August 14, 2020

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

BC Freedom of Information and Privacy Association

BC Civil Liberties Association

Special Committee to Review the Personal Information Protection Act

c/o Parliamentary Committees Office
Room 224, Parliament Buildings
Victoria, BC V8V 1X4
Canada

Dear Members of the Special Committee,

Re: Submission from the perspective of advocacy organizations

The BC Freedom of Information and Privacy Association and the BC Civil Liberties Association make this joint submission in response to the Committee's invitation to provide input on the effectiveness of the *Personal Information Protection Act* in its current form.

We hope that our submission will be of assistance during the Committee's deliberations.

Attached:

- FIPA oral submissions to Committee on June 9, 2020
- BCCLA oral submission to Committee on June 16, 2020

Also available[1]:

- BC FIPA 2008 and 2014 submissions to respective Committee
- BCCLA 2008 and 2014 submissions to respective Committee

[1] Through the Legislative Assembly of British Columbia's parliamentary committees > committee transcripts and audio > committee documents.

Introduction

The BC Freedom of Information and Privacy Association (BC FIPA) is a non-profit advocacy organization established in 1991 for the purpose of advancing freedom of information, transparency, and privacy in British Columbia and Canada. Our work predates both the *Freedom of Information and Privacy Protection Act* (FOIPPA)[2] and the *Personal Information and Protection Act* (PIPA)[3].

The BC Civil Liberties Association (BCCLA) is the oldest and most active civil liberties and human rights group in Canada. The BCCLA has been actively advancing human rights and civil liberties through litigation, law reform, community-based legal advocacy, and public engagement and education for the last half century. We recognize that such rights are inalienable and necessary for the flourishing of individuals and human society.

We are excited for the opportunity to contribute to the reform of a piece of legislation that is increasingly relevant in today's digital age. This legislative review offers British Columbia the opportunity to regain leadership in its privacy protection laws and amend PIPA to offer its citizens the protections they expect and deserve.

PIPA provides a principle- and consent-based framework with clear legal rights and obligations of individuals and organizations. While it lays out a strong foundation for privacy legislation, it requires substantive amendments to keep pace with the growing requirements of increased privacy protections. In an era of digitalization, privacy is too often treated as an afterthought. Compared to other provincial and the federal privacy legislation, since its enactment in 2003, PIPA has undergone zero substantive[4] amendments. The government inaction is not reflective of the public's expectations and the recommendations from both the members of the assembly and all-party special committees, all of which have clear consensus on the need for legislative reform.

[2] *Freedom of Information and Protection of Privacy Act*, RSBC 1996*, c. 165*. ("FOIPPA")
[3] *The Personal information Protection Act,* SBC 2003, c 63. ("PIPA")
[4] Our analysis of substantive amendments excluded amendments that did not significantly alter the meaning of the provision (e.g. grammatical changes, section renumbering, etc.)

Public consultation is a vital aspect of the legislative process, and we make this submission with hope that the much-needed changes will occur this time around.

Our Work

To inform our submission, we analyzed provincial, federal, and international privacy legislation for content, amendments, and committee recommendations. We also consulted with several stakeholder groups to better understand the gaps that we identified in the relevant areas. In addition, we analyzed various survey results, and BC FIPA conducted its own public opinion survey to inform these recommendations.

The Research

2018-19 Survey of Canadians on Privacy[5]

The 2018-19 Survey of Canadians on Privacy conducted by the Office of the Privacy Commissioner highlights the concerns of Canadians in relation to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[6]. These concerns are also relevant to PIPA, and we address them throughout our submission. The survey indicates that 67% of Canadians feel little to no control over how their personal information is being used by companies they do business with, and only 38% of Canadians felt that businesses in general respect their privacy rights. The remaining relevant statistics are summarized in the table below.

[5] Office of the Privacy Commissioner of Canada, "2018-19 Survey of Canadians on Privacy", last modified May 9, 2019, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/ ("OPC 2019 Survey")

[6] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5. ("PIPEDA")

Question	% Canadians
In general, how concerned are you about the protection of your privacy?	92% at least somewhat concerned
How would you rate your knowledge of your privacy rights?	64% at least good
How much control do you feel you have over how your personal information is being used by companies you do business with.	67% feel little to no control
Willingness to do business with the company where a company provides easy to understand information about its privacy practices.	69% more willing
Willingness to do business with the company if under Canadian law, the company would face strict financial penalties, such as large fines, for misusing your personal information.	71% more willing
I feel that businesses in general respect my privacy rights.	38% agreed

BC FIPA's 2020 Survey of British Columbians on Privacy

After reviewing previous surveys, analyzing key legislation, and discussing with our stakeholders, we commissioned an IPSOS poll on BC citizens' opinion regarding BC's private sector privacy laws[7]. The poll results indicate that less than half of British Columbians feel that current laws and practices are sufficient to protect their personal information. Awareness of privacy rights and protections is concerningly low, and British Columbians support increased privacy-related public education. The relevant statistics are summarized in the table below.

[7] BC Freedom of Information and Privacy Association, "British Columbians want action on privacy protection: Polling results.", (June 3, 2020), https://fipa.bc.ca/category/libraries/publications/publication-types/surveys-and-polling/ ("BC FIPA 2020 Survey")

Question	% British Columbians
Existing laws and organizational practices provide sufficient protection of my personal information.	43% agreed
Organizations are open and transparent about how they collect and use my personal information.	33% agreed
How concerned are you about an organization transferring your personal information from BC to organizations outside of Canada?	75% concerned
How important do you consider the following items as components of general public education?	
Resources for individuals regarding personal information and privacy rights	88% think it's important
Resources for individuals learning about how to protect their personal information	87% think it's important
Resources for individuals on obtaining help, information, and advice related to privacy	87% think it's important
Targeted curriculum for K-12 schools relating to privacy rights	75% think it's important
Targeted curriculum for post-secondary schools relating to privacy rights	77% think it's important
Choose the statements that best reflect your knowledge of your privacy rights	
I am aware of BC's *Personal Information Protection Act*	32%
I am aware of BC's Information and Privacy Commissioner	31%
I am aware that I can request access to my personal information from businesses	33%
I am aware of the right to file a complaint relating to the handling of my personal information	40%
None of these	33%

Why Amend PIPA?

PIPA must be amended because its privacy protections are inadequate based on its own stated objectives and in comparison to other jurisdictions (federal, provincial, and international). In addition, public opinion surveys indicate that the public expects increased privacy protections and education, and BC businesses face a real economic risk in light of global privacy standards.

Federal: *Maintain 'Substantially Similar' Designation with PIPEDA*

PIPA is currently designated as 'substantially similar'[8] to the federal PIPEDA. However, the current differences between PIPA and PIPEDA question that designation. Specifically, PIPEDA has a mandatory breach reporting provision and enhanced protections during data transfers, while PIPA has neither. In addition, discussions to modernize PIPEDA to provide enhanced privacy protections are currently in order[9], which may further increase the gap between the two pieces of legislation.

Provincial: *Québec's Enhanced Personal Information Protections – Bill 64*

In June of 2020, the Québec Government introduced Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*[10]. Bill 64 proposes several changes to strengthen the privacy protections afforded by Québec's *Act respecting the protection of personal information in the private sector*[11]. Of note are the following changes:

- data breach reporting and recordkeeping requirements;
- administrative monetary penalties for non-compliance;
- separate consent for each purpose of collection, where purpose is communicated in clear and simple language;

[8] Office of the Privacy Commissioner of Canada, "Provincial laws that may apply instead of PIPEDA", (May 2020), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/

[9] Innovation, Science and Economic Development Canada, "Strengthening Privacy for the Digital Age: Proposals to modernize the Personal Information Protection and Electronic Documents Act", last modified May 21, 2019, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html ("ISEDC")

[10] Bill 64, "*An Act to modernize legislative provisions as regards the protection of personal information",* 1st sess., 42nd Legislature, (June 12, 2020), http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html

[11] *Act Respecting the Protection of Personal Information in the Private Sector*, CQRL, c P-39.1 ("Private Sector Act")

- enhanced adequacy requirements for outsourcing and transfers outside of Québec;
- right to data portability and right to be forgotten;
- algorithmic transparency;
- the right to be informed and to object to automatic processing including the right to be provided with information regarding the personal information used, the reasons, factors, and parameters used;
- the right to have one's personal information corrected; and
- mandatory privacy impact assessments.

