Comments on the Review of Alberta's Personal Information Protection Act

05/31/2024

Submission to the Standing Committee on Resource Stewardship of Alberta

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Introduction

The CBA is pleased to provide comments to the Standing Committee on Resource Stewardship (**Committee**) in their efforts to obtain input on emerging issues relevant to the privacy protection of Albertans, particularly relating to the *Personal Information Protection Act* (**AB PIPA**).

The CBA works on behalf of more than 60 domestic and foreign banks operating in Canada, including several headquartered in Alberta. The CBA advocates for public policies that contribute to a sound, thriving banking system that ensures Canadians, including Albertans, can succeed in their financial goals.

Banks have long been entrusted with significant amounts of their customers' personal information, and protecting the privacy of this information continues to be paramount to maintaining the longstanding trust of their customers. While banks are federally regulated and are governed by the federal *Personal Information Protection and Electronic Documents Act* (**PIPEDA**), substantially similar provincial privacy legislation may apply to any of their provincially regulated subsidiaries. It is in this context that we provide our comments.

The CBA supports measures to harmonize federal and provincial rules and help ensure a consistent approach across Canada to legislating privacy protection in the private sector. Harmonization and interoperability of federal and provincial privacy regimes is an enormous benefit to bank consumers as it enables a familiar and common experience, regardless of their location of residence or whether they are dealing with the bank itself or one of their subsidiaries. We outline further benefits later in our submission.

Given the importance of interoperability and harmonization, we recommend that the Government of Alberta continue to align to federal privacy legislation. As such, we believe it is fundamentally important for the federal process to reach its completion before considering reforms to AB PIPA, to help ensure cross-jurisdictional alignment and harmonization of high-level privacy principles, key definitions, and specific requirements where appropriate.

In this paper, we provide our views on key elements of the Emerging Issues Document (**Document**) released by the Committee given developments relating to federal privacy reform. Our comments are organized in the following manner:

1. **Legislative Approach**
   Jurisdictional Matters
   Interoperability and Harmonization
   Balancing Individual Privacy and Business Needs

2. **Privacy Reform**
   Protection of Sensitive Information
   Consent Exceptions
   Individual Privacy Rights
   Safeguarding Personal Information
   Administrative Monetary Penalties

3. **Regulation of Artificial Intelligence**

1. Legislative Approach

Jurisdictional Matters

The CBA continues to strongly support clear, nonconcurrent jurisdictional boundaries, to help ensure both cross-border data flows and federally regulated businesses are not burdened with duplicative regulatory oversight and potentially different obligations. Information handling of private organizations operating across borders is already subject to federal privacy legislation. We note that the British Columbia *Personal Information Protection Act* (**BC PIPA**) reduces uncertainty with a provision (s. 3(2)(c)) that specifies that BC PIPA does not apply to collection, use and disclosure of personal information that is covered by federal privacy legislation.

Interoperability and Harmonization

In our digital world, many organizations operate across multiple jurisdictions. Harmonization is important to facilitate cross-border operations, increase ease of compliance, enable organizations to provide more consistent products and services, and streamline enforcement and consumer complaint regimes. These

outcomes all drive increased consumer choice and access to innovative products and services, while ensuring consumers' rights in relation to their personal information are effectively and efficiently protected.

Harmonized rules will help ensure interoperability across jurisdictions so that Canadians can benefit from consistent privacy definitions, policies, protections, and regulatory regimes. As trust is a key ingredient to the success of the digital economy, inconsistent privacy requirements across Canada may be a barrier to organizations' ability to build trust; they may lead to unintended consequences such as consumer confusion, misunderstanding of rights, and frustration. In addition, organizations will potentially face increased compliance costs and obstacles to innovation.

While we generally recommend harmonizing to federal privacy requirements set out in the proposed federal privacy reform Bill C-27's *Consumer Privacy Protection Act* (**CPPA**), in limited circumstances, we recommend alignment with provisions set out in Quebec's *Act respecting the protection of personal information in the private sector* (**Quebec Act**).

