Joint Supplementary Submission to the Special Committee to Review the Personal Information Protection Act

July 2021

BC Civil Liberties Association

BC Freedom of Information and Privacy Association

Table of Contents

Introduction

This submission supplements the joint submission made by the BC Freedom of Information and Privacy Association (FIPA) and the BC Civil Liberties Association (BCCLA) to the Special Committee to Review the *Personal Information Protection Act* (PIPA) during the 41st Parliament.[1] Since our initial submission last year, the federal government has introduced *Bill C-11: Digital Charter Implementation Act, 2020*.[2] Bill C-11 would repeal part 1 of the federal *Personal Information Protection and Electronic Documents Act* and enact the *Consumer Privacy Protection Act* (CPPA) in its place.

The CPPA states that it prevails over provincial laws, unless the Governor in Council is satisfied that a province's legislation is substantially similar to the CPPA. BC PIPA is currently designated as substantially similar to the outgoing *Personal Information Protection and Electronic Documents Act*, but it will need significant amendments in order to be declared substantially similar to CPPA. While we have significant concerns about Bill C-11, several of the recommendations presented below would ensure legislative harmony with the CPPA in key areas and make critical changes to BC PIPA.

In addition to Bill C-11, significant changes have taken place in the past year in the way we live and work as a result of COVID-19. These changes highlight just how crucial it is to update BC's personal information protections to safeguard individuals' privacy and protect the rights of British Columbians.

We hope that this additional information, along with our submission to the Special Committee last year assist you in recommending much needed changes to BC PIPA.

---

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

[2] Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts, 2nd Sess, 43rd Parl, 2020, (First Reading 17 Nov 2020) [Bill C-11].

1. Privacy as a Human Right

Privacy *is* a fundamental human right, and it should be recognized as such. As Justices Abella and Cromwell wrote in *Alberta (IPC) v. United Food and Commercial Workers*, "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."[3] Recognizing privacy as a fundamental human right is consistent with multiple Supreme Court of Canada decisions that have engaged and affirmed privacy rights.[4]

An increasing number of voices are calling for privacy legislation to recognize privacy as a human right. In recent remarks, Canada's Privacy Commissioner, Daniel Therrien stated:

Because data-driven technologies have been shown to be harmful to privacy and other rights, I think the starting point to law reform should be to give privacy laws a right-based foundation.

A central purpose of the law should be to protect privacy as a human right in and of itself, and as an essential element to the realization and protection of other human rights.[5]

In a world where almost all aspects of life are impacted by data collection on an increasingly large scale, Theresa Scassa (Canada Research Chair in Information Law and Policy), calls for a paradigm shift that "reframes privacy as a human right, rather than as a trade-off in the race to innovate or to carry out business in Canada."[6]

Such a shift is already taking place in the European context. For example, the EU has expressly infused its legislation with a human-rights approach. Recital 2 of the

---

[3] *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 [emphasis original].
[4] See e.g., *R v Spencer,* 2014 SCC 43*; R v Jones* 2017 SCC 60.
[5] Office of the Privacy Commissioner of Canada, "A Data Privacy Day Conversation with Canada's Privacy Commissioner: Remarks at the University of Ottawa's Centre for Law, Technology and Society" (28 January 2020), online: <www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200128/>.
[6] Theresa Scassa, "A Human Rights-Based Approach to Data Protection in Canada" (5 June 2020) in Dubois, E and Martin-Bariteau, F, eds, *Citizenship in a Connected Canada: A Research and Policy Agenda* (Ottawa: University of Ottawa Press, 2020).

General Data Protection Regulation (GDPR) states that "the principles of and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, including their right to the protection of personal data."[7]

BC PIPA should be grounded in a human rights-based approach. Such an approach would clarify the fundamental obligations that an organization has with respect to an individual's information, while also directing the Act's provisions to be interpreted in a manner that respects the right to privacy. It would also encourage businesses to always handle personal information in a way that is consistent with this human right, even where their legal obligations may be unclear.

FIPA and BCCLA recommend expanding section 2 of PIPA to specify that one of the purposes of the act is to respect the fundamental right to privacy and the protection of personal information.