With Québec moving towards a privacy protection regime that offers increased personal information protection and rights to its citizens, BC is falling further behind relative to its provincial counterparts.

International: *Maintain 'Adequacy Status' With the GDPR*

The *General Data Protection Regulation* (GDPR)[12] from the European Union (EU) has become the *de facto* global standard for data protection because it is modern, progressive, and takes a human rights-based approach to privacy. Though the GDPR is not perfect, it provides a strong framework for the BC Legislature to work with. We make references to the GDPR in our submission where we believe that the GDPR provides strong principles that BC's PIPA can benefit from. However, these references do not imply that BC's PIPA should mirror the GDPR. The differences in BC's business practices and public expectations compared to the EU necessitates that a personalized approach be taken for privacy protection in the province.

To transfer information outside the EU, jurisdictions with laws that are comparable to the GDPR can apply to the European Commission for "adequacy status". Canada's adequacy status with the GDPR expired May 25, 2020 and is currently under review. However, adequacy is not just a national consideration. Québec sought adequacy from the European Commission in 2014, which

[12] *General Data Protection Regulation,* 2016/679 ("GDPR")

is delayed until it makes the necessary amendments to its Private Sector Act.[13] The Working Party's recommendations for amendments to Québec's Private Sector Act centered around several areas of the legislation including clarification of the scope of the act, an obligation on organizations to inform data subjects of the identity and contact details of the data controller, a limitation on the circumstances for withholding information, a definition of "sensitive information", and a requirement that an organization use contractual or other binding provisions with third parties to ensure a comparable level of data protection in information transfers. Québec's newly proposed Bill 64, as discussed above, addresses some of these recommendations.

There is a chance that BC, either by itself or in conjunction with other provinces, may also be subject to an adequacy assessment. Therefore, the discrepancies between PIPA and the GDPR must be addressed. To name a few, compared to the GDPR, PIPA has no mandatory breach notification requirement, and has inadequate provisions concerning international data transfers and the Commissioner's powers. While our recommendations in the aforementioned areas are supported on their own merits as components of a modern privacy framework, the GDPR adequacy status concern introduces an additional trade-related incentive to reform PIPA.

As the GDPR imposes highly stringent data protection requirements for transfer of personal information to countries without adequacy status, a non-adequacy assessment with the GDPR could have "far ranging implications for Canada's trade relationship with the EU"[14] says Privacy Commissioner Daniel Therrien. For example, organizations without an adequacy status are typically required to have "standard data protection clauses, binding corporate rules, approved codes of conduct, or certification"[15] when transferring personal information from the EU.

[13] Data Protection Working Party, "Opinion 7/2014 on the protection of personal data in Quebec", s 29, (June 4, 2014), https://www.dataprotection.ro/servlet/ViewDocument?id=1087

[14] Privacy Commissioner of Canada to Standing Committee on Access to Information, Privacy and Ethics, (December 2, 2016), https://www.ourcommons.ca/Content/Committee/421/ETHI/Brief/BR8668703/br-external/OfficeofthePrivacyCommissionerofCanada-e.pdf ("OPC Letter to ETHI")

[15] Office of the Information & Privacy Commissioner of British Columbia, Guidance Document "Competitive Advantage: Compliance with PIPA and the GDPR", (March 2018), https://www.oipc.bc.ca/guidance-documents/2135. ("OIPC Guidance Doc 2135")

On a global scale, a non-adequacy assessment has the potential to limit trade with other countries which are considered adequacy-equivalent with the GDPR. For example, Japan obtained adequacy-status with the GDPR in 2019[16], and has now implemented a similar adequacy requirement in its privacy legislation. If Canada isn't recognized as being adequate with the GDPR, by extension, it may also not be recognized as being adequate with Japan. For BC businesses, this may have negative economic effects as the exchange of information will be strictly regulated between both the EU and Asia-Pacific. Dr. Colin Bennett addresses this in detail in his submission.[17]

In short, with several substantive differences between the GDPR and PIPA in its current form, the BC government must amend PIPA to ensure that BC businesses can maintain their free-flowing international trade relationships.

Recommendations for Amendments to PIPA

Due to government inaction on our prior recommendations and their continuing necessity, our previous recommendations remain relevant today. Attached, you will find our oral submissions to this Committee. Our 2008 and 2014 submissions are available upon request, as well as part of the official Hansard of the 2008 and 2014 Committees, respectively. In our current submission, we propose new, and repeat some old, recommendations.

Mandatory Breach Notification Requirement

Since November 2018, PIPEDA requires federally regulated organizations to report personal information breaches to the Privacy Commissioner.[18] Alberta's PIPA[19] and the GDPR[20] also contain a mandatory breach notification provision.

[16] The European Commission, "Commission Implementing Decision (EU) 2019/419", *Official Journal of the European Union*, (January 23, 2019): 1–58, http://data.europa.eu/eli/dec_impl/2019/419/oj
[17] Bennett, Colin., Submission to the Special Committee to Review the Personal Information Protection Act, (June 9, 2020), https://www.leg.bc.ca/content/CommitteeDocuments/41st-parliament/5th-session/pipa/2020_06_09_Bennett_Colin_Presentation.pdf
[18] PIPEDA, *supra* note 6, s 10.1
[19] *Personal Information Protection Act*, SA 2003, c P-6.5, s 34.1 ("Alberta's PIPA")
[20] GDPR, *supra* note 12, article 33

Québec and British Columbia are the only two jurisdictions in North America without a mandatory breach reporting provision. Québec's Bill 64 has proposed to amend Québec's Private Sector Act to include a mandatory breach notification. If the bill is passed, BC will stand alone as the only North American jurisdiction without a mandatory breach reporting provision.

There are several reasons why a mandatory breach reporting provision is beneficial. First, the requirement will "benefit the citizens of British Columbia by enhancing accountability and transparency, and helping to mitigate the fallouts of a privacy breach."[21] Mandatory breach reporting serves as an accountability mechanism by ensuring that an organization's data protection practices, as well as their effectiveness, are both a matter of public record. In fact, public accountability may lead to organizations investing more into security safeguards for the protection of personal information. As UK's Information Commissioner Elizabeth Denham stated in her oral presentation to this committee, when a mandatory breach notification came into effect in the UK, organizations invested more into security safeguards for personal information. According to Commissioner Denham, "[i]t took a breach notification regime for boards and company executives to take security, information security, seriously".[22] Second, mandatory breach reporting serves as a mitigation tactic because it allows individuals to take steps to prevent further losses experienced by unauthorized access, such as alerting the applicable external organizations of the breach. Lastly, a mandatory breach reporting provision will harmonize BC's PIPA with other jurisdictions. As several businesses provide services nationally and internationally, harmonization of reporting requirements will help them better understand their legal obligations, which may, in turn, motivate compliance with PIPA.[23]

In addition, the BC Privacy Commissioner should have the power to require organizations to inform individuals affected by the breach where "there is a real risk of significant harm as a result

