STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION ACT

Supplemental submission to the Special Committee to Review the Personal Information Protection Act

FEBRUARY 23, 2021
CANLII CITE: 2021 BCIPC 09
QUICKLAW CITE: [2021] B.C.I.P.C.D. NO. 09

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

PREFACE

This submission supplements my Office's September 16, 2020 submission on modernizing British Columbia's private sector privacy law, the *Personal Information Protection Act* (PIPA).[1] It recognizes that the federal government has since introduced legislation that would replace the federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), with the new Consumer Privacy Protection Act (CPPA).[2]

This is of critical importance to the Special Committee's deliberations for two reasons. The first is that harmonization among federal and provincial laws benefits both businesses and individuals. The second is that the CPPA, like its predecessor law, says it prevails over provincial privacy law unless the federal Cabinet declares that the provincial law is "substantially similar" to the federal one. Such a declaration was made for British Columbia's law in 2004[3] and it is reasonable to assume that British Columbia will seek such a declaration once the new CPPA is in force. To achieve that goal, the *Personal Information Protection Act* will have to be amended in ways that support substantial similarity while respecting British Columbia's policy environment.

This supplemental submission demonstrates how the proposed CPPA and my recommendations of September 16, 2020 align on the matters necessary to maintaining legislative harmony. Read together, they provide the Special Committee a roadmap to recommendations for the long-overdue modernization of British Columbia's law.

There are positive aspects to the proposed new federal law, which has provisions that are consistent with our earlier submission to the Special Committee. However, the proposed legislation also introduces some new features that are not desirable and do not go to the heart of matters requiring substantial similarity in any new BC law.

PIPA was drafted close to 20 years ago and this is its third statutory review. There have obviously been significant changes in technology, business, and society over the past two decades, yet none of the past Special Committees' recommendations have found their way into the statute books. As I have said before, continued inaction is not an option. Privacy laws are being modernized around the world in response to increases in digital economic activity and the challenges posed by new technologies such as artificial intelligence, data analytics, facial recognition, and social media. The sudden shift to remote ways of doing business, learning, and

---

[1] That submission is found here: https://www.oipc.bc.ca/special-reports/3465 (accessed February 14, 2021).

[2] The *Consumer Privacy Protection Act* would be enacted by Bill C-11, the *Digital Charter Implementation Act, 2020*. It was given First Reading in the House of Commons on November 17, 2020. It can be found here: https://parl.ca/Content/Bills/432/Government/C-11/C-11_1/C-11_1.PDF (accessed February 14, 2021).

[3] *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220 (October 12, 2004): https://laws-lois.justice.gc.ca/PDF/SOR-2004-220.pdf (accessed February 14, 2021). Section 1 of that order states that an "organization, other than a federal work, undertaking or business, to which" British Columbia's *Personal Information Protection Act* applies "is exempt from the application of" the federal law, the *Personal Information Protection and Electronic Documents Act*, "in respect of the collection, use and disclosure of personal information that occurs within the Province of British Columbia."

living in response to the COVID-19 pandemic highlights the need to update BC's personal information protection law.

The proposed CPPA reflects this modernizing trend and heightens expectations to amend British Columbia's private sector law. British Columbia's own law can and should keep pace, while promoting expansion of British Columbia's digital economic activity, a vitally important objective that is emphasized in our earlier submission.

This submission assesses aspects of the proposed CPPA with specific recommendations about those components that are suited for British Columbia's needs.

As requested by the Special Committee, this submission also offers general information about the European Union's *General Data Protection Regulation* (GDPR), which came into force in 2018 and continues to influence privacy legislation globally.

I should note here that our original submission contains the detailed reasons for our recommendations, and therefore should continue to be referenced in your deliberations.

It is my honour to support your vitally important work, which will, I am sure, carry significant and enduring benefits for British Columbia's citizens, organizations and economy.

February 19, 2021

ORIGINAL SIGNED BY

Michael McEvoy
Information and Privacy Commissioner for British Columbia

DOMESTIC CONTEXT: PIPEDA & PIPA

What follows is designed to support your understanding of the original policy basis for enactment of both the federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and British Columbia's *Personal Information Protection Act* (PIPA). It then summarizes how the proposed federal Consumer Privacy Protection Act (CPPA) affects PIPA reform.

PIPEDA was enacted in 2000 and came into force on January 1, 2001.[4] Its stated purpose is to establish privacy rules governing collection, use and disclosure of personal information "in an era in which technology increasingly facilitates the circulation and exchange of information", while recognizing "the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[5]

PIPEDA applies to "every organization in respect of personal information that…the organization collects, uses or discloses in the course of commercial activities".[6] Its rules for collection, use and disclosure of personal information largely derive from a private sector source, the Canadian Standards Association's (CSA) *Model Code for the Protection of Personal Information*,[7] which forms Schedule 1 to PIPEDA.

The choice to adopt a private sector organization's voluntary code as the heart of a public law is unusual but it reflects the federal government's concern at the time to get business groups on board with privacy protection. Industry had coalesced around the CSA standards and government did not, at that time, wish to get too far ahead of this consensus, but it also was aware of calls from legislators, civil society groups, academics, and others for a private sector privacy law.

