Submission to the Ontario Ministry of Government and Consumer Services: Modernizing Privacy in Ontario

September 2021

BC Freedom of Information and Privacy Association

PO Box 8308 Victoria Main

Victoria, BC V8W 3R9

Phone: 604-739-9788

Website: https://fipa.bc.ca

Email: fipa@fipa.bc.ca

Prepared by: Evan Brander, Legal Researcher

Table of Contents

About FIPA

The BC Freedom of Information and Privacy Association (FIPA) is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. While we are based in BC, our membership extends across Canada, and we regularly partner with organizations throughout the country.

Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform. We are one of very few public interest groups in Canada devoted solely to the advancement of freedom of information and privacy rights.

Introduction

Privacy is a fundamental right of all Canadians, and we must have strong legislative frameworks in place across the country to protect this right.

We believe that the proposal put forward by the Ontario Government would lay a strong foundation to protect Ontarians' rights. On a number of important issues, it would also set a strong precedent that we hope would be followed by other provinces across the country.

Ontario's proposal would not only benefit individual Ontarians, it would benefit Ontario businesses. It would do this in two key ways. First, research consistently shows that Canadians are more willing to do business with companies that provide easy-to-understand information about their privacy practices, and more likely to do business in jurisdictions where there are

strong privacy laws (including penalties for violating laws) in place.[1] While we acknowledge that increased privacy requirements impose initial compliance burdens on companies, businesses subject to strict privacy requirements would gain a competitive advantage over those in other jurisdictions.

The second way Ontario's proposed privacy law would benefit Ontario businesses is by ensuring there are no barriers to international trade and data transfers with other countries. The European Union's *General Data Protection Regulation* (GDPR) requires international jurisdictions' privacy laws to meet an "adequacy standard" before personal data is allowed to flow across European borders. Other jurisdictions like Japan and Brazil have adopted requirements similar to the GDPR. Strong privacy laws in Ontario will support Ontario's trade relationships with Europe, the Asia-Pacific and other fast-growing regions around the world.

We at FIPA strongly support Ontario's overarching goal of ensuring that Ontarians control the personal data they share, when they share it and who they share it with. The federal government's Bill C-11 is not fit for this purpose. Ontario's proposal to fill the gaps left by C-11 with a strong privacy

---

[1] ***See*** **Office of the Privacy Commissioner of Canada, *2018-19 Survey of Canadians on Privacy*, (9 May 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/>. According to the survey, 71% of Canadians were more likely to do business with a company if under Canadian law, the company would face strict financial penalties for misusing personal information; 69% of Canadians were more willing to do business with a company that provides easy to understand information about its privacy practices.**

law that expands the scope of legislation and strengthens privacy requirements is a significant step in the right direction.

In the enclosed submission, our comments do not comprehensively cover each element raised in Ontario's proposal. Instead, we comment on areas where we are particularly supportive of proposals or where we feel there is room for improvement.

We hope that our submission is helpful as you consider the development of an Ontario private sector privacy act. We congratulate you on the work you have done so far. Should you have any questions about our submission, we are available for further discussion.

Rights-based approach to privacy

Privacy is a fundamental human right, and we strongly support Ontario's proposal to affirm this within its privacy legislation.

Privacy is recognized in international law as a fundamental human right. For example, Article 13 of the UN Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights both recognize privacy as a human right.[2] The latter states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family home or correspondence… Everyone has the right to the protection of the law against such interference or attacks."[3]

Within Canada, privacy is protected as a fundamental right under Section 8 of the *Canadian Charter of Rights and Freedoms*. The Supreme Court has recognized the quasi-constitutional status of federal and provincial privacy legislation, stating in *Lavigne v. Canada* that "The *Privacy Act* is a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society."[4]

Further Supreme Court jurisprudence has emphasized the importance of protecting the fundamental right to privacy.[5] For example, Justices Abella

---

[2] *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948).

[3] *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171, Can TS 1976 No 47 (entered into force 23 March 1976).