[21] Privacy Commissioner of Canada, as cited by the Special Committee to Review the Personal Information Protection Act, (2015), https://www.leg.bc.ca/content/CommitteeDocuments/40th-parliament/3rd-session/pipa/reports/PDF/Rpt-PIPA-40-3-Report-2015-FEB-06.pdf ("2015 Special Committee")
[22] Elizabeth Denham's oral presentation to the Special Committee, (June 17, 2020). ("Elizabeth Denham's Presentation")
[23] 2015 Special Committee, *supra* note 21

of the loss or unauthorized access or disclosure."[24] This power would be similar to the Alberta Privacy Commissioner's power under section 37.1(1) of Alberta's PIPA. Setting a threshold prior to informing individuals about a data breach addresses the concerns related to 'breach-fatigue' and 'information overload' that individuals may experience if they were notified of *every* data breach, whether minor or major. The purpose of providing the Commissioner with this power is that in cases where an organization decides that a breach is not significant enough to report to the public, the Commissioner, based on their own analysis, can still require the organization to notify those affected. This is highlighted in the case of Uber's data breach in 2017 where Uber decided against notifying individuals affected by a data breach because it assessed that "the information at issue was not sensitive and not the type that poses a threat of potential harm that rises to the level of significance required for notification…"[25] The Alberta Privacy Commissioner found to the contrary,[26] and pursuant to her powers in Alberta's PIPA, required Uber to inform all Canadians who were affected by the data breach.[27]

Recommendation: PIPA should be amended 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".[28] The Commissioner should be granted the authority to require an organization to notify the affected individuals where necessary.

Organizations should also be required to "keep and maintain a record of every breach of security safeguards involving personal information under its control", similar to what is required under PIPEDA[29]. In accordance with this, the Commissioner should be granted the power to order organizations to produce these records when required.

[24] Alberta's PIPA, *supra* note 19, section 37.1(1)
[25] Office of the Information and Privacy Commissioner of Alberta, "Personal Information Protection Act: Breach Notification Decision", (February 28, 2018), https://www.oipc.ab.ca/media/979177/p2018_nd_030_007458.pdf
[26] *Ibid*
[27] CBC News, "Uber to inform Canadians affected by data breach", last modified March 9, 2018, https://www.cbc.ca/news/business/uber-breach-data-canadians-1.4570507
[28] PIPEDA, *supra* note 6, s 10.1(3)
[29] PIPEDA, *supra* note 6, s 10.3

The 2008 and 2014 Special Committees also recommended a mandatory breach notification provision, but the provincial government failed to implement it. In addition to repeating that recommendation in this report, this Committee should urge the BC government on its implementation to avoid falling further behind in protecting British Columbians' privacy.

Enhanced Accountability & Transparency by Organizations

47% of British Columbians believe that organizations are not open and transparent about how they collect and use personal information.[30] The next set of recommendations address these concerns by requiring enhanced accountability and transparency practices by organizations.

Meaningful and Informed Consent

Consent allows individuals to autonomously protect their privacy. 67% of Canadians feel that they have little to no control over how their personal information is being used by companies they do business with.[31] According to the federal Office of the Privacy Commissioner, "[i]n order for consent to be considered meaningful... individuals should have a clear understanding of what will be collected, how their personal information will be used, and with whom it will be shared."[32] PIPEDA echoes this, as consent is only valid if an individual can be reasonably expected to understand what they were consenting to.[33]

PIPA's model of consent is based upon a time where information was shared for a limited or defined purpose between two parties. Today's complex information flows and business models involving several third-party intermediaries challenge this archaic model. With the advent of cloud computing, big data, and the Internet of Things, privacy policies have become opaque,

[30] BC FIPA 2020 Survey, *supra* note 7
[31] OPC 2019 Survey, *supra* note 5
[32] Policy and Research Group of the Office of the Privacy Commissioner of Canada, "A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act", last modified May 11, 2016, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/ ("Policy and Research Group of the OIPC")
[33] PIPEDA, *supra* note 6, s 6.1

inaccessible, and complex, making it difficult for individuals to understand who is processing their information and for what purpose.[34]

Where the purpose of collection is provided to individuals, it is often overly vague and high level. As stated by Ms. Robin Bayley, a BC-based privacy consultant:

> "Organizations find nothing in the Act to require them to be able to say what actually *happens* with personal information in a particular circumstance. The truth is usually buried in 'may's'. Organizations also do not believe they are required to inform and individual how they are *authorized* to collect or use personal information in a particular circumstance, and do not know how to answer that question when asked."[35]

Recommendation: In order to maintain meaningful consent, PIPA should be amended to require organizations to provide the purpose of collection to individuals at the time of collection, in a manner that is specific, accessible, and understandable.

Specific means that where possible, separate granular consent options, instead of bundled consent should be required. PIPA allows organizations to collect, use, or disclose only personal information which is "necessary to provide the product or service".[36] In her 2014 written submission to the Special Committee, Ms. Bayley comments that in reality, the "[s]tandard practice is to lump all means of collection, all uses and all disclosures of personal information."[37] This means that an individual consenting doesn't quite know exactly how their personal information will be used and disclosed. The 'separate granular consent' requirement prevents organizations from grouping a purpose which is 'necessary' to provide a product or service with a purpose which is 'unnecessary' to provide a product or service. By separating each purpose of collection (or allowing only similar purposes of collection to be grouped), an individual has more

[34] OPC Letter to ETHI, *supra* note 14
[35] Bayley, Robyn., Submission to the Special Committee to Review the Personal Information Protection Act, (September 2014), https://www.leg.bc.ca/content/CommitteeDocuments/40th-parliament/3rd-session/pipa/submissions/individuals/Submissions-INDIV-PIPA-40-3-Bayley-Robin.pdf ("Bayley")
[36] PIPA, *supra* note 3, s 7(2)
[37] Bayley, *supra* note 35

autonomy and clarity over what personal information is being collected, used, and disclosed, and for what purpose(s).

Accessible means that an organization must make a reasonable effort to bring the relevant documents to the attention of the individual, similar to what is required under PIPEDA.[38] This means that an organization must proactively assist an individual in accessing the relevant documents in order to make an informed decision regarding their personal information. Understandable means the information must be "concise, transparent, [and] intelligible... using clear and plain language", akin to the requirements of the GDPR.[39]

Reformed Privacy Policies

Information about the purpose of collection goes hand in hand with the privacy policies of an organization. Privacy policies are often "opaque and legalistic in nature".[40] An average privacy policy takes 10 minutes to read, and considerably longer to understand.[41] People come across numerous privacy policies in their daily lives and when combined, each 10 minute interval adds up. For example, it would take approximately 200 hours to read all the privacy policies for all the websites the average Internet user visits each year.[42] The legalistic nature of these policies only adds more time.[43] In practice, Ms. Bayley finds that "[w]hen organizations do have written policies and practices available, they are usually inadequate, drafted at the 30,000 foot level or simply reiterating the requirements of the Act, but not telling an individual what the they *actually do* with personal information".[44] It is unrealistic and unfair to expect users to expend such an

[38] Office of the Privacy Commissioner, "Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program", (April 7, 2015), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-001/

[39] GDPR, *supra* note 12, article 12

[40] McDonald, Aleecia M. and Cranor, Lorrie Faith., "The Cost of Reading Privacy Policies.", *I/O Journal of Law and Policy for the Information Society*, (2009): 543–897, https://pdfs.semanticscholar.org/4b51/2e2f5ff42ef00ccceca200d888676e6c506f.pdf?_ga=2.203687568.1281455603.1594835165-1882268101.1594835165 ("McDonald")

[41] 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

[42] *Ibid*

[43] McDonald, *supra* note 40

[44] Bayley, *supra* note 35

amount of time reading, and perhaps considerably more time working to interpret and understand, privacy policies.

Research shows that 69% of Canadians are more willing to do business with companies if they provide easy to understand information about privacy practices.[45] Another report indicates that only 51% of the respondent Canadian companies made their privacy information easily accessible to customers.[46] This calls for change in how organizations draft and distribute their privacy policies to users.

