IBC · BAC
Insurance Bureau of Canada
Bureau d'assurance du Canada

May 31, 2024

Sent by e-mail: RSCommittee.Admin@assembly.ab.ca

Standing Committee on Resource Stewardship
c/o Committee Clerk
3rd Floor, 9820 – 107 Street NW
Edmonton, Alberta
T5K 1E7

To Committee Clerk,

Re: Review of the *Personal Information Protection Act*

On behalf of Insurance Bureau of Canada (IBC) and its members, we would like to provide you with our written submission on themes and questions raised in "Emerging Issues: The *Personal Information Protection Act*" (the "Consultation Paper") released in May 2024.

IBC and its members continue to support the purpose of the Alberta Personal Information Protection Act ("PIPA") and its privacy principles. Property and casualty ("P&C") insurers have long appreciated the need to protect the personal information of their customers and other individuals with whom they deal in the course of underwriting risks and handling insurance claims. IBC and its members were active participants in the Alberta government's consultations in the development of PIPA and will continue to participate actively in consultations on this important law.

Insurance Bureau of Canada and its Members

IBC is the national industry association representing Canada's private home, car and business insurers. Its member companies make up the vast majority of the P&C insurance market in Canada. Since 1964, IBC has worked with governments and regulators across the country to help make affordable home, auto and business insurance available to all Canadians.

The P&C insurance industry plays an important role in underwriting economic and financial risks for Canadians and businesses. Insurance is an enabling sector that supports new ventures that contribute to the country's prosperity. In today's modern digital global economy, insurers use data to accurately underwrite, price risk, incentivize risk reduction, create operational efficiencies, facilitate better claims processing, and more, including efforts to manage the impact of climate change. IBC and its members welcome this opportunity to comment on this important PIPA review to ensure that Alberta is well-equipped to participate in a data-driven, digital global marketplace.

Comments

This written submission addresses the questions raised in the sequence and under the headings set out in the Consultation Paper.

2.0. The Changing Legislative Landscape in Canada and Internationally

1. Are there specific amendments needed to harmonize PIPA with other jurisdictions to make it easier for businesses to operate in all jurisdictions?

Due to the reality of data flows, need for future proofing and interoperability, it is essential that PIPA maintain a legal framework that is based on principles, technology neutrality, transparency and accountability, supported by regulatory guidance as required. Flexibility is key to ensuring that the legislation remains suitable in the long run and the reason why the federal Personal Information Protection and Electronic Documents Act ("PIPEDA"), which is a principles-based legislation, has adapted so well to changing technology over the years. Further, it is critically important that there is consistency between the different federal and provincial private sector privacy laws. It is understood that there will be differences between the laws to accommodate the concerns in specific jurisdictions, but as much as is possible, the intent, wording and implementation of the laws should be substantially similar. To do otherwise is to invite confusion for citizens and organizations, resulting in a less efficient and effective framework for the protection of personal information.

Specific proposed amendments are outlined in our responses below.

2. Are there specific amendments to PIPA needed to modernize the Act for relevant businesses and organizations to conduct business in Alberta?

Having a current, adequate and up-to-date privacy law is critical to the development of a robust digital economy that will stimulate innovation by organizations and provide direct benefits to consumers. Amendments to PIPA to harmonize PIPA with federal and other provincial private sector privacy legislation should guide the modernization work. In addition to the specific amendments set out in our responses to the consultation questions below, amendments to facilitate fraud detection, suppression and prevention is needed.

We note that the federal government recently released a National Action Plan on Combatting Auto Theft that outlines actions focused on disrupting, dismantling and prosecuting the organized criminal groups behind auto theft. Among the proposals is funding to help the Canada Border Services Agency ("CBSA") strengthen intelligence-sharing with Canadian and international law enforcement partners to help identify individuals involved in the stolen vehicle supply chain and support work of the police of jurisdiction to apprehend perpetrators of auto theft. The CBSA is also using advanced data analytics with respect to stolen vehicles to target exporters, shippers ad cargo containers to disrupt the flow of stolen vehicles from Canada. It is clear that the federal government recognizes the value of information sharing and advanced data analytics in combatting organized criminal groups behind crimes such as auto theft.