Recommendation 1:

Recognize privacy as a fundamental human right and adopt a human rights-based approach within PIPA. Amend the purpose statement in the Act to state that its primary purpose is to respect the fundamental right to privacy by putting in place protections for personal information.

[7] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*), [2016] OJ, L 119, online: <https://gdpr-info.eu/>.

2. Enhanced Privacy Commissioner Powers

It is an unfortunate necessity that strong enforcement measures are needed to ensure compliance with privacy legislation. In its current form, PIPA does not contain adequate tools to ensure compliance with its requirements. It also falls below the standard set by Bill C-11.

FIPA and BCCLA continue to advocate for enhanced Information and Privacy Commissioner powers to provide the BC Commissioner with more tools for enforcement. We recommend that the Commissioner have primary fine-making authority. Allowing the Commissioner to impose sanctions on the worst offenders is a much-needed deterrent that will help improve compliance with the Act.

In order to address repeat offenders, we recommend the Commissioner be empowered to impose increasingly large penalties for subsequent offences. We also recommend that the Commissioner be empowered to publicly document organizations that repeatedly fail to meet privacy requirements.

Regarding the administration of monetary penalties, we recommend that the Commissioner have the authority to directly impose fines. The Commissioner has extensive experience administering monetary penalties and any fines imposed would be subject to judicial oversight.

We agree with the conclusions of the Commissioner that it is not necessary to establish a new administrative tribunal to carry out this function in BC (as is proposed in the CPPA).8 A new tribunal would complicate BC's privacy regime, adding unnecessary costs and delays, when its functions could be fulfilled by the Commissioner.

Recommendation 2:

Enhance the BC Information and Privacy Commissioner's enforcement capabilities by giving the Commissioner primary fine-making authority. Allow the Commissioner to impose increasingly severe penalties for and publicly document repeat offenders.

---

[8] Office of the Information and Privacy Commissioner of British Columbia, *Supplemental Submission to the Special Committee to Review the Personal Information Protection Act*, (23 February 2021), online: <https://www.oipc.bc.ca/special-reports/3513>.

3. Law Enforcement

FIPA and BCCLA have major concerns about the provisions contained in PIPA and the proposed CPPA that allow for the disclosure of personal information by private entities to government and law enforcement, without the necessary prior authorization of the individual. Due to the immense power that the state has over individuals – particularly in relation to criminal investigations that can ultimately lead to severe restrictions of human rights and freedoms – we maintain that absent individual consent, the only time that public entities should be able to compel a private entity to share personal information is to comply with a warrant or subpoena issued by a court.

We pointed to the problematic nature of public and private partnerships in last year's submission because legislative gaps and inconsistencies enable privacy protections to be downgraded or circumvented altogether.[9] Our alarm has only grown since then, considering the findings of privacy commissioner investigations into Clearview AI facial recognition technology and its use by police agencies here in BC and across Canada. The Clearview AI scandal highlights the dangerous and growing tension between consent-based privacy rights for individuals, and existing and emerging mechanisms for governments to surreptitiously gather information about citizens from private third parties, such as social media behemoths like Facebook.

As it is currently drafted, the CPPA is constitutionally contentious because it allows law enforcement to request privately held personal information absent prior judicial authorization based on reasonable and probable grounds. CPPA replicates (and possibly expands) legal provisions that enable the government to seek disclosure of personal information from companies on a massive scale which has the potential to adversely impact human rights and freedoms. PIPA's s. 18(1)(c) and (j) reflect these mechanisms, though are slightly narrower in scope. These mechanisms allow for personal information to be shared without the express consent of the individual from whom it was collected – and without explicitly requiring prior authorization. Unless the personal information is such that the individual would have no reasonable expectation of privacy, such disclosures

[9] ***Supra*** **note 1.**

violate sections 710 and 811 of the Canadian Charter of Rights and Freedoms and do not constitute reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

The recent investigations into the use of facial recognition software provided by Clearview AI – a private corporation – to public policing agencies in British Columbia and across the nation highlight the significant human rights at stake when corporations share personal information with law enforcement agencies. They also reveal the inadequacy of privacy protections provided by PIPA and PIPEDA, and those proposed in CPPA. In February 2021, four privacy commissioners – including British Columbia's – released an unequivocal report on the illegal practices of Clearview AI and how 48 law enforcement agencies ran thousands of searches using Clearview AI's facial recognition software database.[12]