Recommendation: PIPA should be amended to specify that an organization's privacy policies must be accessible and understandable[47].

PIPA currently requires organizations to make their privacy policies available upon request, rather than publicly available.[48] Ms. Bayley's 2014 submission addresses the practical shortcomings of the current legislative framework. In her experience with making requests to organizations for privacy policies, she stated that many "organizations do not have written personal information policies and practices" while others "find out that the Act applied to them for the first time" when a request was made.[49] This raises a serious concern that in some cases where individuals provide personal information, organizations may not have an organized protocol (i.e. privacy policies) on how that personal information will be protected from unauthorized collection, use, and disclosure. Requiring an organization's privacy policies to be publicly available will ensure that, most importantly, organizations have privacy policies in place to protect individuals' personal information, and secondly, allow individuals to assess these policies *prior* to providing their personal information.

[45] OPC 2019 Survey, *supra* note 5
[46] Office of the Privacy Commissioner of Canada, "2019-20 Survey of Canadian businesses on privacy-related issues", last modified June 9, 2020, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2020/por_2019-20_bus/
[47] See the definition of accessible and understandable on page 14
[48] PIPA, *supra* note 3, s 5(c)
[49] Bayley, *supra* note 35

Recommendation: PIPA should be amended to require that an organization's privacy policies be publicly available, rather than available on request.

The next two recommendations focus primarily on the internal operations of an organization, which is a key consideration in the GDPR. As noted by Certified Information Privacy Professional and Corporate Legal Counsel Samantha Delechantos, privacy compliance is ineffective without private sector responsibility, as there are increased privacy complaints and privacy breaches in organizations that haven't properly trained their staff to handle data, developed proper privacy tools, or had some internal responsibility for compliance[50]. Therefore, organizations must work with the Office of the Information and Privacy Commissioner (OIPC) for BC to ensure that they are adequately protecting the personal information of British Columbians.

Mandatory Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is an "assessment tool used to evaluate privacy impacts, including compliance with the privacy protection responsibilities".[51] In addition to contributing to consumer confidence in how personal information is managed, PIAs promote transparency and accountability in an organization's operations.[52]

Furthermore, the Office of the Privacy Commissioner of Canada recognizes that:

> "PIAs are an early warning system, allowing institutions to identify and mitigate risks as early and as completely as possible. They are a key tool for decision-makers, enabling them to deal with issues internally and proactively rather than waiting for complaints, external intervention or bad press.

[50] Delechantos, Samantha., Email message to author, (June 7, 2020)
[51] Privacy and Legislation Branch, Office of the Chief Information Officer, "Privacy Impact Assessment Guidelines", (May 2014), https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/pia_guidelines.pdf
[52] *Ibid*

> An effective PIA can help build trust with Canadians by demonstrating due diligence and compliance with legal and policy requirements as well as privacy best practices.
>
> A PIA report documents the PIA process. The real value comes from the analysis that occurs as part of the process of working through the PIA questions."[53]

The GDPR requires data controllers to complete a PIA "before commencing any processing activity that has a high risk of infringing on a natural person's rights and freedoms".[54] FOIPPA also has a PIA requirement for public bodies[55], and Québec's Bill 64 has proposed such a requirement for private organizations in its Private Sector Act.

PIAs are a means to ensure that in its internal operations, an organization is compliant with data protection laws.[56] Though the OPIC BC expects private organizations to undertake PIAs[57], this expectation is not legally enforceable.

Recommendation: To enhance transparency and accountability by organizations, PIPA should be amended to require organizations to perform mandatory PIAs. In accordance with this, the Commissioner should be given the power to require an organization to produce reports of these assessments when necessary. The frequency, content, and reporting requirement of PIAs should be defined by regulations.

As PIAs require an investment of resources, they may be burdensome for small businesses. However, their functionality as an identification, assessment, and mitigation tool is vital in today's digital era. In addition, detection and neutralization of a privacy breach is likely to be less costly (both financially and reputationally) than mitigation upon breach (see "Concern: Cost of Compliance" below).

[53] Office of the Privacy Commissioner of Canada, "Expectations: OPC's Guide to the Privacy Impact Assessment Process", last modified March 3, 2020, https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/>.
[54] GDPR, *supra* note 12, article 35
[55] FOIPPA, s 69(5)
[56] Office of the Information & Privacy Commissioner of British Columbia, Guidance Document "Privacy Impact Assessments For The Private Sector", (January 28, 2020), https://www.oipc.bc.ca/guidance-documents/2382
[57] OIPC Guidance Doc 2135, *supra* note 15

To balance the burden of PIAs with their usefulness, the content and frequency of a PIA can vary depending on the sensitivity and volume of personal information that an organization works with. These requirements can be defined by regulations. To further alleviate the burden of PIAs, the BC OIPC can provide PIA templates for organizations to provide guidance on what is expected (similar to PIAs under FOIPPA).

Professional Standards Through Accreditation

Where an organization processes highly sensitive or large-scale personal information, those in charge of data protection in that organization ("privacy officer") should have "expert knowledge of data protection law and practices", similar to the GDPR.[58] In practice, this means that the data protection officer should receive professional training, certification and registration. For example, in the European context, Eric Lachaud, author of the article "Should the DPO be Certified?, states that "[t]he most appropriate certification for the DPO [data protection officer] is a combination of the IAPP's Certified Information Privacy Professional credential for EU professionals (CIPP/E) and Certified Information Privacy Manager (CIPM)." [59]

Professional accreditation would provide the privacy officer with both the knowledge and means by which they can ensure that their organization's privacy policies and practices adequately comply with PIPA. This requirement will not be overly burdensome for all organizations as it will be limited to those who process highly sensitive or large-scale amount of personal information. Moreover, training an individual to identify, understand, and neutralize privacy risks, in the long run, will most likely be less costly compared to post-breach mitigation (see Concern: Cost of Compliance).

[58] GDPR, *supra* note 12, article 37
[59] Lachaud, Eric., "Should the DPO be certified?", *International Data Privacy Law* 4, no. 3 (May 2014): 189–202, https://doi.org/10.1093/idpl/ipu008

Recommendation: PIPA should be amended to specify that where an organization processes highly sensitive or large-scale personal information, those designated to ensure compliance with PIPA have "expert knowledge of data protection law and practices".[60]

Accountability of Organizations in Interjurisdictional Transfers

A 2019 paper by Innovation, Science and Economic Development Canada recognizes that "[d]ata is the fuel to grow the Canadian data-driven economy, yet complex data flows involving numerous parties, often across borders, can reduce an individuals' sense of control over of their personal information and ultimately their trust that it can be adequately protected."[61]

75% of British Columbians are concerned about an organization transferring their personal information from BC to organizations outside of Canada.[62] The next set of recommendations aim to increase personal information protection during international data transfers.

Contractual Agreements

With the growing use of data storage and processing systems that are typically located in other countries, data is being shared across international borders, sometimes in jurisdictions with insufficient data protections. For data processing purposes, oftentimes the organization that originally possesses the data ("controller") is different from the organization that ultimately processes the data ("processor"). In addition to being two distinct organizations, they are often situated in different jurisdictions, meaning that the two would be subject to different privacy protection standards. The GDPR safeguards against the downgrading of privacy standards during data transfers by requiring the data controller to "[be] responsible for, and be able to demonstrate compliance with" the GDPR requirements.[63] In other words, while data controllers can outsource their data processing to another organization, they cannot outsource their requirements to comply with the GDPR, and neither can they outsource the risks of non-

[60] GDPR, *supra* note 12, article 37
[61] ISEDC, *supra* note 8
[62] BC FIPA 2020 Survey, *supra* note 7
[63] GDPR, *supra* note 12, article 5(2)

compliance with the GDPR standards. This ensures that the personal information of European citizens is protected to the GDPR standard regardless of where it is being processed. On the contrary, BC PIPA's current provisions are inadequate to ensure that personal information of British Columbians is still being protected to a standard similar to PIPA during data transfers.