Balancing Individual Privacy and Business Needs

Some stakeholders are calling for federal and provincial privacy legislation to be grounded with privacy as a human right. While there is currently no formal language regarding privacy as a human right in PIPEDA, BC PIPA or AB PIPA, those privacy statutes have always sought to *balance* the privacy rights of consumers with the need of organizations to manage personal information for reasonable business purposes. At the time of the writing of this document, it seems likely that the CPPA would include a reference to privacy as a fundamental right in its preamble, should Bill C-27 pass.

We understand that some stakeholders are also advocating for the CPPA to further introduce language that would have personal privacy *take precedence* over business needs in all cases. We have serious concerns with such a significant change to the long-time foundation of balance in Canada's privacy frameworks, as it does not a) acknowledge that reasonable and legitimate business purposes do exist and b) it does not set expectations regarding limitations to privacy rights, including those set out as exceptions or alternatives to consent.

Business needs can often reflect other government priorities (e.g., addressing fraud or money laundering) or protect or benefit groups of customers (e.g., through ensuring fair business practices or protecting the vulnerable). A categorical prioritization of one individual's privacy at the expense of other valid and

reasonable needs can provide a weapon or shield to bad actors, enabling them to abuse privacy rights at the expense of protection or benefit to others.

Canadian jurisprudence has commented on the limits of privacy[1], and the Universal Declaration of Human Rights Article 29(2), the European Convention on Human Rights Article 8(2), and section 1 of the Canadian Charter of Rights and Freedoms also include limiting language.

Instead, we believe that the appropriate purposes test set out in the CPPA's s. 12(2) will provide appropriate privacy protections by codifying the legal test Canadian courts currently apply when interpreting subsection 5(3) of PIPEDA (e.g., Turner v. Telus Communications[2]). This test balances the interests of consumers with the needs of an organization by ensuring the following are taken into account:

a) the **sensitivity** of the personal information;
b) whether the purposes represent **legitimate business needs** of the organization;
c) the **effectiveness** of the collection, use or disclosure in meeting the organization's legitimate business needs;
d) whether there are **less intrusive means** of achieving those purposes at a comparable cost and with comparable benefits; and
e) whether the individual's loss of privacy is **proportionate** to the benefits in light of the measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.

2. Privacy Reform

Protection of Sensitive Personal Information

Should provisions be added to AB PIPA to further protect potentially sensitive information? If so, for which information?

The sensitivity of data can be highly circumstantial; for example, any personal information may be sensitive if linked to an organization or use that may lead to reputational damage to an individual.

[1] "Like all Charter rights, the s. 8 right to privacy is not absolute — instead, the Charter protects a reasonable expectation of privacy." R. v. Gomboc, [2010] 3 S.C.R. 211, at 17.
[2] *Turner v. Telus Communications Inc*. 2005 FC 1601 (CanLII) | Turner v. Telus Communications Inc. | CanLII

Conversely, in the Supreme Court of Canada's decision in *Royal Bank of Canada v. Trang,*[3] certain information typically considered sensitive was determined to be less sensitive. The Court determined that the sensitivity of financial information must be assessed in the context of the situation, which can be influenced by numerous factors such as, but not limited to, the intended purpose, information already in the public domain, nature of relationships, and impact to other parties. While there may generally be a higher set of expectations for the handling of sensitive personal information (e.g., express consent, higher safeguards), it is still important to accommodate some flexibility depending on the situation (e.g., it is unlikely bad actors would provide express consent for monitoring of sensitive personal information for ongoing fraud detection).

Ultimately, we believe that a definition or definitive categorical list of "sensitive information" would continue to be more appropriately addressed through regulatory guidance. If a legislative definition is required, we recommend that the definition acknowledge the contextual nature of determining sensitivity and use a principles-based approach that does not provide a prescriptive list of information types that could be unnecessarily inflexible and lead to unintended impacts to standard industry practices, customers, and organizations. Quebec's private sector privacy legislation includes a contextual definition of sensitive personal information.

Should provisions be added for biometric information?

We believe that the principles-based nature of AB PIPA permits a risk-based approach that sufficiently accommodates the appropriate protection of biometric information. As a result, we recommend that any further need for clarity could be addressed through regulatory guidance.