We also draw your attention to the Office of the Privacy Commissioner of Canada's subsequent rejection of the argument that the RCMP's use of Clearview AI is authorized by virtue of being related to an operating program or activity of the RCMP.[13]

In April 2021, the Vancouver Police Department disclosed to their board – pursuant to a policy complaint – that an officer had used the facial recognition technology

---

[10] For example, see *Cheskes v. Ontario (Attorney General)*, 2007 CanLII 38387 (ONSC), which held that "the individual's ability to control the dissemination of personal information is an element of the right to privacy" protected under s. 7 of the *Charter* (at para 62). Various provisions in Ontario's *Vital Statistics Act* were held invalid because they allowed the Ontario government to disclose an individual's personal information without their consent, in violation of the s. 7 right to liberty.

[11] 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".

[12] Office of the Privacy Commissioner of Canada, the Commission d'access a l'information du Quebec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, *Joint Investigation of Clearview AI, Inc.,* PIPEDA Report of Findings #2021-001 (2 February 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

[13] Office of the Privacy Commissioner of Canada, "Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology" (June 10, 2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc4-1> at paras 21-32. [*OPC Clearview AI Report*]

despite no formal approval or policy having been made about the technology.[14] While the Vancouver Police Department claims that the one search was done in the context of an investigation, we cannot verify this and note that the police department has stopped using the software in the face of public scrutiny.

These examples underscore that law enforcement agencies cannot always be trusted to work within their legal mandates, and that a third-party decision maker should always be involved where law enforcement seek access to information over which a person has a reasonable expectation of privacy.

BC PIPA should be amended to ensure that companies can only share personal information in their possession with a government institution and/or law enforcement if the individual from whom the information was collected has consented to the disclosure, or the disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of personal information.

Recommendation 3:

Amend BC PIPA to add a strict prohibition on private entities from disclosing any personal information that they have collected from individuals to law enforcement bodies unless one of the following applies:

(a) exigent circumstances exist,

(b) the individual about whom the information is about has clearly consented to the private entity sharing the information with law enforcement (as a safeguard, the request for consent from the individual must be in plain language to best ensure they understand the agreement),

(c) judicial authorization has been granted to law enforcement to collect the personal information about an individual from the third-party company.

---

[14] Service or Policy Complaint #2021-001 Response to Facial Recognition Report (Vancouver: Vancouver Police Department, 2021), online: Vancouver Police Board <vancouverpoliceboard.ca/police/policeboard/agenda/2021/0415/SP-5-2-2104C03-SP-Complaint-FacialRecognition.pdf>.

4. Notification obligations for organizations suffering data breaches

Our initial submission included a recommendation that BC introduce a mandatory breach notification provision, requiring organizations to notify the Office of the Information and Privacy Commissioner when they experience data breaches.

Section 58 of the CPPA requires an organization to report breaches of personal information to the Privacy Commissioner and the individual whose information was compromised. Specifically, the CPPA states:

> **58 (1) An organization must report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.**
>
> **(2) The report must contain the prescribed information and must be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.**
>
> **(3) Unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.**

Given the inclusion of this section in the CPPA, we reiterate our recommendation that PIPA be amended to require organizations to notify the Office of the Information and Privacy Commissioner of breaches of personal information. Such an amendment would ensure that BC is no longer a major outlier as one of only two jurisdictions in all of North America without a mandatory breach notification provision for private sector organizations.[15]

---

[15] The other jurisdiction without a mandatory breach notification requirement is Quebec. Quebec is in the process or introducing Bill 64 to modernize the province's privacy legislation. The bill includes an amendment to Quebec's private sector privacy act to include a breach notification provision. Once enacted, this will leave BC as the *only* jurisdiction in North America without such a provision.

Recommendation 4:

Amend PIPA to require organizations to report personal information breaches to the BC Privacy Commissioner where there is a "real risk of significant harm to an individual." The Commissioner should be granted the authority to require an organization to notify the affected individuals where necessary.