Recommendation: Similar to PIPEDA and Québec's Bill 64, PIPA should be amended to specify that "an organization is responsible for using contractual or other means with third parties" [64] to ensure that adequate privacy protections are in place when a third-party has access to British Columbians' personal information.

Contents of Contractual Agreements

To ensure that a third-party organization is given adequate direction in protecting the personal information in its custody, PIPA should require the agreement to contain certain mandatory components. For example, the agreement must contain, *inter alia,* the following:

- GDPR-like auditing powers where the processor makes available to the controller all information necessary to "allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller."[65] This would allow the controller to ensure that the processor is adequately protecting personal information because ultimately, the organization is responsible for ensuring the protection of personal information under its control, even if not in its custody.[66]
- Clauses limiting the processor's use and disclosure of information. For example, the processor will act only on the organization's documented instructions; will not contract to a sub-processor without the organization's prior approval; and will destroy and/or return all personal data to the controller at the end of the contract.

[64] PIPEDA, *supra* note 6, schedule 1 s 4.1.3
[65] GDPR, *supra* note 12, article 28 3(h)
[66] PIPA, *supra* note 3, s 4(2)

- A requirement that in the case of a data breach, the processor will notify the controller without delay. This will allow the controller to take action(s) to mitigate the effects of the breach and protect the privacy of British Columbians without unreasonable delay.

Recommendation: PIPA should be amended to include certain mandatory contents of a contractual arrangement between a data controller and processor. In addition, the Commissioner should be given the authority to review and audit these contracts for compliance as necessary.

Consent Before Transfer

Alberta's PIPA requires that organizations notify individuals when transferring personal information outside of Canada.[67] The GDPR requires explicit consent for transferring personal information to a jurisdiction without adequacy status and appropriate safeguards.[68] As discussed above, consent is a means by which individuals can exercise control over their personal information. An individual should be able to refuse a transfer of their personal information as they find necessary. For example, if an individual feels that the third-party organization their personal information is being transferred to is in a jurisdiction that doesn't afford adequate data protection, they should be able to refuse the transfer of their personal information to that organization. However, this can only happen if the data controller is required to seek an individual's consent prior to transferring their personal information outside of Canada.

Recommendation: PIPA should be amended to require an organization to seek consent from an individual before transferring their personal information outside of Canada.

[67] Alberta's PIPA, *supra* note 19, s 13.1
[68] GDPR, *supra* note 12, article 49

Expansion of the Commissioner's Powers

As private organizations move towards business models that monetize the collection and use of personal information, significant deterrents for non-compliance with PIPA need to be introduced in order to maintain the trust and privacy of British Columbians.

Ability to Levy Administrative Monetary Penalties (AMP)

71% of Canadians are more willing to do business with a company if it faces strict financial penalties for non-compliance.[69] A study done in the UK concluded that AMPs improve data protection compliance, as organizations issued these penalties take data protection more seriously and increase staff privacy training.[70] AMPs are proposed in Québec's Bill 64 for the Private Sector Act.

On March 25, 2020, the Ontario government amended Ontario's health privacy law to allow the Information and Privacy Commissioner the authority to levy monetary penalties against those in contravention of Ontario's *Personal Health Information Protection Act.* Ontario is the first Canadian province to provide the Commissioner with such a power, demonstrating that such authority is both feasible and necessary in today's digital era.

Recommendation: PIPA should be amended to provide the Commissioner with the authority to issue administrative monetary penalties for non-compliance.

Providing the Commissioner with the ability to levy AMPs will not mean that the Commissioner will only levy AMPs. In her oral presentation to this Committee, UK Commissioner Elizabeth Denham noted that in BC "the OIPC, has always emphasized a remedial educational approach to privacy regulation." However, where an organization acts deliberately, negligently[71], or displays

[69] OPC 2019 Survey, *supra* note 5
[70] Information Commissioner's Office, "Review of the impact of ICO Civil Monetary Penalties", (July 23, 2014), https://ico.org.uk/media/1042346/review-of-the-impact-of-ico-civil-monetary-penalties.pdf
[71] Zimmer, Bob., "Towards Privacy by design: Review of the *Personal Information Protection and Electronic Documents Act.* Report of the Standing Committee on Access to Information, Privacy and Ethics", (February 2018), https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf ("ETHI Report")

substantial or systemic non-compliance with PIPA[72], education simply isn't enough. Commissioner Denham stated that in its current form, PIPA allows "organizations [to] just flout the law without fear of real consequences, which is unfair to organizations that take their obligations seriously and diligently comply with the law." The basic tenants of our legal system are fairness and proportionality, and in order to uphold these values, "the most serious offenses deserve the most serious consequences".

In addition, Commissioner Denham pointed out that AMPs would be subject to meaningful controls as "there would be the need for some sort of fact-finding process to confirm that a violation has occurred, and then a notice to the organization of a possible penalty, then hearing from the organization and an assessment of an appropriate penalty, with ultimate oversight by the courts."[73] Therefore, the Commissioner's authority to levy AMPs, if granted, will not be absolute.

A concern typically raised is that such enforcement powers will hinder dialogue and cooperation between an organization and the Commissioner. More specifically, the concern is that organizations will be less likely to seek the Commissioner's assistance in how to comply with PIPA as the Commissioner will seem to have more of an enforcement, rather than an ombudsperson role. However, in the UK, where the Privacy Commissioner has such fine-making authority, concerns of a lack of cooperation or dialogue have not arisen.[74] In short, stronger enforcement powers have not undermined the UK Commissioner's ombudsperson role.

Ability to Order External Audits and Compliance Programs

Another method to motivate an organization's compliance with PIPA is to order the organization to undergo an external audit and compliance process. PIPEDA currently allows the Commissioner to enter into compliance agreements with an organization if "the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit

[72] *Ibid*
[73] Elizabeth Denham's Presentation, *supra* note 22
[74] OPC Letter to ETHI, *supra* note 14

an act or omission that could constitute a contravention" of the Act.[75] We recommend that in PIPA, the Commissioner should be granted the authority to require an organization to undergo an audit and compliance program through a third-party organization and produce a report as the Commissioner sees fit. This would ensure that non-compliant organizations (or those likely to be non-compliant) receive the necessary education and training to comply with PIPA from an accredited third party. A benefit of this approach is that it eases the workload on the Commissioner's Office while ensuring that non-compliant organizations work towards correcting their privacy practices and building PIPA-compliant privacy protection programs. Similar to AMPs, this approach will be discretionary and only used when necessary.

Recommendation: PIPA should be amended to grant the Privacy Commissioner with the authority to order organizations to undergo mandatory third-party external audits and compliance programs. The Privacy Commissioner should also be granted the authority to require reports from such organizations as necessary.

Order Making Authority in Absence of Complaints

Our public opinion survey revealed that there is concerningly low public awareness of privacy rights and protections. If people are unaware of their rights and protections, or are unsure on how to enforce them, complaints for non-compliance with PIPA are likely underreported.

In cases where the public lacks the knowledge or resources to file complaints for non-compliance, the Commissioner's investigatory role becomes vital. Currently, the Commissioner does not have the authority to make binding orders upon audits and investigations conducted without a complaint. However, non-compliance is non-compliance and should be corrected, whether discovered via a complaint, audit, or investigation. Therefore, where the Commissioner initiates an investigation or audit without a complaint, the Commissioner should have the authority to make binding orders against non-compliant organizations. Without this order-making authority, non-compliance by an organization will likely stand uncorrected unless a formal complaint is

[75] PIPEDA, *supra* note 6, s 17.1

made. However, there is no guarantee on how long it would take for such a complaint to be made, or if it even will be made. Moreover, given the Commissioner's limited resources, there is no guarantee on how long it would take for the complaint to be investigated and adjudicated upon. Throughout all this uncertainty and delay, the non-compliant organization will be able to continue its PIPA-infringing practices, putting the personal information of British Columbians at risk. If the Commissioner was granted order-making authority during audits and investigations, such uncertainty and delay may be prevented in many cases, meaning that not only will non-compliant organizations be required to correct their behaviour, they will be required to do so sooner.