Any definition of biometrics should be appropriately scoped to focus on biological, unique, and immutable behaviours and/or characteristics. There should be clear acknowledgment that behaviour patterns that are not unique nor biological in nature (e.g., spending patterns) are clearly out of scope.

Any guidance or requirements should be principles-based and scalable to level of identifiability and risk. To elaborate, there is a very wide range of biometric characteristics that may rank very differently on an identification or risk sensitivity spectrum depending on the circumstances and controls and safeguards in place. For example, an organization may merely monitor keystroke patterns to assess whether a human is entering information in an online form versus an automated bot or script attempting to impersonate someone, conduct fraud or clog the system – this involves no identification and no matching to an

[3] *Royal Bank of Canada v. Trang,* Royal Bank of Canada v. Trang - SCC Cases (scc-csc.ca)

individual. Conversely, another organization may monitor keystroke patterns to assess whether the person who seeks to gain access is, in fact, the person to whom the credentials belong (potentially in combination with other security layers) – this involves identification and matching to an individual on file.

Any provisions or guidance should acknowledge that there can be valid reasons for consumers to choose to benefit from products or services that leverage biometrics (e.g., choosing facial or thumbprint access for a device), and there are scenarios where organizations are encouraged or required by other regulators to implement biometrics.

Provisions or guidance should also contemplate that the collection and use of certain biometric information may be integral and essential for certain legitimate purposes and as a result require different treatment. For example, know your customer requirements and fraud detection and prevention are integral parts of providing financial services to customers across all channels (e.g., branch, online, mobile or telephone) and the collection and use of behavioural patterns and, in some cases, non-immutable biometrics, are increasingly critical elements of these activities. Guidance or provisions that require express consent or prohibit retention do not make sense in these contexts.

Should provisions be added to enhance the protection of children's personal information?

Should provisions be added to enhance the protection of children's personal information, we urge that the scope of the provision be highly targeted to address the right risks (e.g., online harm, reputational risk), with care taken so that the products, services and activities of organizations *not* targeting children are not unduly impacted.

Consent Exceptions

Are the provisions in AB PIPA dealing with forms of consent and the conditions attached to their use appropriate?

We propose that in addition to retaining existing exceptions to consent, lawmakers incorporate additional exceptions to consent that are outlined in Bill C-27's CPPA, to promote harmonization and interoperability. The introduction of targeted exceptions to consent would help organizations meet their regulatory obligations and achieve objectives that benefit Canadians. For example, organizations may be required to provide personal information to support a federal or provincial beneficial ownership registry.

In addition, the inclusion of fraud, investigation and anti-money laundering exceptions to consent would help organizations combat financial crime that impact Albertans and the Albertan economy. PIPEDA (and

the CPPA) currently includes exceptions to obtaining an individual's consent for an organization to share personal information with another organization in order to conduct investigations and prevent, detect and suppress fraud, subject to certain conditions. Additionally, the federal government is poised to update federal privacy and anti-money laundering legislation to enable certain organizations to share personal information with each other to detect and deter money laundering, terrorist financing and sanctions evasion in a privacy protective way.[4] These amendments will include a safe harbour to limit criminal and civil risks for good faith use of these provisions to remove barriers to information sharing. Appropriate exceptions may also be warranted for organizations to share such information with federal or provincial government agencies.

Aligning Alberta's exceptions to consent with the federal approach will help to protect Albertans, ensuring private sector organizations can continue to proactively combat fraud and other financial crimes. If alignment is not pursued, Alberta risks becoming an outlier in Canada – a jurisdiction that fraudsters and money launders target, understanding that they can easily avoid detection in the absence of legislative protections. The *Commission of Inquiry into Money Laundering in British Columbia* (Cullen Commission Report)[5] is an excellent resource for understanding the scope and nature of financial crime at a provincial level. We would be pleased to provide more information on this topic should the Committee require.

Individual Privacy Rights

Should AB PIPA include other protections for individual information, such as an individual's right to be forgotten or de-indexed?