5. Algorithmic Transparency and Accountability

As organizations increasingly rely on artificial intelligence (AI) to make decisions, there is growing concern about a lack of transparency and biases that may be built into those decisions.

Artificial intelligence systems are currently used by private companies to evaluate individuals' creditworthiness, assess their security risk, and analyze resumes during hiring processes.[16] Individuals may be unaware that AI was involved in making decisions that impact them or have no concept of the factors considered by the AI systems to arrive at their decisions. They may have concerns that there were racial, gender or other biases built into the algorithms making decisions about them that led to unfair outcomes.

Algorithmic decision-making systems can reflect and reinforce existing societal biases.[17] In one example, women were systematically discriminated against in hiring decisions for management positions at a company because the data used to train the algorithm was drawn from resumes of managers hired over the previous decade (who were primarily white and male).[18] Further, the analytical processes used by algorithms can be so complex that it is impossible for humans to understand the specifics of how they arrived at a decision – so it may be difficult to detect biases.[19]

Bill C-11 attempts to address the issues created by the use of automatic decision-making systems by requiring that organizations using such systems must:

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

---

[16] Electronic Privacy Information Center, "AI and Human Rights," online: <https://epic.org/ai/>.
[17] 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*].
[18] 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/>.
[19] *Transparency International*, *supra* note17.

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.

Articles 21 and 22 of the GDPR set a much higher standard.[20] The GDPR allows individuals the right to refuse to be subject to a decision based solely on automatic processing, subject to certain narrow exceptions. Our position is that PIPA should be amended to:

1. **Require companies to notify individuals whenever they will be subject to an automated decision-making system.**
2. **Require companies using automated decision-making processes to provide customers with an explanation of how automated processing was used, the criteria that were followed and reasons for the decision that was made. This explanation should be provided without customers having to request it.**
3. **Give individuals the right to object to a decision that was made by an automated decision-making system by submitting complaints to an individual at the company with the authority to review and change a company's decision.**
4. **Give individuals the right to object to the use of AI systems to make decisions about them (subject to limited exceptions).**

Finally, we have significant concerns regarding the use of automated decision-making systems where biometric data is involved. This includes the use of facial recognition software or personal health information from smart devices. The use of such information is highly intrusive on individuals' privacy.[21] In order to protect individuals against such intrusive practices, article 9 of the GDPR prohibits the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

---

[20] ***General Data Protection Regulation***, ***supra*** **note 7.**

[21] ***OPC Clearview AI*** **Report, *supra* note 12, For example, Clearview AI unlawfully scraped public websites to amass a database of over three billion images of faces and biometric identifiers, including children and a vast number of Canadians. They then used the biometric data for inappropriate purposes that were unrelated to the purposes for which the images were posted.**

Within the context of automatic decision-making processes, we believe that if any form of biometric data is to be used in AI systems, this should require the explicit consent of the individual whose data is being used, and the ability to easily opt out at any time after consent has been given.

Recommendation 5:

Where an organization makes use of automated decision-making systems, require that they disclose this fact to customers and provide customers with an explanation of the criteria used by the system and the reasons for the decision about the individual customer. In addition, customers should have the ability to object to a decision that was made or to opt out of the use of an automated decision-making system altogether.

6. De-Identification

In our initial submission, we stressed the need for BC privacy legislation to incorporate a clear and context-driven definition for de-identified information. An express definition, grounded in a risk-based approach, recognizes the increasingly sophisticated means through which individuals may be re-identified from de-identified data sets. In conjunction with this approach, we also stressed the need to implement proportionate safeguards, standards, and transparency requirements regarding the creation, collection, use, and disclosure of de-identified data sets. These amendments, while maintaining technological neutrality, should aim to promote certainty around assessments of de-identification methods and disclosures of de-identified data sets to third parties.