Recommendation: PIPA should be amended to specify that where the BC Privacy Commissioner conducts investigations or audits without a complaint, they have order-making powers for non-compliant organizations.

Failure to Respond

Alberta's PIPA, Québec's Private Sector Act, and PIPEDA all have a provision specifying that an organization's failure to respond to a request for information is deemed to be a refusal of the request.[76] BC OIPC's policies currently deem a non-response after 30 days a refusal. However, these policies have not been formalized into binding legislation.

Recommendation: To adequately address an organization's non-response, as well as ensure harmonization with other jurisdictions, PIPA should be amended to explicitly state that failure to respond within 30 days is deemed refusal of a request.

[76] *Supra* note 19, s 28(2.1); *supra* note 11, s 32; *supra* note 6, s 8(5) respectively

Third-party Source of Information

In an era where the purchase of personal information from third parties is becoming increasingly common by private organizations, it is pivotal to note the source of the data in order to ensure its accuracy and completeness.

Recommendation: PIPA should be amended such that where an organization obtains personal information about individuals from third parties, those third party sources must be noted in the individual's file, similar to what is required by Québec's Private Sector Act.[77]

Increased Protections for De-Identified Information

We are concerned that seemingly de-identified information that is actually identifiable may be treated as falling outside the scope of PIPA. PIPA only protects personal information, while non-identifying information remains unregulated.

As is noted by the former BC Privacy Commissioner Elizabeth Denham, "the determination of what is truly non-identifying information is a complex and vexing question and is a specialized area of expertise."[78] The analysis is highly case-specific, depending on what type of data is being shared, the form, and what it is combined with.

Many examples exist where information claimed to be de-identified or anonymized was easily identifiable. The Australian government released a supposedly anonymized dataset of medical billing records that included prescriptions and surgeries. Again, researchers found it surprisingly easy to identify individuals when additional datasets were cross-referenced.[79] In the U.S., New York City officials accidently released a supposedly de-identified data set with the detailed whereabouts of individual taxi drivers, yet with as little as five random location data points,

[77] *Private Sector Act, supra* note 11, s 7

[78] Elizabeth Denham, "A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector" at 23, (April 30, 2014), https://www.oipc.bc.ca/special-reports/1634

[79] Bennett, Holly., "Research reveals de-identified patient data can be re-identified", (December 18, 2017), https://about.unimelb.edu.au/newsroom/news/2017/december/research-reveals-de-identified-patient-data-can-be-re-identified

individual drivers were uniquely identifiable 95% of the time.[80] In addition to privacy concerns for individuals, the sharing of de-identified information with the public has the potential to impact groups of people as well. For example, Strava, a fitness data platform, created an aggregate heat map that ended up revealing the secret locations and movements of US military service members in conflict zones.[81]

Although it is challenging to determine what is non-identifying, it is critical to ensuring that privacy is protected. By PIPA remaining silent on the scope of non-identifying information, and without comprehensive guidance, it is highly likely that this legislative gap leads to companies sharing personal information that they deem non-identifying, without implementing the protections required by PIPA.

Recommendations: PIPA should be amended to include a clear definition of "de-identified information," along with related terms such as "anonymized information," "pseudonymized information," and "aggregate information."

De-identification should be treated as a relative concept that is evaluated contextually and takes into account a variety of factors, including but not limited to: the nature of the data, the reasonable expectations of potentially affected individual(s), the intended purposes for its use, the release environment, the availability of other linkable data, the likely incentives to re-identify the data, the costs and level of expertise required to re-identify data, and, the potential harm to individuals should an individual be re-identified.

[80] Goodin, Dan., "Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts", (June 23, 104), https://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/
[81] Burgess, Matt., "Strava's data lets anyone see the names (and heart rates) of people exercising on military bases", (January 30, 2018), https://www.wired.co.uk/article/strava-military-bases-area-51-map-afghanistan-gchq-military

We further recommend that PIPA include privacy and security requirements for any de-identified information that is reasonably linkable to an individual or group, including to assess de-identification methods as they evolve, and to require a more rigorous standard for any information shared or made available to the public.

Finally, PIPA should require private sector entities to describe methods for de-identifying personal information and provide that private sector entities that share personal information with another entity are responsible for overseeing the third parties use of the de-identified information.[82]

Nothing About Me Without Me

Algorithmic Transparency

Machine learning and predictive systems are being employed in various fields. These systems have the potential for undesirable effects, such as "targeting of certain groups based on race, ethnic origin or socio-economic considerations".[83] Despite this, users have little to no information about how these systems work, or how their personal information is being used by them. PIPA provides individuals the right to know how their information is being used by an organization[84] – new technologies shouldn't undermine that right.

Recommendation: Similar to the GDPR, PIPA should be amended to give individuals who are subject to automated decision making a right to know about the logic involved in such decisions, including the factors considered and their weight.[85] To protect legitimate commercial interests, algorithmic transparency should not extend to require an organization to reveal confidential commercial information to an individual.[86]

[82] Policy and Research Group of the OIPC, *supra* note 32
[83] ETHI Report, *supra* note 71
[84] PIPA, *supra* note 3, s 10
[85] GDPR, *supra* note 12, article 13
[86] ISEDC, *supra* note 9

Overcollection of Employee Personal Information

Today's digital economy facilitates the overcollection of personal information and the employer-employee relationship is no exception. PIPA's vague definition[87] of "employee personal information" raises concerns about employers over-collecting personal information without consent. PIPA must clarify how employee personal information can be collected, used, and disclosed by an employer so that employees are assured that their personal information will be managed appropriately. A submission from BC Government and Employees' Union (BCGEU) will focus on these details to greater extent and we support their recommendations.

Blurred Lines – Public Funding Private Companies

There is a legislative gap that intersects PIPA and FOIPPA in instances where private companies provide a public service through contract or funding by public bodies.

First, private entities performing public functions should not, by default, submit personal data to public entities. Private sector contractors should be able to provide confidential services with appropriate privacy and security provisions for clients, as applicable. Similarly, there needs to be strict legislative parameters and transparency for how public entities in such relationships disclose personal information with private actors.

Recommendation: PIPA should be amended to expressly prohibit the down-grading of privacy rights protections by contractual agreement between public and private entities.

Second, we advocate for legislative reform to address issues of accessibility, transparency, and accountability arising from the corporate veil afforded by PIPA. Per BC FIPA's 2018 poll, 87% of British Columbians support such legislative reform.[88]

[87] PIPA, *supra* note 3. Under PIPA, "employee personal information" is "personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment." [emphasis added]

[88] BC Freedom of Information and Privacy Association, "The results are in! Poll shows BC wants a stronger FOI system", (January 29, 2018), https://fipa.bc.ca/poll-2/

Certain private entities perform public functions and services, sometimes with public funds, but are not subject to the same level of access and transparency as public bodies because they're regarded as private organizations. For example, several private organizations such as bars, nightclubs and restaurants are able to collect personal information about individuals in association with programs such as Bar Watch and Restaurant Watch. However, as these private organizations are subject to PIPA, there is a lack of public access and transparency in how personal information is protected from unauthorized collection, use, and disclosure.