Most existing Canadian privacy legislation (e.g., PIPEDA, AB PIPA and BC PIPA) already incorporate a strong accountability obligation for any information organizations collect or use, a requirement for organizations to retain any personal information only as long as required to fulfill the intended purposes, and complaint mechanisms should a consumer have concerns.

As a result of these existing Canadian requirements, should additional protections be required, they should be limited to address the unique risks pertaining to online platforms, by focusing on de-indexing or

[4] The *Notice of Ways and Means Motion to introduce a bill entitled An Act to implement certain provisions of the budget tabled in Parliament on April 16, 2024* includes provisions, to be set out in the federal Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), that would permit certain regulated entities to exchange personal information with each other, with safe harbour protection for good faith compliance to Codes of Practice. Both AML and privacy regulators would have an oversight role relating to the Codes, with regulations providing more detail. There would be a consequential amendment to federal privacy legislation for a provision that would permit this sharing, pointing to the AML legislation.

[5] Refer to recommendations 48 and 49 in the Commission of Inquiry into Money Laundering in British Columbia (cullencommission.ca)

removal of personal information from online sources, where there may be reputational risk to individuals. We note that the Quebec Act adopted a very targeted approach to focus on de-indexing and ceasing dissemination of online information upon request, while relying on general retention and disposal requirements in all other situations.

Upon an individual's request, should organizations be required to transfer that individual's digital personal information to another organization in a structured, commonly used, and machine-readable format when it is technically feasible (data portability)?

Data portability rights can lead to potential risks such as those relating to consumer protection, security, and confidentiality, as the data provider would not have any ability to assess or manage the risk associated with the data recipient. When a customer directs an organization to release their personal information to themselves or to another organization of the customer's choosing due to a general data portability right, it should be clear that the organization releasing the information is no longer accountable for the privacy and security of the information upon release. In addition, the organization releasing the information must not be held accountable for assessing risks associated with the recipient organization on behalf of the customer (e.g., levels of safeguards including cybersecurity practices, or any potential differences in jurisdictional privacy obligations for the data recipient), as the customer is ordering release of the information.

In particular, a data portability right should not override the privacy protections being developed for the federal Consumer-Driven Banking (**CDB**) framework. The CDB framework participants are meant to meet certain common accreditation and safeguarding standards designed to appropriately manage the sharing of financial information. The movement of very sensitive personal and confidential information should be handled under applicable standards to help ensure that personal information is managed securely and effectively, and consumer choice is not limited only to choices within their own province.

Careful consideration must be given to any data that will be subject to a data portability requirement. Such a right should be limited to information collected from the individual, and explicitly exclude derived or inferred data, as these could provide an unfair competitive advantage to recipient organizations, with no clear benefit to consumers. The Quebec Act's data portability right will exclude created (derived) and inferred data.

Should organizations be required to provide individuals with the logic involved in automated decision making about that individual (algorithmic transparency)?

We recommend that the right to algorithmic transparency in privacy legislation be limited to a providing a general explanation of an automated decision, which may include the type of personal information that was used to make the decision, the source of the information, and the reasons or principal factors that led to the prediction, recommendation or decision.an explanation. This would be consistent with federal policy intent as proposed in the CPPA and would avoid overlap with separate transparency requirements targeted at regulating artificial intelligence (please refer to section 3 for our comments on Regulation of Artificial Intelligence).

In addition, the right should be limited to scenarios where a) the decision is exclusively automated (without a meaningful "human in the loop") and b) where the decision may have a significant impact on an individual. As part of clause-by-clause review of Bill C-27's CPPA, a federal definition of significant impact will be prescribed; we recommend harmonization. Without these thresholds, requiring explanations upon request may result in numerous requests with minimal consumer benefits, set an unreasonable expectation for what consumers can demand of organizations, and enable nuisance requests or embolden those who may engage in fishing for competitive intelligence.

We also suggest introducing the possibility for regulations to clarify the nature, scope and limits of explanations relating to automated decision making systems, as unforeseen issues may arise due to the unique and novel nature of this transparency requirement (e.g., volumes of complaints, technical challenges).