Harmony between BC and federal privacy legislation is important. However, we encourage the Committee to consider a BC-led approach that accounts for the shortcomings within proposed federal legislation and recognizes the uneven efforts across the country to bring de-identified information within the scope of modern privacy legislation. The proposed CPPA, for example, addresses the risk of re-identification through direct and indirect identifiers by adopting a "reasonably foreseeable" standard.[22]

This language, seemingly imported from Ontario's *Personal Health Information Protection Act,*[23] not only departs from the existing PIPEDA standard of "serious possibility" most recently followed by the federal privacy commissioner in its Cadillac Fairview investigation,[24] it has also not been judicially considered outside of the health information context. The proposed CPPA definition also stands in contrast to the reasonable expectation standard, which *has* been considered judicially.[25] Further, former BC Privacy Commissioner Elizabeth Denham has

---

[22] ***Bill C-11, supra*** **note 2, *s* 2.**
[23] ***Personal Health Information Protection Act, 2004*****, SO 2004, c 3, Sched. A, [*****PHIPA*****].**
[24] **Privacy Commissioner of Canada, Information and Privacy Commissioner of Alberta, Information and Privacy Commissioner for British Columbia, *Joint investigation of the Cadillac Fairview Corporation Limited*, PIPEDA Report of Findings #2020-004 (28 October 2020), at para 143.**
[25] **See *Ontario (Attorney General) v. Pascoe*, 2001 CanLII 32755 (ON SCDC) at para 15; *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII) at para 43.**

affirmed that BC investigative reports and orders have followed the reasonable expectation approach.[26]

Quebec's Bill 64 distinguishes between de-identified and anonymized information by protecting against direct identification in the former, and direct and indirect identification in the latter.[27] In a similar vein, the EU's GDPR subjects "pseudonymous" information to its data protections, and excludes anonymous information from its scope.[28] Nevertheless, at the Canadian federal level, calls to promote clarity by avoiding any reference to anonymity have apparently been heeded in the proposed CPPA.[29]

These varying approaches reflect lingering questions about whether de-identified information should attract the same protections as personal information, or whether it is a distinct category worthy of additional safeguards. In light of this unsettled landscape, we invite the Committee to consider and set a clear standard most appropriate to the BC context.

We maintain that the core analysis for de-identified data sets should remain contextually driven. Consistent with the CPPA, a risk-based approach recognizes narrow circumstances in which de-identified information may be collected and used for internal R&D purposes or disclosed to public institutions for socially beneficial purposes.[30] These permissible situations, however, must also be accompanied by a strong prohibition against re-identification.[31] Recognizing that the risk of re-identification cannot be completely eliminated, we note that a legislative prohibition –coupled with robust penalties and safeguards restricting the transfer of de-identified information to specified third-parties – will disincentivize re-identification efforts and ensure that organizations apply the

---

[26] Elizabeth Denham, "Updated guidance on the storage of information outside of Canada by public bodies" (16 June 2014) at 3, online at <https://www.oipc.bc.ca/public-comments/1649>, referring to Order P12-01, 2012 BCIPC No 25 at para 82. See also discussion of the "mosaic effect" by former BC Commissioner David Loukidelis in Order 01-01, [2001] BCIPCD No 1.

[27] Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Leg, Quebec, 2020, online: <http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html>.

[28] *General Data Protection Regulation*, *supra* note 7, Recital 26.

[29] *Canadian Anonymization Network*, "States of Data" (October 2020), online at <https://deidentify.ca/wp-content/uploads/2020/10/CANON-States-of-Data-One-Pager.pdf>.

[30] Bill C-11 *supra* note 2, ss 20, 21, 39.

[31] *Ibid*, s 75, organizations are prohibited from re-identifying an individual except to test security safeguards.

legislative provisions and innovative methods needed to protect de-identified data sets.

Finally, amended legislation must ensure that organizations are transparent about their use of de-identification techniques and data sets at a level that does not subject individuals to an increased risk of re-identification.

Recommendation 6:

BC PIPA should include a clear definition for de-identified information, or the process of de-identification, that is appropriate for the BC context. A contextual approach that recognizes permissible uses and disclosures of de-identified information must also be coupled with an express prohibition against re-identification. It should also specify safeguards to protect against third-party disclosures and ensure that organizations are transparent about their use of de-identification techniques and de-identified data sets.

7. Inter-provincial & International Transfers

Recent high-profile investigations, including those into Cambridge Analytica and Clearview AI, demonstrate how easily and frequently information flows across borders. These have highlighted the need for organizations, regardless of their size, to identify and disclose their transfers of data that cross provincial and international borders.