Bar Watch and Restaurant Watch, also known as 'inadmissible patron programs', purport to operate under legal authorities provided by the *Trespass Act*, PIPA and FOIPPA, yet none of this legislation is robust enough to protect people's privacy, nor do they provide effective remedies to those whose liberty and privacy interests are adversely impacted. Not only are the details of these various programs completely opaque to citizens, the nature of the information sharing between food and drink venues and police agencies poses a significant risk to the privacy and liberty of individuals. In at least one instance, an individual who shared their drivers licence information while dining in a participating restaurant had that information incorrectly recorded in a police database as he was labeled an associate of a gang member, a designation that can seriously impact employment and volunteering prospects due to civilian screening programs.[89] In another example, the Vancouver police department easily accessed personal information through the Bar Watch program that was used in a criminal investigation. The Supreme Court of BC found that this disclosure of information breached the patron's reasonable expectation of privacy under section 8 of the Canadian *Charter of Rights and Freedoms*, and that the police should have obtained prior judicial authorization (e.g. a search warrant).[90] These instances highlight the legislative gap present in the current privacy legislation where private organizations

[89] "Letter to the Police Complaint Commissioner from the Executive Director of the BCCLA re: Vancouver Police Department policy complaint regarding collection and storage of personal information in PRIME-BC", (January 23, 2012), https://vancouver.ca/police/policeboard/agenda/2012/0222/SPCRCAgenda.pdf
[90] *R v Roudiani,* 2018 BCSC 1101 at para 51

performing public functions are not subject to the same level of access and transparency on the collection, use, and disclosure of personal information as public organizations.

Other entities in this domain include the BC Association of Chiefs of Police, Lifelabs, and Real Estate Divisions in post-secondary institutions, such as UBC[91, 92]and SFU[93]. Once again, as these organizations are private by designation, they're not subject to Freedom of Information (FOI) requests, meaning that individuals cannot inquire into the operations of these organizations, such as how they use, collect, and disclose personal information or public funds. Numerous public concerns have been raised regarding the actions of these private entities, yet legislative reform has not occurred. Organizations that exercise public functions, sometimes via public resources, should be required to be transparent and accountable to the public, regardless of whether they're public or private in nature.

Recommendation: The BC Legislature address the legislative gap which enables private entities to exercise public functions while displaying a lack of transparency and access on how personal information is collected, used, and disclosed. We recognize that in order to address this gap, complementary amendments to both PIPA and FOIPPA may need to be made.

Increased Public Education

Per BC FIPA's 2020 survey of British Columbians, less than half of the respondents were aware of PIPA, the Privacy Commissioner, the ability to make complaints, and the ability to request access of personal information from organizations. 33% were aware of none, 28% didn't know if existing laws provide sufficient protection for personal information, and 20% didn't know if organizations are transparent in the use of their personal information. This has highlighted that increasing public education is an important element in the protection of privacy rights.

[91] Order F09-06, "The University of British Columbia", (April 21, 2009), https://www.oipc.bc.ca/orders/993
[92] Order F11-3, "Reconsideration of Order F09-06", (October 20, 2011), https://www.oipc.bc.ca/orders/1038
[93] *Simon Fraser University v British Columbia* (Information and Privacy Commissioner), 2009 BCSC 1481

The majority of BC citizens strongly support increasing public education about privacy rights and protections, as well as resources on where to get help. They also support changing secondary and post-secondary education curriculums to include privacy rights awareness programs.

According to Federal Privacy Commissioner Daniel Therrien, "people are unlikely to file a complaint about something they do not know is happening, and in the age of big data and the 'Internet of Things', it is very difficult to know and understand what's happening to our personal information."[94] If individuals don't have the requisite education of their privacy rights and protections, they cannot exercise them. We must educate British Columbians on their privacy rights and protections for PIPA to be effective. Furthermore, public education is important in keeping the legislation updated, as public awareness of PIPA's shortcomings will create a greater imperative on the government to act and make the necessary changes.

The British Columbia Teacher's Federation (BCTF) report[95] highlights these knowledge deficiencies. The report reveals that only 28% of teachers were privacy trained. Out of that 28%, only half of them found the training to be adequate. This means that 85% of teachers using online student information systems, learning management systems, applications, and communication platforms did not have the adequate privacy training for the software. This is especially concerning in light of the Covid-19 pandemic where many educators use digital platforms to manage student information, as well as to educate and communicate with students. Where the personal information of minors is concerned, educators should be provided with the knowledge and skills necessary to ensure that personal information is protected. The BCTF report urges the Ministry of Education and the Information and Privacy Commissioner "develop a guidebook for parents, teachers, and administrators on privacy policies and practices related to digital technology"[96].

[94] Robertson, Susan K., "Calls grow for Canada to modernize privacy laws amid EU changes", (July 24, 2017), https://www.theglobeandmail.com/report-on-business/industry-news/marketing/calls-grow-for-canada-to-modernize-privacy-laws-amid-eu-changes/article35778176/

[95] British Columbia Teachers' Federation, "A Brief to the Ministry of Education from the BC Teachers' Federation", (August 2017), https://bctf.ca/publications/BriefSection.aspx?id=46996

[96] *Ibid*

The BC OIPC has undertaken several educational initiatives, such as developing guidance documents for individuals and organizations, privacy-related lesson plans for students, as well as the PrivacyRight program for organizations. However, as identified by the Canadian Bar Association's 2014 submission, these public education initiatives have in turn compromised the efficiency of processing and adjudicating complaints.[97] On a federal level, there are currently more than 300 PIPEDA-related complaints which are older than a year.[98] If complaints are not addressed in a timely manner, non-compliant organizations are allowed to continue their non-compliance for even longer. In addition to potentially backlogged complaints at the provincial level, the Commissioner has not issued adequate guidance on certain issues, as highlighted by the BCTF report. This indicates that perhaps the BC OIPC requires more resources in order to carry out its mandate of public education, dispute resolution, and complaint investigation.

Recommendation: An increase in resources to public education campaigns re: PIPA so that the BC OIPC can carry out is mandate in public education, PIPA enforcement, and complaint adjudication.

Increased Organization Education

The BC OIPC expends a great number of resources in creating and distributing guidance documents for organizations. These documents contain easy to understand and practical information to assist organizations in complying with PIPA.

On a federal scale, nearly two-thirds (63%) of Canadian organizations responded that they were not aware of OPC's resources for business, which include guidance documents.[99] Therefore, despite their informative and practical content, guidance documents (at least on a federal level) are not utilized to their fullest potential.

[97] Canadian Bar Association, Submission to the Special Committee to Review the Personal Information Protection Act, (February 2015), https://www.leg.bc.ca/content/CommitteeDocuments/40th-parliament/3rd-session/pipa/reports/PDF/Rpt-PIPA-40-3-Report-2015-FEB-06.pdf

[98] Privacy Commissioner of Canada, "Reforming Canada's privacy laws: Shifting from the whether to the how", last modified June 18, 2019, https://www.priv.gc.ca/en/opc-news/speeches/2019/sp-d_20190523/

[99] OPC 2019 Survey, *supra* note 5

There is a lack of publicly available statistics on both the awareness of and the usage of guidance documents at the provincial level, especially for organizations. BC FIPA addressed part of this gap in its general public survey by measuring awareness of the OIPC and increased education of resources. The results indicate that only 31% of the provincial respondents were aware of the OIPC, and 87% of the respondents believe that it is important to provide education on resources for individuals on obtaining help, information, and advice related to privacy.

This Committee has heard from various stakeholders that the 6-year review period for PIPA is too long, especially in an era where technological change is accelerating. Guidance documents are a means by which our privacy protection laws can keep pace with the rapidly changing technology without the need to constantly modify the overarching legislation. Specifically, as PIPA is a broad, technology neutral piece of legislation, guidance documents have the ability to provide an interpretive framework for organizations to understand their present-day privacy obligations and requirements. As these documents provide practical solutions for organizations to comply with PIPA, they're easier to understand, and thus comply with. Furthermore, unlike legislation, these documents do not have to go through a lengthy review process prior to their release, which means that the Commissioner can provide guidance on key issues (e.g. COVID-19 and contact tracing) in a timely manner.