Several recent decisions at the federal level[6] have resulted in providing individuals access to information that organizations would historically have considered confidential, and an inclusion of strong rights-based provisions without balance or limits (as discussed in an earlier section) could lead to other confidential information being required to be shared. There is a concern that anything beyond generally worded explanations will need to include a level of detail about decision processing rules that may divulge information that may impact an organization's competitiveness or may provide information on fraud detection or prevention systems to bad actors who may seek to circumvent them. It is important to include clear exceptions to providing any proprietary or confidential commercial information as part of decision explanations, particularly for systems that manage risk (e.g., fraud detection).

[6] *Bertucci v. Royal Bank* Bertucci v. Royal Bank of Canada - Federal Court (fct-cf.gc.ca) and *An insurance company's internal ombudsman office is not a "formal dispute resolution process" under PIPEDA* PIPEDA Report of Findings #2016-006: An insurance company's internal ombudsman office is not a "formal dispute resolution process" under PIPEDA - Office of the Privacy Commissioner of Canada

Safeguarding Personal Information

Should AB PIPA regulate the de-identification and/or anonymization of personal information within the control of an organization and the subsequent use or disclosure of the de-identified or anonymized information? If so, how?

Should Alberta choose to regulate de-identification and anonymization of personal information, interoperability of terms and concepts with other Canadian jurisdictions should be a paramount consideration. If provinces choose to set out definitions and provisions different than those set out federally, Canadian organizations are likely to find it difficult to comply with all approaches. A key element of a definition of whether information has been anonymized is whether it is *reasonable in the circumstances* that an individual could be re-identified. For example, there are substantially different potential risks between whether anonymized information should be made public or should be securely retained within the accountability of the organization for its own purposes. We recommend exploring the views of the Canadian Anonymization Network (CANON)[7] with regards to anonymization and de-identification in a privacy context.

Another key consideration is how the government would plan to regulate personal information after it has been anonymized. Once personal information has been sufficiently anonymized, it ceases to be personal information and would be outside of the scope of AB PIPA's applicability.

Should organizations be required to have a privacy management program and provide written information about the program to individuals and the Commissioner?

Many organizations share a privacy policy on their websites already; any new formal requirement should leverage this existing practice. A requirement to proactively provide written information should be limited to answering questions on an as needed basis to reduce unnecessary administrative burden for organizations and the regulator.

Should organizations be required to complete and submit a privacy impact assessment to the Commissioner for specific initiatives involving personal information?

We believe privacy impact assessments (PIAs) are helpful, best practice tools to assist organizations in meeting their comprehensive compliance obligations, but they are not necessary as a legal requirement. Doing so would most impact small and medium sized enterprises. Should lawmakers determine they are

[7] CANON-Proposed-Amendments-to-Bill-C-27-re-De-identify-and-Anonymize-May-24-2023.pdf (deidentify.ca)

necessary, the legislation should focus on higher level principles to provide flexibility to the requirements that consider the situation, and set a materiality threshold to reduce unnecessary burden on organizations that may deal with less sensitive information or less complex data flows, processes or systems.

Under current principles-based privacy legislation, organizations are already accountable for complying with all privacy requirements and for scaling their efforts (e.g., form of consent, safeguarding) to the sensitivity of the personal information involved. Large Canadian organizations typically already have privacy management policies, processes and employee training in place to manage compliance. Many of these organizations also already incorporate best practices relating to PIAs. As customer trust is critical for many organizations, the reputational and legal risks associated with a potential privacy breach have been strong motivators for managing privacy risk, especially with the introduction of notification requirements to regulators and impacted individuals.

We advise against a requirement to submit PIAs to the Commissioner, even for specific initiatives. We are not aware of any other jurisdiction that has such a privacy sector requirement. This could be particularly burdensome for small and medium-sized businesses. Depending on the expectations of the Commissioner's role, this could lead to a very resource-intensive process that could result in significant delays and could dampen innovation. Further, PIAs can contain a lot of confidential information and there may be concerns that the information may be subject to access to information requests of the Commissioner, or even data breaches within the Commissioner's Office.

Administrative Monetary Penalties

Should AB PIPA include the ability of the Commissioner to levy administrative monetary penalties against an organization for certain contraventions of the Act?