[4] Lavigne v Canada (Office of the Commissioner of Official Languages) 2002 SCC 53, at 25.

[5] See e.g. *R v Spencer,* 2014 SCC 43*; R v Jones* 2017 SCC 60.

and Cromwell wrote in *Alberta (IPC) v. United Food and Commercial Workers*, that "the ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy."[6]

Recognizing privacy as a human right would also bring Ontario's privacy legislation in line with the EU's General Data Protection Regulation (GDPR). Aligning Ontario's law with the GDPR would be highly beneficial to Ontario businesses. Article 45 of the GDPR requires a country's privacy laws (or those of a region within a country) to afford an adequate level of protection for personal data to be transferred to it from the EU. Recognizing privacy as a human right would help Ontario's privacy law to achieve adequacy status from the EU. This would ensure that there is no disruption to Ontario businesses that rely on the transfer of personal data from the EU.

We are supportive of the proposed Preamble in Ontario's draft privacy law that would recognize privacy as a fundamental right and establishing principles for the appropriate collection, use and disclosure of personal information. We particularly support the inclusion of a strong statement that individuals are entitled to a fundamental right to privacy and the protection of their personal information. This would set a strong precedent that we hope will be followed in other provinces across Canada.

---

[6] **Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401, 2013 SCC 62.**

Safe use of automated decision-making

FIPA has substantial concerns about the use of automated decision-making systems and strongly believes that a legislative response is needed to address the challenges that they pose. Ontario's proposal would represent a significant improvement over the federal government's proposal in Bill C-11.

Automatic decision-making systems can significantly improve efficiency, but they can also reflect and reinforce existing social biases.[7] In one example, women were systematically discriminated against by a hiring algorithm trained to screen candidates for management positions. This was because the company using the system had trained their algorithm with data drawn from resumes of managers hired over the previous decade (who were primarily white and male).[8] Protections need to be in place to ensure that – if a company is going to make use of automated decision-making systems – they are not resulting in biased decisions.

A further problem comes from the fact that the analytical processes used by algorithms can be so complex, it is impossible for humans to understand the

---

[7] Niklas Kossow, Svea Windwehr and Matthew Jenkins, "Algorithmic Transparency and Accountability," Transparency International (5 Feb 2021), online: <https://knowledgehub.transparency.org/assets/uploads/kproducts/Algorithmic-Transparency_2021.pdf>. [*Transparency International*]

[8] Nicol Turner Lee, Paul Resnick and Genie Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms," Brookings (22 May 2019), online: <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>

specifics of how they arrived at a decision. Because of this, it may be difficult to detect biases in some cases.[9]

As Ontario's white paper notes, Bill C-11 attempts to address the issues created by the use of automatic decision-making systems by requiring that organizations using such systems:

- **Make available a general description of the organization's use of such a system to make predictions, recommendations or decisions (s. 62(2)(c));**
- **Upon request by an individual, provide them with an explanation of the prediction, recommendation, or decision and how the personal information that was used to make the prediction, recommendation or decision was obtained (s. 63(3)).**

We do not feel that this solution adequately addresses the challenges posed by the use of automatic decision-making systems. The onus should not be placed on the individual to request information about the automatic decision-making process, and it does nothing to address potential biases built into the AI system in the first place.
Ontario's proposed provisions mirroring the GDPR are much stronger, and FIPA believes that this is a significant improvement over the approach in Bill C-11.

---

[9] Transparency International, supra note 7.

We strongly agree with the proposed restrictions on the use of automatic decision-making where such systems could have serious implications. This is an important step that will alleviate concerns about the impact of AI systems in perpetuating bias and discrimination.

We would expand the prohibition to prevent the use of any automatic decision-making system that relies on biometric data to arrive at its decisions. Such systems are too invasive of privacy and have been shown on many occasions to incorporate racial and gender bias.

We also agree with the list of actions that an individual may take where an automatic decision-making system is in place but would go further. We believe that any company using automatic decision-making systems should be required to automatically provide individuals with reasons and the principal factors that led to the decision. In proposed subsection (2)6, we would add that the reviewing individual should have sufficient knowledge to review *and the ability to change the decision about the individual*.