The CPPA expressly recognizes that data is constantly flowing across borders and geographical boundaries [s.5]. Taken together, CPPA sections 6 and 62(2)(d) clarify an organization's obligations with respect to cross-border data flows. Section 62 in particular, requires an organization to disclose whether they carry out any international or interprovincial transfer or disclosures that may have reasonably foreseeable privacy implications.

We continue to advocate for heightened safeguards in BC PIPA as cross-border flows of information become increasingly obscure and complex.

Specifically, we recommend that PIPA be amended to include a provision requiring a privacy impact assessment before information can be released outside of BC to another province or international jurisdiction. We also recommend that the sharing and receiving organizations be required to enter into a contractual agreement that personal information will be protected to at least the standard required by PIPA. This could be modeled after s.70.1 of Quebec's *Act respecting Access to documents held by public bodies and the protection of personal information,* which requires the following:

> **Before releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf, a public body must ensure that the information receives protection equivalent to that afforded under this Act.**
>
> **If the public body considers that the information referred to in the first paragraph will not receive protection equivalent to that afforded under this Act, it must refuse to release the information or refuse to entrust a person or a body outside Québec with the task of holding, using or releasing it on its behalf.[32]**

---

[32] ***Act respecting Access to documents held by public bodies and the protection of personal information*, CQLR c A-2.1, s 70.1.**

Recommendation 7:

Require organizations to conduct a privacy impact assessment prior to transferring data to another province or international jurisdiction, to ensure that privacy protections in the receiving jurisdiction are at least equivalent to those in BC. Require sharing and receiving organizations to enter into contractual agreements that ensure personal information is protected to at least the standard required by PIPA.

8. Plain Language

Our submission discussed the fact that the average privacy policy that individuals encounter is legalistic and difficult to understand. We highlighted research showing that it would take an individual 200 hours to read the privacy policies for all of the websites that the average internet user visits in a year.[33] It is obviously unrealistic to require this of the average individual – when they agree to dense and opaque privacy polices without understanding them, this does not constitute meaningful consent.

In light of this context, reform is critically needed to require organizations to provide plain language notice about the collection, use or disclosure of personal information in order for consent to be valid.

The CCPA includes new plain language requirements. Bill C-11 states that:

> **15 (3) The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, it provides the individual with the following information in plain language:[34]**
>
> - **the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4);**
> - **the way in which the personal information is to be collected, used or disclosed;**
> - **any reasonably foreseeable consequences of the collection, use or disclosure of the personal information;**
> - **the specific type of personal information that is to be collected, used or disclosed; and**
> - **the names of any third parties or types of third parties to which the organization may disclose the personal information. [s. 15(3)].**
>
> **62 (1) An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfil its obligations under this Act.**
>
> **66 (1) The information referred to in section 63 must be provided to the individual in plain language.**

---

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

[34] Bill C-11, *supra* note 2, (emphasis added).

Consistent with Bill C-11, BC PIPA should be amended to explicitly require organizations to present individuals with privacy policies written in a plain, understandable manner. It should also explicitly require organizations to provide individuals information regarding the purpose of collection, use, and disclosure of their personal information in plain language, similar to section 15(3) of Bill C-11.

The Office of the Information and Privacy Commissioner would be well placed to develop guidance materials for organizations on drafting plain language privacy policies in a way that is easy for the average individual to understand.[35]

In addition, where an organization provides individuals with information relating to automated decision-making (See recommendation 3 above), that information must also be provided to the individual in plain language. Such a requirement would be consistent with section 66(1) of C-11.

Recommendation 8:

Amend PIPA to include plain language requirements for organizations subject to the act to provide access to privacy policies in a plain, understandable manner, including information on the collection, use and disclosure of any personal information, and the use of automated decision-making.

[35] The OIPC produces excellent guidance documents on a variety of privacy-related topics, available online: <https://www.oipc.bc.ca/resources/guidance-documents>.

9. Optional "Codes of Practice" and "Certification Programs"

Firm or sector-specific codes of practice and certification programs may be an effective tool for private sector organizations to meet their legal obligations with respect to the protection of privacy, while adapting practices to their own specific operations.