Policymakers were also aware that in 1995 the European Union (EU) had issued a privacy directive, which came into force in 1998, that carried implications for data flows to and from the EU.[8] In a nutshell, the directive set out privacy standards that EU member states were

---

[4] As its title signals, PIPEDA also creates electronic transaction rules, which are not relevant for present purposes.
[5] Section 3. Section 2 of PIPA contains a similar purpose statement, although it does not refer to the impact of technology on personal privacy.
[6] Section 4(1). PIPEDA also applies to federal works, undertakings, or businesses, and applies Sections 4(1) and (1.1) also extend PIPEDA to certain other organizations, including some federal Crown corporations. Section 2(1) defines the term "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." We discuss below how PIPEDA does not apply where a province has enacted a substantially similar privacy law.
[7] CAN/CSA-Q830-96.
[8] The directive is *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. That now-repealed directive can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN (accessed February 14, 2021).

required to implement in domestic legislation. It also would impose restrictions on the free flow of personal information to and from other countries unless, among other options, the European Commission ruled that the other country's privacy protections were adequate. This EU development was undoubtedly a factor in PIPEDA's development. Since the directive could create barriers for Canadians seeking to do business in the EU, the enactment of an adequate Canadian privacy law was almost certainly the best response to the EU developments.

It is worth noting here that another factor the federal government was aware of in developing PIPEDA was the 1980 Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[9] As an OECD member, Canada had supported the adoption of those guidelines. A core objective was to protect privacy in the context of international data flows while not seriously disrupting important economic activities involved in transborder data flows. Member states were encouraged to use the OECD guidelines to achieve this balance and at the same time, through their adoption, promote harmonization of privacy legislation across nations.

To sum up, PIPEDA was a response to domestic developments, including the CSA's *Model Code for the Protection of Personal Information*, and it responded to international pressures, notably the EU's move to require adequate privacy protections in countries to which EU data subjects' information might be exported.

As discussed below, PIPA was itself, at least in part, a response to PIPEDA's arrival. British Columbia policymakers set out to fashion a law that reflects the province's needs while enabling British Columbia's enterprises to do business domestically and internationally. As the size of our digital economy grows, the imperative of keeping citizens' trust that their privacy will be appropriately protected is stronger than ever. To engender that trust and to support BC organizations, PIPA needs to catch up with and support our digital economy through significant, internationally harmonious amendments.

EUROPE'S GENERAL DATA PROTECTION REGULATION

This section offers a high-level overview of recent EU developments, which have doubtless been a driver in the federal government's decision to update the federal private sector privacy law. For further detail about the *General Data Protection Regulation* (GDPR), you can refer to our 2018 guidance, *Competitive Advantage: Compliance with PIPA and the GDPR*.[10]

The 1998 EU directive mentioned above is no longer in force, having been replaced in 2018 by the GDPR. The GDPR is a "data protection", or privacy law that, unlike the predecessor directive, has direct force in EU member states. As explained below, the GDPR also has implications for Canadian privacy laws.

---

[9] http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Accessed February 15, 2021). The OECD guidelines were updated in 2013.

[10] https://www.oipc.bc.ca/guidance-documents/2135 (accessed February 14, 2021).

The GDPR applies to both the public and private sectors and has slightly different rules for each. It applies to the "processing" of "personal data" by a "controller" or "processor".[11] The GDPR states the objectives of these rules. The first is to protect individuals' fundamental rights and freedoms, including their right to protection of personal data, and the second is to protect the free movement of personal data within the EU.[12]

Many of the GDPR's rules are familiar to Canadian eyes, including:

- the duty to obtain individuals' consent for collection, use or disclosure of personal information;
- exceptions to the duty to get consent;
- a duty to collect the minimum personal information necessary for the organization's purpose;
- obligations relating to the accuracy of personal data;
- a duty to implement security measures to protect personal data;
- a right of individuals to object to collection, use or disclosure;
- a duty on organizations to be able demonstrate compliance with the GDPR; and
- a requirement for EU member states to provide independent compliance oversight and enforcement.[13]

The GDPR also introduced rights and obligations that do not feature in existing Canadian privacy laws, including:

- rules giving heightened protection for sensitive personal information;[14]
- the right to data portability;[15]
- the right to be forgotten;[16] and
- the right to object to automated decision-making.[17]

The GDPR's enforcement provisions differ from existing Canadian privacy laws in a significant way. They authorize EU privacy regulators to fine organizations that break the law. These monetary penalty powers offer significant incentives to all organizations, including globally

---

[11] Processing can be automated in whole or in part, or not automated at all. This is explicitly stated in article 2(1), noting also that the definition of "processing" refers to the collection, use and disclosure of personal data without limiting such activities to automated processes. The term "controller" is defined to include a "legal person, public authority, agency or other body" that "determines the purposes and means of processing personal data".

[12] Article 1.

[13] This summary of course translates GDPR terms into Canadian terms.

[14] Article 9(1) prohibits the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning a natural person's sex life and sexual orientation; genetic data or biometric data." Articles 9(2)-(4) establish exceptions to that prohibition and rules that condition the exceptions.

[15] Article 20.

[16] Article 17.

[17] Articles 21 and 22.

active businesses, to take privacy seriously. Our original submission to the Special Committee urged you to recommend that PIPA be amended to introduce a monetary penalty scheme, and the CPPA would do so. This aspect of the GDPR and CPPA, is discussed later.

The last feature of the GDPR meriting mention here is its impact on the transfer of personal information outside the EU. The GDPR prohibits the export of personal information to a state outside the EU unless certain conditions apply. An organization may export information if it has "provided appropriate safeguards", and where "enforceable data subject rights and effective legal remedies" are available.[18] Appropriate safeguards can take the form of adequate contractual clauses between the data exporter and recipient organization.[19]

This approach to data export may be applied to specific business relationships, or individual transactions, and that may appeal to some businesses, but it is not a plenary state-to-state solution. Like its predecessor EU directive of 1998, the GDPR enables export of personal information from the EU to another country where the European Commission has decided that the other country "ensures an adequate level of protection".[20] In making this decision, the European Commission must consider a range of elements, including the nature of the other state's privacy laws, public security laws, access to personal information by public authorities, and effective and enforceable individual privacy rights.[21] It must also consider "the existence and effective functioning" of "independent supervisory authorities" responsible for "ensuring and enforcing compliance" with privacy laws, including whether those authorities have "adequate enforcement powers".[22]

HARMONIZING PIPA WITH THE GDPR & CPPA

In 2001, the EU issued an adequacy ruling for PIPEDA under the EU directive then in place, a decision that has for 20 years enabled personal information from the EU to be transferred to organizations in Canada. Adequacy facilitates the operation of Canadian businesses inside the EU, whether they are manufacturers, financial or professional service organizations, airlines or other businesses that use personal information (including employees' information) in their businesses.

