codes of conduct and privacy certifications

Codes of conduct and privacy certifications should be incentivized (but not mandated) by privacy laws. This can be accomplished by calling them out as factors to be considered in connection with a due diligence defence.

TECHNATION CA

Concluding remarks

We hope that this submission will be helpful to your deliberations on privacy reform in the Province. The issues you are tackling are critical to Ontarians – both because of the importance of protecting their personal information and because of the importance of data to the Ontario economy and the health and well-being of all residents of the Province.

We would welcome the opportunity to discuss our submission and this privacy review. Please contact TECHNATION to discuss, we can bring together experts from the tech sector to provide greater input and feedback. Our membership ranges from large multinationals, to Canadian telecommunication companies and Ontario based SMEs.

Sincerely,

Nevin French

Nevin French
Vice-President, Policy
TECHNATION
nfrench@technationcanada.ca
Cell 613-240-7378

5090 Explorer Drive, Suite 510,
Mississauga, Ontario, L4W 4T9