CPPA provides organizations with the option to enact codes of practice.[36] Organizations would have the ability to apply to the Privacy Commissioner for a declaration that their firm-specific codes of practice provide equal or greater protection of personal information covered under the CPPA.

This is an innovative solution that places accountability on an organization yet provides them with enough flexibility to implement codes/programs in a manner that suits their needs. It also allows for smaller organizations with limited administrative capacity to work with sector organizations to develop a sector-specific policy.

BC PIPA should provide organizations or sectors with a similar option, allowing them to apply to the BC Information and Privacy Commissioner for approval of firm or sector-specific codes and programs. However, it should also include a requirement that these codes and programs remain up to date (i.e., require them to be updated and re-approved on a regular basis). This will ensure that they conform with evolving standards.

Recommendation 9:

Amend PIPA to allow organizations or sectors to develop privacy codes of practice or certification programs on a voluntary basis that are adapted to their specific business practices. Require that the codes be approved by the Information and Privacy Commissioner and updated and reapproved at regular intervals to ensure they conform with evolving standards.

---

[36] Bill C-11, *supra* note 2, ss 76(1), 77(1).

Conclusion

FIPA and BCCLA stress the crucial importance of updating BC's privacy legislation to meet current challenges and better reflect the reality of modern technologies. The recommendations that we made through our initial submission in July 2020, along with these additional recommendations would make key legislative changes that are needed to achieve this goal.

The people of BC expect and have a right to better protection of their personal information. Urgent action is needed to ensure PIPA protects British Columbians' rights, create transparency in the use of their personal information and restore trust in the province's privacy framework.

We look forward to reviewing your recommendations and are available for further consultation, should you have any questions.

Summary of Recommendations

1. **Recognize privacy as a fundamental human right and adopt a human rights-based approach within PIPA. Amend the purpose statement in the act to state that its primary purpose is to respect the fundamental right to privacy by putting in place protections for personal information.**

2. **Enhance the Privacy Commissioner's enforcement capabilities by giving the Commissioner primary fine-making authority. Allow the Commissioner to impose increasingly severe penalties for and publicly document repeat offenders.**

3. **Amend BC PIPA to add a strict prohibition on private entities from disclosing any personal information that they have collected from individuals to law enforcement bodies unless one of the following applies:**

    a. **exigent circumstances exist,**

    b. **the individual about whom the information is about has clearly consented to the private entity sharing the information with law enforcement (as a safeguard, the request for consent from the individual must be in plain language to best ensure they understand the agreement),**

    c. **judicial authorization has been granted to law enforcement to collect the personal information about an individual from the third-party company.**

4. **Amend PIPA to require organizations to report personal information breaches to the BC Privacy Commissioner where there is a "real risk of significant harm to an individual." The Commissioner should be granted the authority to require an organization to notify the affected individuals where necessary.**

5. **Amend PIPA to require any organization using an automated decision-making system to notify individuals that such a system is in use and provide them with an explanation of how decisions about them were made. This should include the factors considered in arriving at the decision and the weight applied to each factor.**

6. **BC PIPA should include a clear definition for de-identified information, or the process of de-identification, that is appropriate for the BC context. A contextual approach that recognizes permissible uses and disclosures of de-identified information must also be coupled with an express prohibition against re-identification. It should also specify safeguards to protect against third-party disclosures and ensure that organizations are transparent about their use of de-identification techniques and de-identified data sets.**

7. **Require organizations to conduct a privacy impact assessment prior to transferring data to another province or international jurisdiction, to ensure that privacy protections in the receiving jurisdiction are at least equivalent to those in BC. Require sharing and receiving organizations to enter into contractual agreements that ensure personal information is protected to at least the standard required by PIPA.**

8. **Amend PIPA to include plain language requirements for organizations subject to the act to provide access to privacy policies in a plain, understandable manner, including information on the collection, use and disclosure of any personal information and the use of automated decision-making.**

9. **Amend PIPA to allow sectors or organizations to develop optional privacy codes of practice or certification programs (mirroring provisions in the CPPA), with the approval of the Commissioner. Create a requirement that they be updated every two years to ensure they conform with evolving standards.**