There can be little doubt that, in preparing the CPPA, the federal government had it in mind to aim for adequacy with the GDPR. The CPPA itself states that it applies "in respect of personal information…that is collected, used or disclosed interprovincially or internationally by an

[18] Article 46(1).
[19] The GDPR's enforcement coordination body, the European Data Protection Board, has issued an opinion, and template clauses, for this purpose. (The members of the Board are the national level privacy regulators for each EU member state.) The January 14, 2021 *EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors*, and template clauses, is found here: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en (accessed February 14, 2021).
[20] Article 45(1).
[21] Article 45(2).
[22] Ibid.

organization".[23] This indirectly highlights the importance of maintaining Canada's adequacy status for GDPR purposes. The importance of this for Canada's digital economic activity, and thus cross-border data flows, is also confirmed by these ministerial comments during Second Reading of the CPPA bill:

> It is also important to note that the legislation would help protect the privacy of Canadians, while strengthening the ability of Canadian businesses to compete globally. This positions Canada to succeed internationally.
>
> When PIPEDA was introduced in 2000, it was considered a global leader among data protection laws. In 2002 [*sic*], the European Commission found that PIPEDA provided adequate protection relative to EU law. The finding of adequacy gave us an international edge by allowing us to have free flow of data between Canadian and EU companies.
>
> More recently in 2018, the EU brought into force its GDPR, the general data protection regulation. Since then, the EU has been reviewing Canada's adequacy against the GDPR. They have made it clear that we must reform our privacy regimes in order to maintain our advantage when it comes to this status. I believe the legislation would achieve GDPR adequacy while maintaining the made in Canada approach.[24]

The provincial government will decide, of course, whether to approach the EU directly to seek an adequacy ruling for PIPA. It did not do so under the GDPR's predecessor directive, perhaps because it was thought best to leave the issue of international harmonization to the federal government. The Quebec government did seek a direct adequacy ruling under the EU directive but was not successful in doing so. For practical purposes, therefore, it is best to assume that the CPPA will be the vehicle for addressing GDPR adequacy directly, with the question of whether PIPA is "substantially similar" to the CPPA sufficing.

Like PIPEDA, the CPPA contemplates that it applies within a province unless the federal Cabinet is satisfied that "legislation of a province that is substantially similar" to the CPPA "applies to an organization, a class of organizations, an activity or a class of activities".[25] In that case, Cabinet may, by order, "exempt the organization, activity or class from the application" of the CPPA "in respect of the collection, use or disclosure of personal information that occurs within that province".[26] The factors to be applied in making this decision will be established by regulation under the CPPA.[27]

---

[23] Section 6(2). It should be noted here that the assertion that the CPPA applies to interprovincial collection, use or disclosure of personal information does not necessarily mean that PIPA cannot also apply where personal information collected in the province is transferred to another province.

[24] Hansard, vol 150, number 35, November 24, 2020, page 2289. https://www.ourcommons.ca/Content/House/432/Debates/035/HAN035-E.PDF (accessed February 14, 2021). At

[25] This language is found in what will become section 119(2) of the CPPA.

[26] Ibid.

[27] Ibid., note 18 above, at page 2307.

This aspect of the CPPA obviously raises the question for the provincial government of whether it will again seek a declaration of substantial similarity. The possibility that it will do so, as it did under PIPEDA, is reason enough to modernize PIPA in a meaningful way. In any case, even if the provincial government decided not to seek a declaration, there is a compelling public interest in updating PIPA so that it remains at the forefront while keeping it in harmony with the CPPA and other modern privacy laws. The following discussion therefore focuses only on those CPPA features—several of which echo our earlier recommendations—that align with what we believe is the minimum needed to ensure that PIPA remains fit for purpose in the coming years and to achieve a declaration of substantial similarity to the CPPA, if desired.

CONSUMER PRIVACY PROTECTION ACT CONSIDERATIONS

The Digital Charter Implementation Act, 2020, which proposes enactment of the CPPA, is part of the federal government's Digital Charter initiative, which began some five years ago. In a 2019 report on its public consultations, the government had this to say about privacy laws and the digital economy:

> Digital and data transformation has led to an explosion of data, with a large proportion of the world's data created recently. Data is helping to fuel innovations like AI, machine learning, and the Internet of things. However, the rapid acceleration of data being created, and its use as a commodity means Canada must re-evaluate the frameworks it has in place. While the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and other marketplace frameworks continue to provide important protections, particularly as they were situated as technologically neutral in orientation, there remains important questions about how to ensure these frameworks are transparent and have the appropriate approach to maintain Canadian's privacy and trust in an increasingly data-driven world.
>
> Canada has a mature regulatory environment, however, with the growing complexity of vast amounts of data flows, privacy, and cross-border markets, many Canadian companies, in particular SMEs, expressed difficulty understanding how best to comply with existing data and privacy legislation and the corresponding regulations. …
>
> Canadians told us that the current privacy legislation, PIPEDA, needs to be modernized and streamlined however, the Government must ensure that updates both support innovation and protect Canadians. Rules must be supported by clear guidance on implementation and applicability and must consider effective and appropriate enforcement measures to hold players accountable and ensure Canadians have confidence and trust in these protections. Effective enforcement must also include ease of understanding and compliance, strong advocacy, and a commitment to due process in order to not add undue burden and costs to firms.
>
> We also heard that updates must consider emerging privacy norms, particularly internationally, and work coherently across other important marketplace frameworks, including competition and intellectual property, as well as emerging regulations for particular disruptive technologies and business models, such as blockchain or open