If the OIPC is provided with increased resources in order to communicate and raise awareness on the presence and usefulness of guidance documents, organizations may be more likely to utilize them, motivating compliance with PIPA.

Recommendation: An increase of resources in education campaigns for organizations re: PIPA, so that the BC OIPC can carry out is mandate in public education, PIPA enforcement, and complaint adjudication.

Political Parties and BC's Leadership

As BC's PIPA protects personal information in the political domain, BC is a national leader for others to follow. It is also consistent with the GDPR. We strongly support the BC OIPC's report for recommendations[100] in this area and urge BC to continue leading in this respect.

Concern: Cost of Compliance

Our recommendations call for stricter privacy protections under PIPA. If PIPA is amended to afford greater privacy protections for BC citizens, organizations will likely need to invest more resources to ensure compliance with PIPA. Such an investment may include hiring and/or training staff, investing in privacy-protective technologies to curtail risk, undertaking audits and PIAs, and developing privacy-compliant business policies. While these initiatives may seem quite burdensome, the costs associated with non-compliance are far more onerous.[101] Business disruption, productivity loss, revenue loss, reputational damage, monetary fines, penalties, and settlement costs are only a few consequences of non-compliance with PIPA.

A study done in the United States by Ponemon Institute indicates that the total costs of non-compliance with privacy legislation are nearly three times higher than the costs of compliance.[102] Therefore, while compliance requires an investment of resources, it is beneficial for organizations to proactively take measures to ensure compliance than to risk the onerous consequences of non-compliance.

[100] Office of the Information & Privacy Commissioner for British Columbia, "Full Disclosure: Political parties, campaign data, and voter consent", (February 6, 2019), https://www.oipc.bc.ca/investigation-reports/2278
[101] Ponemon Institute LLC, "Whitepaper: The True Cost of Compliance with Data Protection Regulations", (December 2017), http://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf
[102] *Ibid*

Conclusion

In some respects, BC has been a leader in the field of privacy law, sometimes even ahead of PIPEDA – PIPA grants the Commissioner order-making powers while PIPEDA does not; PIPA applies to political parties while PIPEDA does not. It is evident that, based on today's standards, BC's PIPA is in dire need of reform and, therefore, cannot wait for its federal counterpart.

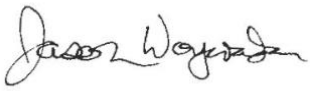
We have provided a list of recommendations to amend BC PIPA. Given that today, more than ever, personal information is being collected and stored in exponential amounts, processed in advanced analytics, and highly prone to being compromised, BC has an opportunity to regain leadership and amend its legislation to offer its citizens the protections they expect and deserve.

BC FIPA thanks the Special Committee to Review the PIPA for the opportunity to provide these thoughts and recommendations, and we look forward to your own recommendations for action on this important issue.

Thank you for your time.

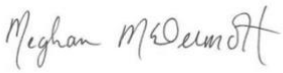
Sincerely,

BC Freedom of Information and Privacy Association



Jason Woywada
Executive Director
P: (604) 739-9788
E: fipa@fipa.bc.ca

BC Civil Liberties Association



Meghan McDermott
Interim Policy Director
P: (604) 630-9752
E: info@bccla.org

List of Recommendations

1. PIPA should be amended 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".[103] The Commissioner should be granted the authority to require an organization to notify affected individuals where necessary.

Organizations should also be required to "keep and maintain a record of every breach of security safeguards involving personal information under its control", similar to what is required under PIPEDA[104]. In accordance with this, the Commissioner should be granted the power to order organizations to produce these records when required.

2. In order to maintain meaningful consent, PIPA should be amended to require organizations to provide the purpose of collection to individuals at the time of collection, in a manner that is specific, accessible, and understandable.

3. PIPA should be amended to specify that an organization's privacy policies must be accessible and understandable[105].

4. PIPA should be amended to require that an organization's privacy policies be publicly available, rather than available on request.

5. To enhance transparency and accountability by organizations, PIPA should be amended to require organizations to perform mandatory PIAs. In accordance with this, the Commissioner should be given the power to require an organization to produce reports of these assessments when necessary. The frequency, content, and reporting requirement of PIAs should be defined by regulations.

[103] PIPEDA, *supra* note 6, s 10.1(3)
[104] PIPEDA, *supra* note 6, s 10.3
[105] See the definition of accessible and understandable on page 14

6. PIPA should be amended to specify that where an organization processes highly sensitive or large-scale personal information, those designated to ensure compliance with PIPA have "expert knowledge of data protection law and practices".[106]

7. Similar to PIPEDA and Québec's Bill 64, PIPA should be amended to specify that "an organization is responsible for using contractual or other means with third parties"[107] to ensure that adequate privacy protections are in place when a third-party has access to British Columbians' personal information.

8. PIPA should be amended to include certain mandatory contents of a contractual arrangement between a data controller and processor. In addition, the Commissioner should be given the authority to review and audit these contracts for compliance as necessary.

9. PIPA should be amended to require an organization to seek consent from an individual before transferring their personal information outside of Canada.

10. PIPA should be amended to provide the Commissioner with the authority to issue administrative monetary penalties for non-compliance.

11. PIPA should be amended to grant the Privacy Commissioner with the authority to order organizations to undergo mandatory third-party external audits and compliance programs. The Privacy Commissioner should also be granted the authority to require reports from such organizations as necessary.

12. PIPA should be amended to specify that where the Commissioner conducts investigations or audits without a complaint, they have order-making powers for non-compliant organizations.

[106] GDPR, *supra* note 12, article 37
[107] PIPEDA, *supra* note 6, schedule 1 s 4.1.3

13. To adequately address an organization's non-response, as well as ensure harmonization with other jurisdictions, PIPA should be amended to explicitly state that failure to respond within 30 days is deemed refusal of a request.

14. PIPA should be amended such that where an organization obtains personal information about individuals from third parties, those third party sources must be noted in the individual's file, similar to what is required by Québec's Private Sector Act.[108]

15. PIPA should be amended to include a clear definition of "de-identified information," along with related terms such as "anonymized information," "pseudonymized information," and "aggregate information."

We further recommend that PIPA include privacy and security requirements for any de-identified information that is reasonably linkable to an individual or group, including to assess de-identification methods as they evolve, and to require a more rigorous standard for any information shared or made available to the public.

Finally, PIPA should require private sector entities to describe methods for de-identifying personal information and provide that private sector entities that share personal information with another entity are responsible for overseeing the third parties use of the de-identified information.[109]

16. Similar to the GDPR, PIPA should be amended to give individuals who are subject to automated decision making a right to know about the logic involved in such decisions, including the factors considered and their weight.[110] To protect legitimate commercial interests, algorithmic transparency should not extend to require an organization to reveal confidential commercial information to an individual.

[108] *Private Sector Act, supra* note 11, s 7
[109] Policy and Research Group of the OIPC, *supra* note 32
[110] GDPR, *supra* note 12, article 13

17. PIPA should be amended to expressly prohibit the down-grading of privacy rights protections by contractual agreement between public and private entities.

18. The BC Legislature address the legislative gap which enables private entities to exercise public functions while displaying a lack of transparency and access on how personal information is collected, used, and disclosed. We recognize that in order to address this gap, complementary amendments to both PIPA and FOIPPA may need to be made.

19. An increase in resources to public education campaigns re: PIPA so that the BC OIPC can carry out is mandate in public education, PIPA enforcement, and complaint adjudication.

20. An increase of resources in education campaigns for organizations re: PIPA, so that the BC OIPC can carry out is mandate in public education, PIPA enforcement, and complaint adjudication.