Data transparency for Ontarians

With the advent of cloud computing, big data, and the Internet of Things, privacy policies have become complex and inaccessible, making it difficult for individuals to understand who is processing their information and for what purpose.[10] A poll commissioned by FIPA in 2020 found that 47% of British Columbians believe that organizations are not open and transparent about how they collect and use personal information.[11] We anticipate that a similar proportion of Ontarians would hold the same view that organizations are not up front about their collection and use of their data.

Privacy policies are often opaque and legalistic. An average privacy policy takes 10 minutes to read, and considerably longer to understand.[12] Research suggests that it would take approximately 200 hours to read all the privacy policies for all the websites the average Internet user visits each year.[13] The legalistic nature of these policies only adds more time. It is unrealistic and unfair to expect users to expend such an amount of time reading, and perhaps considerably more time working to interpret and understand, privacy policies.

---

[10] OPC Letter to ETHI, *supra* note 14

[11] BC FIPA 2020 Survey, *supra* note 7

[12] Out-Law News, "Average privacy policy takes 10 minutes to read, research finds", (October 6, 2008), https://www.pinsentmasons.com/out-law/news/average-privacy-policy-takes-10-minutes-to-read-research-finds

[13] Ibid

We believe that for consent to be meaningful, individuals need to have a clear and complete understanding of the information that is being collected, how it will be used and who it will be shared with.

We strongly support enhanced transparency measures that would require organizations to make information about their privacy policies and practices readily available in plain language. Ontario's proposed list of details that organizations would be required to provide is comprehensive and would greatly improve transparency. This represents a large step forward from Bill C-11.

One area where FIPA would recommend additional measures to improve data transparency is where organizations intend to introduce privacy-impacting technologies or practices. Ontario's legislation could require organizations to conduct a privacy impact assessment of any new technologies or practices they intend to implement that will impact the collection, use or retention of personal information and publish the assessment upon implementation.

Ontario's proposal to set certain requirements for consent to be valid would also represent a positive development. We are again very supportive of this proposal.

Protecting children and youth

Many young people are constantly connected to the internet through their phones, tablets, smart toys and other connected devices. For many children, online presences are key to their identities, expression, and social interactions. This can lead to children sharing information without considering the potential privacy implications of doing so. Research has shown that children often post information wherever there is a field to do so on a site and will share more information when a site promises greater benefits.[14] A report from England's Children's Commissioner calculated that by the time a child turns 18, there are likely to be about 70,000 posts about them on the internet.[15]

Children and youth may not understand the risks to themselves or their families that come with their data being constantly collected. Studies have shown that ongoing online monitoring of children can have significant developmental impacts, leading to a lack of trust and reduced autonomy and independence.[16] There are also concerns that the wealth of data

---

[14] Valerie Steeves, *Summary of Research on Youth Online Privacy*, Commissioned by the Office of the Privacy Commissioner of Canada (March 2010), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/yp_201003/>.

[15] Children's Commissioner for England, *Who Knows What About Me?,* (Dec 2018), online: <https://www.childrenscommissioner.gov.uk/digital/who-knows-what-about-me/>.

[16] Research Group of the Office of the Privacy Commissioner of Canada, *Surveillance Technologies and Children*, (Oct 2012), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/opc_201210/>.

collected about children can end up impacting important aspects of their later life, including university admissions, job applications and credit or insurance availability.[17]

In light of these significant concerns, it imperative that appropriate protections be put in place to safeguard the privacy of young Ontarians.

We are supportive of Ontario's approach to requiring parental consent for the collection, use and disclosure of the personal information of a child under 16. This is similar to the approach in the US, where the *Children's Online Privacy Protection Act* requires parental consent to collect the personal data of children under the age of 13.