The insurance industry is particularly affected by fraud which has serious consequences for all policyholders because of its impact on premiums. The detection, suppression and prevention of insurance fraud is a priority issue for the insurance industry. Insurance fraud is an area where the ability for insurers to collect, use, disclose and pool data for the limited purposes of detecting, suppressing and preventing fraud could go a long way in

helping to combat insurance fraud. Security experts recognize the inherent value of sharing information to combat fraud and cybercrime. Prevention must be at the heart of any anti-fraud strategy. PIPA needs to be flexible enough to allow insurers to develop and use legitimate tools to detect, suppress and prevent insurance fraud, to the benefit of all Albertans.

PIPA currently only includes an exception to disclose without consent for the purposes of protecting against, or for the prevention, detection, or suppression of fraud. For clarity, we recommend amending PIPA to explicitly include an exception to also collect and use without consent for the same purposes. Further, the exception to collect, use and disclose without consent for the purpose of fraud prevention, detection or suppression should be expanded to all organizations that have a legitimate need for this limited purpose instead of being restricted to the current list of organizations in section 20(n).

3.0 Artificial Intelligence

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

IBC and our members support the need to maintain the right balance between ensuring a proper use of artificial intelligence ("AI") and the need to use AI to innovate and remain competitive, which would benefit customers.

However, in order to maintain harmonization with federal and other provincial private sector privacy legislation, PIPA should remain technology agnostic. Federal Bill C-27, which would replace PIPEDA with the new *Consumer Privacy Protection Act* ("CPPA"), also addresses the design, development and deployment of artificial intelligence systems in separate proposed legislation, the *Artificial Intelligence and Data Act* ("AIDA").

Accordingly, IBC recommends waiting for the adoption of AIDA and a federal solution. The design, development and deployment of AI is generally not contained within the borders of a province and it would be difficult for companies that operate across Canada to innovate while complying with various provincial AI frameworks.

4.0 Application

1. Should all non-profit organizations be fully subject to PIPA for all their activities?

IBC supports the application of privacy obligations on all organizations that collect, use, disclose and retain personal information. We understand that many jurisdictions have a separate privacy-related legislation to govern political parties and/or not-for profit organizations. While it is our view that there should be privacy-related legislation that apply to these entities, we have no preference as to whether it is PIPA or other legislation.

2. Should PIPA apply to political parties?

Same comment as above.

5.0 Protection of Sensitive Personal Information

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

There is no need to add specific provisions to further protect sensitive information. However, IBC and our members support the general principle that the protection of personal information should take into consideration the sensitivity of the information, including the requirement to obtain express consent when collecting sensitive personal information. This principle is consistent with existing expectations under PIPEDA and Quebec private sector privacy law.

If PIPA is revised to include a definition of sensitive information, the revised definition should harmonize, to the extent possible, with existing legislation or guidance. In order to maintain a principles-based framework and remain consistent with existing guidance issued by the Office of the Privacy Commissioner of Canada ("OPC"), sensitive information should be defined in manner that takes into account context.

For example, the OPC proposed the following definition as part of former Bill C-11:

Sensitive information means personal information for which an individual has a heightened expectation of privacy, or for which collection, use or disclosure creates a heightened risk of harm to the individual. This may include, but is not limited to, information revealing racial or ethnic origin, gender identity, sexual orientation, political opinions, or religious or philosophical beliefs; genetic information; biometric information for the purpose of uniquely identifying an individual; financial information; information concerning health; or information revealing an individual's geolocation.

Should provisions be added for biometric information?

There is no need for specific provisions for biometric information. As above, the addition of biometric information could be included the definition of sensitive information.

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

When an organization requires the personal information of children to offer or provide products or services to them, it will be difficult for these organizations to operationalize different expectations specific to children's personal information. PIPA already prohibits an organization from, as a condition of supplying a product or service, requiring an individual to consent to the collection, use and disclosure of personal information beyond what is necessary to provide the product or service.

However, defining a minimum age at which a minor can give consent to the collection, use and disclosure of their personal information could be helpful. Consideration should be given to align with the age that a minor can enter into contracts for necessaries.

6.0 Consent Requirements

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

All private sector privacy laws in Canada operate on a consent model in which the individual is asked to consent to the collection, use and disclosure of their personal information for specified purposes. The privacy laws provide for exceptions in limited circumstances when consent is not required from the individual, such as investigating an instance of suspected fraud or complying with laws.