> banking. The Government must consider the accelerated pace at which the technological ecosystem evolves and ensure that measures are agile and flexible enough to remain responsive. And it is important to continue working proactively and in partnership with industry to ensure benefits for both businesses and citizens are optimized.[28]

Several CPPA provisions echo recommendations we made to you in our September 2020 submission. However, other proposals contained in the federal bill are not desirable, as we explain below.

We begin with the observation that fully 10 of the 12 recommendations we made to the Special Committee in our earlier submission are found in the proposed CPPA (although in some instances with a difference in approach).

In response to the Special Committee's request, the discussion that follows is a consideration of our earlier recommendations in relation to the CPPA proposals. Please refer to our original submission to you for a complete assessment of our recommendations and the detailed arguments for them.

Mandatory Breach Notification (OIPC Recommendation 1)

British Columbia is now an outlier at home and internationally because PIPA does not require organizations to notify affected individuals of a privacy breach. PIPEDA's breach notification scheme was enacted in 2018 and Alberta's *Personal Information Protection Act* has had breach notification requirements since 2010. Major business groups, notably, the Insurance Bureau of Canada, Canadian Marketing Association, Canadian Medical Protective Association, and BC Real Estate Association support amending PIPA to require breach notification. Civil society groups such as the BC Freedom of Information and Privacy Association and British Columbia Civil Liberties Association have added their voices to this call for reform, as have other groups such as the BC NDP and the BC Government Employees' Union.[29]

Breach notification allows individuals to take steps to protect themselves when there is a risk of harm. This is why we recommend that PIPA be amended to require organizations to notify affected individuals of incidents involving the loss of, or unauthorized access to or disclosure of, personal information where it is reasonable to believe that there is a real risk of significant harm to an individual. We also recommend that these amendments should authorize the Commissioner to require an organization to notify affected individuals where the organization has not done so. There should also be requirements, we said, relating to the timing of notice,

---

[28] Innovation, Science and Economic Development Canada, *Canada's Digital Charter In Action: A Plan by Canadians, for Canadians*, pages 9-10 (footnotes omitted): https://www.ic.gc.ca/eic/site/062.nsf/vwapj/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf (Accessed February 14, 2021).

[29] https://www.leg.bc.ca/parliamentary-business/committees/41stParliament-5thSession-pipa/meetingdocuments to read submissions to the Special Committee.

the contents of notices, supporting information that must be provided to the Commissioner, and record-keeping duties for organizations about the incidents they have experienced over time. Last, we recommended that the PIPA amendments should be crafted to harmonize as far as possible with Alberta's rules and those in PIPEDA.

The CPPA will essentially replicate PIPEDA's existing breach notification requirements, with some modifications that need not be discussed here, and those requirements align very well with our recommendations last autumn.

This aspect of the CPPA underscores the need for British Columbia to act now, to help ensure that PIPA remains relevant and in harmony with that law and other similar laws in Canada. Failure to introduce breach notification in British Columbia's law would likely be a real factor in assessment of PIPA's similarity to the CPPA.

Protecting Personal Information Transferred to Service Providers (OIPC Recommendation 2)

As noted in our original submission, unlike many other laws, PIPA does not expressly hold organizations responsible for the personal information they transfer to one of their service providers, such as a payroll processing company or a cloud-based service provider. Under PIPEDA, the GDPR, the Alberta legislation, and soon Quebec's privacy law,[30] organizations have explicit responsibilities in such cases. We continue to recommend that PIPA should explicitly state that an organization remains responsible for its customers' or clients' personal information when it is entrusted to a service provider. The rules need not be overly prescriptive. Organizations should simply be required to use contractual or other means to ensure their service providers comply with the law.

The CPPA's approach will be consistent with our recommendation. It will define as a "service provider" any organization, including a corporate affiliate, that "provides services for or on behalf of another organization to assist the organization in fulfilling its purposes."[31] It will require an organization that transfers personal information to a service provider to "ensure, by contract or otherwise, that the service provider provides substantially the same protection of the personal information as that which the organization is required to provide under this Act."[32] The service provider will not need to get consent for collection, use or disclosure of personal information that the client organization gives to it for the purpose of performing services for the client.[33] As long as the service provider stays in its lane and only uses the personal

[30] This refers to amendments to be enacted by Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* [Quebec Bill 64]. http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html. (Accessed February 14, 2021). At the time of writing, the Bill has yet to be enacted.
[31] Section 2.
[32] Section 11(1).
[33] Section 11(2). This consent exemption does *not* apply if service provider "collects, uses or discloses that information for any purpose other than the purposes for which the information was transferred" to it by the client.

information to provide the services to the client organization, the client remains responsible under the CPPA.

We support this approach, which mirrors our recommendation on how to handle transfers of personal information to service providers.

Modernizing Consent Requirements (OIPC Recommendation 3)

The adequacy of current approaches to consent in the evolving digital marketplace has been hotly debated for years. PIPA was crafted roughly 20 years ago, before the complex ecosystem of digital technologies and services had really started to evolve. Its approach to consent is therefore essentially bilateral, assuming that there is a straightforward, simple transaction between one business and one customer. This has been unrealistic for years.