However, we have some concerns about this approach. The Canadian Civil Liberties Association has noted parental consent may be undermined by youth simply lying about their ages, or by firms attempting to circumvent requirements by relying on generic statements that their websites are not intended for children.[18]

Additional measures beyond parental consent are needed to protect children's privacy online. We support Ontario's proposal to establish a "no-go zone" stating that the legitimate needs of an organization cannot include

---

[17] Children's Commissioner, supra note 14.

[18] Canadian Civil Liberties Association, "Submission to the Special Committee to Review the *Personal Information Protection Act* in the Province of British Columbia," (14 Aug 2020), online: <https://ccla.org/cclanewsite/wp-content/uploads/2020/10/2020-08-14-CCLA-submission-BC-PIPA-review-1.pdf> at 14.

monitoring or profiling of an individual under the age of 16 for the purposes of influencing their behaviour.

We would further advocate for a right for Ontarians to have all data collected on them when they were 18 years of age or younger deleted.

A fair, proportionate, and supportive regulatory regime

It is an unfortunate necessity that there needs to be strong enforcement measures in place to ensure compliance with privacy legislation. FIPA has advocated in past submissions to the BC government for increased Privacy Commissioner powers that would expand tools for enforcement.19

This is why we are strongly supportive of Ontario's proposed enforcement regime. Allowing the commissioner to impose sanctions on the worst offenders is a much-needed deterrent that will help improve compliance with the act. Giving the commissioner the authority and resources to initiate and conduct audits and investigations and make orders is crucial to building a strong privacy enforcement regime.

We support Ontario's proposal to empower the commissioner to impose financial penalties that vary depending on the severity of non-compliance and mitigating circumstances. We believe that the mitigating circumstances listed in Ontario's white paper are appropriate.

We prefer Ontario's proposed approach to administering the financial penalty regime to that contained in Bill C-11. The CPPA would create a new administrative tribunal to hear privacy complaints, where the Privacy Commissioner has recommendation powers to the tribunal. Ontario's approach of directly empowering the commissioner to impose penalties is

---

[19] BC Freedom of Information and Privacy Association and BC Civil Liberties Association, *Joint Submission to the Special Committee to Review the Personal Information Protection Act*, (14 Aug 2020), online: <https://fipa.bc.ca/wp-content/uploads/2020/08/20200814_BCFIPA_BCCLA_PIPA_Committee_Submission.pdf>.

simpler and would reduce costs and delays – while still being subject to oversight by the judiciary.

We also support the proposed statutory offences. In particular, we are happy to see a proposal for an offence for the re-identification of previously de-identified information, as we view this as a significant and growing threat to privacy.

Ontario has proposed creating a strong enforcement regime that will go a long way towards ensuring compliance with privacy laws in the province.

Conclusion

We again wish to congratulate Ontario on the proposal it has developed to create a strong privacy law that would protect the fundamental rights of Ontarians.

While we agree with the large majority of the proposals included in Ontario's White Paper, we note that there is limited discussion of some key privacy issues. The first missing issue is specific privacy protections relating to the collection, use and distribution of biometric data. The collection and use of this data is highly intrusive on privacy, and we feel that the law needs to clearly define individuals' rights and organizations' responsibilities relating to biometric information.

Additionally, we note that there is limited discussion of the collection of personal information by law enforcement. We feel it is important for any Ontario privacy law to specify that personal information may only be shared with law enforcement with prior judicial authorization, as is required by the *Canadian Charter of Rights and Freedoms*.[20]

---

[20] For example, in *Hunter et al. v Southam Inc.*, 1984, 2 SCR 145, Justice Dickson held that section 8 of the Charter "extends at least so far as to protect the right of privacy from unjustified state intrusion. Its purpose requires that unjustified searches be prevented ... This can only be accomplished by a requirement for prior authorization".

We have also made suggestions above for improvements to various aspects of Ontario's proposal, where we feel that additional privacy protections would be beneficial.

In spite of these concerns, Ontario's proposal represents a significant improvement over existing Canadian privacy legislation and the proposed *Consumer Privacy Protection Act*. If Ontario's proposals were enacted in law, the province would be demonstrating leadership on the protection of privacy and set a precedent for the federal government and other provinces to follow.