PIPA's consent model works, but there are situations in which a consumer's consent is not a primary consideration; for example, an organization's obligation to adhere to laws or where a consumer cannot practically give meaningful consent (for example, the use of one of a myriad of third-party vendors), or where explicit consent is not practicable (for example, to collect, analyze, use and disclose personal information for the purposes of detecting, suppressing and preventing insurance fraud). In addition, the concept of deemed consent is unique to PIPA and consideration should be given to replace deemed consent in PIPA with clearly defined exceptions to the requirement for express consent. This approach would better align PIPA with the reasonable and practical approach taken in Federal Bill C-27 in which there are defined exceptions to the requirement for consent, including a list of defined "business activities."

2. Should individuals receive notice in plain language when organizations explain the purposes for which personal information is collected, used or disclosed?

Privacy legislation requires organizations to be open to individuals in how they collect, use and disclose the individual's personal information. This has led, in some cases, to organizations developing lengthy and complicated privacy statements and policies which can lead to consent fatigue that may cause consumers to rush through consent choices regardless of whether it is in plain language or not.

While agreeing that privacy policies and consent language need to be written so that they can be understood by individuals, there are a number of factors to be considered, such as the nature of the activity in question. As such, a prescriptive list of required disclosures may not necessarily enhance privacy protections. For example, the privacy statement or consent language regarding a one-time purchase of a chair is very different than that of an ongoing financial or insurance relationship with the individual. It is not just using plain language that should be considered but also providing the right amount and type of information in the organization's privacy statement or consent language that are appropriate to the circumstances. It should be noted that the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioner of Alberta and British Columbia jointly issued a guidance document for obtaining meaningful consent in May 2018. Any PIPA requirements introduced must be harmonized with PIPEDA. Further, while organizations are open and transparent in their fair information practices, they should not be expected to disclose commercially sensitive information.

With respect to the use of automated decision systems, IBC supports expressly providing organizations, not the consumer, with the right to determine the appropriate level of disclosure necessary to comply with transparency obligations (with potential avenues for individuals to object or submit complaints to the regulator). Further, business considerations such as company intellectual property and confidential information protection should

be included in any proposed legislation as a valid consideration when businesses are determining what information to disclose.

7.0 Individual Rights that are Not Included under PIPA

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

IBC supports an individual's right to have control over their own information. On the other hand, businesses including insurance companies have a legitimate need to retain information to provide products and services, including to appropriately rate and underwrite insurance policies, comply with legal requirements, and detect and prevent fraud. To this end, companies develop retention schedules based on the length of time information is needed for the purpose it was collected and have processes in place to delete records once the retention period has expired.

While respecting an individual's right to control their own information, there is also a need to avoid unanticipated consequences resulting from a deletion request, such as the unintended enabling of fraud and the deletion of records of business activities or claims records. The deletion of this information would result in the inability to furnish evidence to respond to litigation or erode the ability of an insurer to build adequate models for rating, underwriting, and loss prevention through accurate reporting and analysis. IBC recommends that there should be appropriate exceptions to the right to require deletion including limiting this right to personal information provided by the individual. Further, there should be an exception to the right of deletion in circumstances where the information relates to the reasons set out above, including legitimately needed to provide the produce or service (e.g., accurately set rates or underwrite insurance), for fraud detection or prevention, or for claims investigation purposes. The absence of an exception could severely undermine the legitimate efforts deployed by insurers and the insurance industry to prevent, suppress and detect fraud. Patterns of fraud are often detectable only after the passage of time. It is possible that an insured or third party claimant, who might have reason to believe that their fraudulent activities are under suspicion by the insurer or police, would be able to have any potential evidence against them disposed of, by simply exercising their rights for the deletion of their personal information.

2. 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 is used in the P&C insurance industry to enable underwriting, rating, pricing, marketing and claims handling. It also provides a consumer experience that is tailored to their needs and risk profiles.

Any discussion on data portability within the context of the P&C insurance industry, must recognize the organizations' proprietary interest in derived data. With innovative products, such as usage-based insurance, a clear divide must be made between the personal information provided by the consumer, such as their name, contact details and claims history, and the derived data that is created from that information by the insurer, such as that individual's risk profile. The personal information provided by the individual, would fall under data portability, but the derived information would fall under an organization's propriety interest and would not be portable. This is key for insurers because they need to ensure that they can continue to invest in innovative tools

for the benefit of the customers without being at risk of their confidential commercial information being disclosed to a third party via data portability requests.