As we discussed in our earlier submission, among the deficiencies in PIPA is that it does not require written notice to individuals who are being asked to consent to the collection, use or disclosure of their information. Nor does it require any written notice that is given to be clear, easy to understand and comprehensive. Examples of legalistic and lengthy notices that take hours to read, while managing to be imprecise, are all too typical, leaving individuals in the dark about who will do what with their information.

Policymakers have increasingly tried to grapple with this problem in recent years, and we made three specific recommendations for an improved approach to consent, recommendations that would better protect individuals without imposing undue burdens on businesses. Similar approaches are found under the GDPR, in Quebec and now at the federal level, through the CPPA.

Under the CPPA, express consent will be required unless it is appropriate to rely on implied consent.[34] For express consent to be valid, organizations will have to provide, "in plain language", information about the purposes for the collection, use or disclosure of information, the way the information is to be collected, used or disclosed, any foreseeable consequences of the collection, use or disclosure, and the names of any third parties (or types of third parties) to which the information may be disclosed. These requirements are close in spirit and letter to our consent-related recommendations to the Special Committee.[35]

The CPPA also carries forward existing PIPEDA consent exceptions, which are very close to PIPA's consent exceptions. However, and this is where we have serious reservations about the federal proposal, the CPPA would introduce new exceptions to consent that are overly broad or ambiguous. We are far from the only observers who have grave concerns about these new

[34] This takes into consideration the individual's reasonable expectations and the sensitivity of the personal information involved.

[35] We continue to believe that PIPA should also require organizations to provide notice for consent purposes separate from other legal terms, and to assist any individual to understand what they are being asked to agree to if the individual asks.

exceptions. This aspect of the CPPA has prompted one of Canada's most respected and experienced privacy scholars to refer to the CPPA consent exceptions as "quite frankly a data protection disaster".[36]

Reactions like this, which are widely shared, conceivably could result in some of the proposed exceptions being removed or narrowed as the bill proceeds, but they are not a model for PIPA reform. Exceptions to consent are appropriate, and PIPA contains at least 14 of them, but modern privacy laws remain consent-based by default and exceptions should be limited, narrow, and clearly justified. In light of the recommendation made below about the CPPA consent exceptions, it is necessary to make only a few points to underscore why there are grave concerns about the CPPA's consent exceptions for our purposes.

The first point is that some of the new CPPA consent exceptions are overly broad and ambiguous. The second is that, in addition to dispensing with individual control through consent, they also eliminate transparency, enabling organizations to secretly collect, use and disclose our personal information without having to tell us what they are up to. This is inconsistent with long-accepted, internationally recognized, data protection principles.

The first example of these concerns is the exception that would allow organizations to use people's personal information "without their knowledge or consent to de-identify that information",[37] and then use it—without any transparency,[38] much less individual control—"for the organization's internal research and development purposes, if the information is de-identified before it is used."[39]

Setting aside the glaring lack of transparency and accountability that this contemplates, it is widely accepted that modern information technologies make it almost impossible to truly de-identify personal information. The clear risk is that organizations will have a free hand, without anyone knowing what they are doing, to purportedly de-identify personal information and then use it for their own "research and development" (a concept that covers a lot of ground). This is of particular concern since internal research and development is increasingly likely to involve the use of data analytics, which could result in covert creation of information about identifiable individuals.

Another concern is the proposed consent exception for "business activities". Granted, there are some controls on this, such as the rule that an organization may only collect or use personal

---

[36] Teresa Scassa, "The Gutting of Consent in Bill C-11", blogpost, December 21, 2020. Teresa Scassa is a law professor and Canada Research Chair in Information Law and Policy at the University of Ottawa, Faculty of Law. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=336:the-gutting-of-consent-in-bill-c-11&Itemid=80. (Accessed February 15, 2021).

[37] Section 20.

[38] Sections 12(3) and 14(2)(a) will, in combination, require an organization to "record" that new use, but this does not require the organization to proactively disclose this use to affected individuals. The CPPA's other transparency requirements are not likely to remedy this concern.

[39] Section 21.

information for a CPPA-specified business activity if "a reasonable person would expect such a collection or use for that activity". Further, an organization may not collect personal information under this exception "for the purpose of influencing the individual's behaviour or decisions".[40]

Yet the list of "business activities" set out in the CPPA—a list that can be enlarged by regulation, not legislation—is wide and ambiguous. It includes, for example, any "activity that is carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk". As a leading privacy scholar has rightly suggested, this could include profiling of individuals, using artificial intelligence, to assess their credit risk, all done secretly and with no individual input.[41]

Another example is "an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual". This could enable indirect collection of personal information without any apparent limits on what activity the business might be pursuing, and with no sense about why the impracticability of consent should be determinative.[42]

At the time of writing, the bill enacting the CPPA has not been scrutinized by the relevant House of Commons committee, and it conceivably could change during that process. For the reasons outlined above, however, we urge the Special Committee not to recommend adoption of all of the CPPA's consent exceptions. Rather, we urge you to recommend only that the government monitor progress of the CPPA on this issue as part of its assessment of what, if any changes, are appropriate for PIPA's consent exceptions. We urge the Special Committee also to affirm that the concept of individuals' control over their own personal information is, through consent, a core principle of PIPA.

Automated Decision-making (OIPC Recommendation 4)

Our submission made several recommendations to protect British Columbians from harm through inappropriate use of automated decision-making systems. While the CPPA commendably includes provisions in this area, it falls short of what we believe is necessary to protect citizens from the use of opaque, otherwise unregulated, decision-making technologies.