We understand that in today's privacy environment, privacy oversight bodies are seeking enhancements to their enforcement and oversight powers. We suggest that any new or expanded enforcement powers be accompanied with guardrails that reflect, at a minimum, the principles of natural justice and procedural fairness. Examples of appropriate guardrails include safeguards such as ensuring organizations subject to an enforcement action are provided the right to understand the allegations, the right to be heard and retain counsel, the right to written reasons, and the right to an impartial hearing and appeals process. These guardrails are critical in the Canadian context where legislation is principles-based and proportionate, where different stakeholders may come to a different interpretation of how a particular provision should be applied.

We support including a due diligence defense for a penalty, as it may encourage and incentivize organizations to create and maintain a robust privacy management program and will also help ensure that harsh penalties are reserved for those organizations who do not take their privacy obligations seriously.

We believe the CPPA's provisions for Codes of Practice and Certification Programs have the potential to help reduce this type of uncertainty for organizations and boost consumer confidence in the associated privacy protections. The Codes of Practice can set out key common requirements in a particular sector or type of activity, which cannot be achieved directly in legislation that needs to be sector- and activity agnostic. A key element of this approach that helps to reduce uncertainty is that penalties would not apply if the program had been reviewed and approved by the federal Office of the Privacy Commissioner of Canada and the organization had been following the approved requirements. To further reduce uncertainty, we recommend that provinces support the federal Code framework by exempting fines and penalties for good faith compliance to those Codes, as they would be based on substantially similar principles and have the potential to build consumer trust in many potential typical business activities. This would also promote harmonization and interoperability.

Formal coordination between provincial and federal privacy commissioners and associated processes (e.g., appeals) will be key to manage issues involving more than one jurisdiction that may lead to potential fines and penalties. Without such coordination, there is a risk that an organization may be subject to cumulative penalties that collectively may be unreasonable for an individual incident, or to a series of disparate or contradicting orders that are challenging to implement and unworkable for business operations.

3. Regulation of Artificial Intelligence

Should AB PIPA include a framework to regulate the design, development, and/or use of artificial intelligence systems within Alberta? If so, what should be included?

The CBA is aligned with policy objectives that aim to promote the responsible development and use of AI systems (**AIS**) in a manner that supports existing principles under Canadian law and consistent with the Organisation for Economic Co-operation and Development's (**OECD's**) AI principles.

We recommend that any law seeking to regulate AIS be kept separate from privacy legislation, as regulation of AIS typically goes far beyond the handling of personal information, to include handling of non-personal information and to address different and broader types of risks (e.g., data quality,

representativeness). This would be consistent with the approach taken in other G7 jurisdictions. In addition, we recommend that any provincial AIS law be aligned with any federal AI legislation, such as the federal Bill C-27's *Artificial Intelligence and Data Act* (AIDA), to avoid the potential for regulatory fragmentation, overlap or conflict.

In a rapidly evolving field like AI, we believe a flexible, risk-based targeted regulatory AI framework is necessary to help ensure Canadian organizations can serve consumers in a manner that fosters confidence and builds trust in the responsible development, deployment, and use of AIS. For this reason, it is important that provincial efforts intended to protect individuals from the potential harms of AI systems remain principles-based, outcomes-focused and focus on gaps not addressed by a federal framework.

We note that the Canadian federal and provincial privacy Commissioners have released Principles for responsible, trustworthy and privacy-protective generative AI technologies; it is our observation that these principles go beyond the scope of the federal AIDA and are highly prescriptive. Any guidance should provide clarity of definitions of key terms (e.g., definitions for developer or deployer) and ensure that provisions do not offer overlapping or conflicting advice.

While it is best for provinces to consider a focus on addressing regulatory gaps and avoid designing legislation that overlaps or conflicts with existing or proposed legislation, harmonization of legislative requirements will be paramount in instances where overlap cannot be avoided, particularly since many of the issues may be already addressed in other regulations. Should the government see value in moving ahead, it is, for example, important to align with guidance that is being developed by financial market regulators such as the Canadian Investment Regulatory Organization, who will be consulting on AI and Machine Learning, with a view of providing guidance.