Information technologies are evolving in ways, and at rates, that can raise serious risks for individual rights and interests, in both the private and public sectors. Advances in data analytics and artificial intelligence can undoubtedly help improve services to individuals and communities, but they also can create risks for individuals' privacy (and other rights). The GDPR takes note of that fact and contains significant protections for individuals in this area. It gives individuals the right—with some exceptions—to prohibit an organization from making a decision about them based only on automated processing of personal information, including

[40] Section 18.
[41] Ibid., note 36 above.
[42] These two exceptions are both found in section 18.

profiling, that produces legal effects related to the information or significantly affects the individual.[43]

The CPPA, on the other hand, does not meaningfully address these pressing concerns. It usefully defines the term "automated decision systems" as "technology that assists or replaces the judgment of human decision makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning and neural nets".[44] However, its substantive provisions in this vital area fall short.

Those provisions merely require an organization to provide, as part of its duty to make plain language information available about its policies and practices, a "general account" of its "use of any automated decision system to make predictions, recommendations or decisions about individuals that could have significant impacts on them".

There is real concern that an organization's "general account", may bury, in a standard transparency disclosure document, case-specific details that individuals reasonably need to protect their privacy and other rights.

Specific examples might be where a financial institution uses an automated decision system to deny a much-needed mortgage or screen out someone from a job opportunity without meaningful explanation. Such systems are far from infallible, not least because they depend on personal information that may be outdated, false, incomplete, or otherwise defective.

These concerns are exacerbated by the fact that an organization is only required to provide a generic statement where its systems make predictions, recommendations or decisions that could have "significant impacts on" individuals.

The GDPR perhaps swings too far in the other direction, enabling individuals to, with some exceptions, veto the use of automated decision-making in ways that affects them. We do not support that approach, preferring instead to reaffirm our recommendation 4, which calls for amendments to PIPA to require an organization using automated processing of personal information to:

- notify an individual that automated processing will be used to make a decision about them;
- on request, disclose the reasons and criteria used; and
- receive objections from individuals to the use of automated processing by someone within the organization that has the authority to review and change the decision.

---

[43] Article 22, with Article 4 defining "profiling" as "the "automated processing of personal data" to "evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

[44] Section 2.

The kind of notification we recommend is a critical individual right in a regulatory environment that requires individuals to complain to a regulator if they believe their personal information was used in a manner not permitted under the law. But for notification, individuals would have no way of knowing that automated processing was used in a decision about them.

Right to Be Forgotten (OIPC Recommendation 5)

As noted in our earlier submission, some jurisdictions, including the EU,[45] have implemented rights enabling individuals to require organizations to remove or destroy personal information that is no longer accurate, reliable or legally relevant. In Canada, Quebec Bill 64 will enable individuals to require organizations to do so. Individuals will also be able to require organizations to stop disseminating information about them that is inaccurate, incomplete, or equivocal and, notably, "to de-index any hyperlink attached to [their] name that provides access to the information by a technological means".[46] The Quebec proposal sets out several factors that organizations must consider in assessing a request, creating complex and potentially onerous conditions for organizations and individuals.

The CPPA does not propose a "right to be forgotten" as expressed in the GDPR or Quebec Bill 64 but it does go one step beyond PIPA's present approach to disposal of personal information. PIPA requires an organization to destroy personal information, or render it unidentifiable, "as soon as it is reasonable to assume that…the purpose for which that personal information was collected is no longer being served by" its retention (and retention is not necessary for legal or business purposes).[47] This duty is passive in the sense that an organization must consider and apply that standard, without any explicit right for individuals to require disposal. By contrast, the CPPA will give individuals the express positive right to require an organization to, as soon as feasible, "dispose of personal information that it has collected from the individual".[48]

We agree with the CPPA's creation of a positive right for individuals to require organizations to dispose of their personal information (subject to reasonable exceptions). This could enhance individuals' control over their information in the hands of organizations that no longer have a business or legal reason to retain it. We therefore recommend that the Special Committee recommend enactment of such a right.

Beyond this, we recommend as our earlier submission states, that, rather than amend PIPA to implement a form of the "right to be forgotten", the provincial government should continue to monitor developments, with a view to ensuring that PIPA continues to protect individuals from

[45] GDPR, article 17.
[46] Individuals will also be able to "require that the hyperlink providing access to the information be re-indexed". Quebec Bill 64, section 113.
[47] Section 35.
[48] Section 55(1). This right will be qualified by exceptions similar to those now found in PIPA. We note that this duty only applies to personal information "collected from the individual", which raises the question of whether personal information collected from another source, or personal information the organization has created about the individual, is covered by this provision.

the impact of the use or disclosure of outdated, inaccurate or incomplete personal information (including through indexing by internet search engines).

Right to Data Portability (OIPC Recommendation 6)

We recommended that PIPA should be amended to give individuals a right to obtain a copy of their own personal information from organizations, or to have it sent to another organization, in a format that enables its ongoing use. This recommendation honors the reality that services across a wide range of our daily activities are now delivered electronically and involve large quantities of our personal information.

Privacy laws have long honoured the principle that individuals are entitled to have reasonable control of their own information, including the right of access to that information. Recent legislative efforts to ensure that individuals have reasonable control of their own information have taken the form of a right to obtain that information and, in effect, take it elsewhere.[49] The GDPR does this, for example, by giving individuals the power to obtain their own personal information "in a structured, commonly used and machine-readable format", and to transfer that information to another organization without interference.

The CPPA will introduce a data portability right. An individual will be entitled to require an organization to transfer the individual's personal information to an organization that the individual designates, but only if both organizations "are subject to a data mobility framework" established by regulation.[50] The regulations will stipulate what safeguards must exist to enable secure disclosure and collection of personal information, "parameters for the technical means for ensuring interoperability in respect of the disclosure and collection", specifying organizations that are subject to a data mobility framework, and providing for exceptions, including exceptions related to the protection of proprietary or confidential commercial information.[51]

Our recommendation for PIPA is generally consistent with this CPPA feature. We recommend that PIPA should give individuals the right to obtain their own electronic personal information from an organization in a structured, commonly used, machine-readable format, and at no expense. We also recommend that organizations should have to transfer the personal information to an organization that the individual designates if it is technically feasible to do so without undue cost to the organization. The portability right also should be subject to limits, such as whether transfer is technically feasible, whether the request would interfere with a law enforcement matter or prejudice the legal rights of the organization.

We continue to make this recommendation. As noted in our earlier submission, this right could

[49] This innovation also could, it is reasonable to suggest, help lower barriers to market entry for smaller, newer, electronic service providers, by enabling individuals to transfer their electronic personal information to that new business.
[50] Section 72.
[51] Section 120.

have economic benefits because it can sharpen competition among businesses and may help prevent personal information monopolies from forming. Requiring organizations to provide personal information in a structured, commonly used, and machine-readable format can also promote interoperability. In repeating this recommendation, we acknowledge that the provincial government will likely need to work closely with the federal government to seek harmonization between the CPPA regulations for a data portability framework and PIPA's provisions on this issue.

Administrative Monetary Penalties (OIPC Recommendation 7)

There is little doubt that, if PIPA is to be considered substantially similar to the CPPA, PIPA's enforcement framework will have to be significantly enhanced, including by authorizing the Commissioner to impose monetary penalties on organizations for breaches of the law. CPPA will do this by enabling the imposition of monetary penalties to a maximum of the higher of $10,000,000 or 3% of the previous year's gross global revenues. This important enhancement of the federal regulatory toolkit is shared with the GDPR, the United Kingdom's *Data Protection Act, 2018* and Quebec Bill 64.[52]

As noted in our original submission, PIPA is, plainly stated, largely toothless when it comes to enforcement of British Columbians' privacy rights. In essence, the Commissioner can only sanction serious, flagrant violations of British Columbians' privacy rights solely by ordering organizations to do what the law requires in the first place, i.e., to comply with PIPA's requirements. Yet in most cases the damage will have already been done, rendering an order to obey the law that has already been broken practically speaking moot while creating no real deterrence for other organizations. This is woefully inadequate and not at all reassuring to British Columbians, who expect their privacy rights to be protected through meaningful sanctions.

This Office will always emphasize educational, remedial, approaches to compliance, working with organizations, business groups, civil society, and others to secure compliance by persuasion and education wherever possible. It is clear, however, that there are bad actors out there who do not respect their duty under the law and thus must face significant penalties, where they are absolutely necessary, to sanction and deter breaches of the law. The need for these measures is widely acknowledged, as is illustrated by the fact that several groups that made submissions last year supported this change, including the Insurance Bureau of Canada and Canadian Bankers Association, as well as civil society groups such as the Canadian Civil Liberties Association, BC Civil Liberties Association and BC Freedom of Information and Privacy Association.[53]

However, we do not support the CPPA's approach to monetary penalties, which involves creating a new statutory tribunal, the Personal Information and Data Protection Tribunal. Under

[52] http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html
[53] https://www.leg.bc.ca/parliamentary-business/committees/41stParliament-5thSession-pipa/meetingdocuments

the CPPA, the federal Privacy Commissioner will be able to recommend imposition of monetary penalties to this tribunal, but only the tribunal will be able to impose them.[54] Creation of a new body to discharge this role is unprecedented in the Canadian privacy oversight world and in the EU context.

Without commenting on this policy choice in the federal context, this model absolutely should not be followed in British Columbia. There is no case to be made that such a step is necessary in terms of institutional design or necessity in this province. Further, creation of a new tribunal for the province would introduce unnecessary complexity—and attendant cost, delay and uncertainty—for individuals and organizations alike. It would also impose costs on the public purse, which would have to fund the operation of this new body.

As is noted in our original submission, this Office already has extensive experience administering a monetary penalty scheme, under the *Lobbyists Transparency Act*. In addition to the usual robust judicial oversight that applies to our work, that Act creates procedural fairness safeguards, including a duty to reconsider a penalty when requested. Our experience in this area, and these significant safeguards, are more than adequate to protect the interests of organizations and individuals alike in the administration of a monetary penalty scheme.[55]

Compliance Agreements with Organizations (OIPC Recommendation 8)

Our previous submission recommended that PIPA should be amended to enable the Commissioner to enter into a compliance agreement with an organization on such terms as the Commissioner considers appropriate, with enforcement by the court in cases of non-compliance. As noted in our submission, compliance agreements are widely used compliance tools, offering flexibility in achieving compliance.[56] They would allow us to secure compliance without the expense and delay of a formal investigation and compliance order where that is appropriate in the circumstances.

Parliament recognized this by amending PIPEDA to authorize the federal Privacy Commissioner to enter into compliance agreements, and the CPPA will do the same. We recommend PIPA should follow suit.

[54] The tribunal will also be charged with hearing appeals from certain of the federal commissioner's decisions and orders. Again, this is not suited for British Columbia, as it would introduce unnecessary cost, complexity and delay for organizations and individuals.

[55] As noted in our original submission, other British Columbia agencies also have monetary penalty powers. This includes the Chief Electoral Officer, WorkSafeBC, and the British Columbia Securities Commission.

[56] For example, as noted in our earlier submissions section 83 of the *Workers Compensation Act* authorizes WorkSafeBC to enter into compliance agreements.

Improving Regulatory Information Sharing and Cooperation (OIPC Recommendation 9)

As noted in our earlier submission, personal information knows no borders and effective privacy regulation increasingly depends on information sharing and cooperation, both domestically and internationally. Even organizations that process personal information and only operate in BC are likely to have some element of the processing be outside of BC. The CPPA will carry forward the existing PIPEDA authority for the federal Privacy Commissioner to enter into information-sharing and cooperation agreements with domestic and foreign privacy regulators. This is welcome and should, as recommended in our earlier submission, be a feature of the PIPA amendments.

The CPPA will also enable the federal Privacy Commissioner to enter into cooperation and information sharing arrangements with domestic regulators who have overlapping jurisdiction. This is also desirable in the British Columbia context. As an example, we have in the past worked with other officers of the Legislature—notably the Ombudsperson, Auditor General and Chief Electoral Officers—on investigations involving personal information practices. Explicit authority to engage with these offices—and with other regulators in the province—would better support our work. It would also enhance oversight, and thus the public interest, by bringing complementary areas of expertise to bear on complex, boundary-crossing issues. Last, it could promote efficient use of resources by avoiding multiple review efforts by different agencies.

Our recommendation for such a change to PIPA would better support our activities and would help align PIPA with the federal law.

Enhancing and Clarifying Oversight Powers (OIPC Recommendation 10)

The CPPA will significantly overhaul the federal Privacy Commissioner's enforcement powers, which are relatively weak under PIPEDA. Under PIPEDA, the federal Commissioner has investigation and adjudication functions, but can only issue recommendations to organizations found to have breached that law. Further enforcement requires costly and time-consuming proceedings in the Federal Court of Canada, which creates an access to justice barrier for many individuals. The proposals in the CPPA will strengthen the federal oversight framework.[57]

Similarly, PIPA's oversight framework must be strengthened as we outlined in our earlier submission. Although the PIPA oversight framework is stronger than PIPEDA's, PIPA is, for reasons given in our earlier submission, sorely in need of a complete rewrite on this front. As this Office first observed in detail in its 2008 submission on PIPA reform Parts 10 and 11 of PIPA are confusing, complex and unclear. This unnecessarily hampers organizations' compliance efforts, erects barriers to citizens' understanding and enforcement of their rights, and hinders

[57] An important exception is, as noted earlier, the creation of a new tribunal to enforce monetary penalties and hear appeals from the commissioner's orders. This is not desirable in British Columbia.

flexible and fair enforcement efforts. Again, Parts 10 and 11 of PIPA should be replaced with a scheme of oversight powers substantially the same as those in Parts 4 and 5 of the *Freedom of Information and Protection of Privacy Act*, with the further enhancements outlined in our original submission to you.

CONCLUSION

Economies of the world are interlinked and so too is the flow of personal data that attaches to global trade. As a prolific trading jurisdiction, it is critical that British Columbia ensure that our personal information privacy laws are leading edge, and to the greatest extent possible, harmonized nationally and internationally.

The GDPR, through its adequacy standard, has moved the Canadian government to propose enhanced privacy protection standards which in turn are causing us to do the same so that we maintain substantial similarity with the federal legislation. The recommendations my Office made to the Special Committee in 2020 in many ways foreshadowed what the CPPA now proposes.

PIPA and the CPPA need not be identical, but it is in the interests of economic growth in the province, and citizens' privacy, for our law to be modern, robust, and balanced, while harmonizing with federal law and international developments.

We trust we have equipped you with information you need to assess the CPPA's implications for PIPA reform and in particular the CPPA's positive aspects that merit consideration for British Columbia's law.

PIPA REFORM AND PROPOSED CPPA PROVISIONS

The proposed federal Consumer Privacy Protection Act (CPPA) is a welcome step forward in protecting Canadians' privacy.

Here are 10 major areas covered by CPPA, how they align with OIPC recommendations for PIPA reform, and where we can do even better to protect British Columbians' privacy rights.

1 MANDATORY BREACH NOTIFICATION

Essential, long overdue – CPPA's proposed rules about notifying people in the wake of privacy breaches align with OIPC recommendations.

2 PROTECTING PERSONAL INFORMATION TRANSFERRED TO SERVICE PROVIDERS

CPPA reflects OIPC's view that organizations should be responsible for customer or client personal information after it's been sent to a service provider.

3 MODERNIZING CONSENT REQUIREMENTS

Informed consent and people's right to control their information must be guiding principles. CPPA's consent exceptions are overly broad.

4 AUTOMATED DECISION MAKING

Organizations using automated decision making should notify people of that fact. CPPA's provisions fall short of that requirement.

5 RIGHT TO BE FORGOTTEN

We agree with CPPA's proposal to give people the right to require organizations to dispose of their personal information.

6 RIGHT TO DATA PORTABILITY

The CPPA framework is consistent with OIPC call to give people the right to obtain their own electronic personal information in an accessible manner.

7 ADMINISTRATIVE MONETARY PENALTIES

The CPPA model of imposing fines is long overdue. However, BC should adopt its own model for administering monetary penalties.

8 COMPLIANCE AGREEMENTS WITH ORGANIZATIONS

These agreements are an effective compliance tool for Commissioners. The CPPA will recognize this and PIPA should do the same.

9 IMPROVING REGULATORY INFORMATION SHARING AND COOPERATION

Data knows no borders. PIPA needs reforms similar to CPPA to allow BC's Privacy Commissioner to share information with foreign regulators.

10 ENHANCING/ CLARIFYING OVERSIGHT POWERS

CPPA strengthens regulatory oversight. PIPA's oversight framework must also be strenghtened.