Furthermore, although data portability provides certain advantages to both consumers and businesses, it comes with inherent risks to consumer protection, privacy and confidentiality, and cyber security, and it also risks decreasing innovation and competition.

IBC recommends waiting to align with the approach that will be taken under the CPPA as it will be difficult for companies to comply with a variety or provincial transfer requirements. There have been significant challenges in implementing data portability in other jurisdictions. As such, for the purpose of ensuring harmonization and reduce compliance burden, IBC recommends that PIPA not be revised to include data portability until the implementation challenges have been adequately addressed. For example, Quebec private sector privacy law has shown that data portability is only feasible if a corresponding regulatory framework is in place that achieves:

i. verification and registration of organizations that wish to receive personal information via portability transfers – including registered coordinates at which registered organizations can be contacted to facilitate transfers;

ii. minimum security standards and technological standards regarding transfers and formats;

iii. mandatory measures for identification of the individual submitting the request and a significant period of time for the organization to complete identity verification of the individual, the recipient, and to receive guidance from the regulator if necessary;

iv. clarity regarding apportioning of liability in the event of a breach at the recipient or in transit, or any circumstance in which a third party is able to meet the regulatory standards for verification of the requesting individual or the recipient of the transfer resulting in a breach; and

v. clarity regarding the scope of the information that is subject to such a request – for example, protected intellectual property and trade secrets of the organization receiving the request must not be subject to such a request, nor should information that would permit the recipient organization to reverse-engineer protected IP and trade secrets.

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

A consumer's right to access information regarding automated decision-making processes must be balanced with an organization's interest in safeguarding its confidential commercial information. This right to access should not apply to systems used only to make predictions and recommendations, but rather, should apply only to automated decision systems that would be used to make a decision without any human assistance that has a material impact on the individual.

P&C insurers in Canada operate in a heavily regulated and highly competitive environment. In many circumstances, an insurer's competitive advantage is based on its proprietary algorithmic decision-making programs. There need to be limits on what must be disclosed and how much detail will have to be provided by an organization. For example, transparency should not include disclosing the details of fraud detection analytics,

as doing so would undermine the effectiveness of such tools. Accordingly, while it may be appropriate to provide consumers with broad explanations of which factors were used in the algorithmic decision-making programs, PIPA should not require the disclosure of the specific process behind the automated decision.

8.0 Safeguarding Personal Information

1. Should 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?

IBC and its members support the existing approach under PIPEDA and Canadian case law which defines personal information as information about an identifiable individual or is reasonably capable of identifying an individual either alone or when combined with other available sources of information. Under this approach, information that has been de-identified by removing or replacing direct identifiers from a data set and which can subsequently be re-identified would be considered personal information while fully anonymized information which cannot reasonably be re-identified would be outside the scope of privacy legislation. In our view, the definitions and standards for terms such as "de-identified" and "anonymized" require consistency across federal and provincial privacy legislation. This will support continued development of innovative solutions by Canadian organizations and will avoid creation of a patchwork system wherein certain provinces include diverging restrictive requirements on de-identified and/or anonymized data.

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

IBC supports a principles based and proportionate approach that includes a materiality threshold with respect to privacy management programs and PIAs. Section 6(1) of PIPA currently requires an organization to develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act. Further, section 6(3) of PIPA currently requires organizations to make written information about their policies and practices available on request. In our view, a guidance document issued by the regulator that incorporates a principles based and materiality approach instead of prescriptive legislative requirements would be more effective.

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

Same comment as above. In the event that an organization determines that a privacy impact assessment (PIA) is needed for an initiative that involves the collection, use or disclosure of personal information and completes a PIA, the organization should be not required to submit the PIA to the Commissioner. The resulting volume of submissions to the Commissioner from such a process would stifle innovation in the province. It would also be difficult for organizations that operate across Canada to comply if there are provincial variations in PIA related requirements. In addition, there would be concern that competitors with operations outside of Alberta could conduct research on their competitor's products by accessing their competitor's submitted PIAs.

9.0 Breach Notification

Are the provisions for notification of breaches to the Commissioner and individuals under PIPA appropriate?

The existing breach notification provisions in PIPA are adequate and appropriate. With the exception of other privacy legislation requiring that impacted consumers be notified at the same time as the Commissioner, PIPA breach notification provisions generally align with the other federal and provincial private sector privacy legislation. In order to minimize compliance burden on businesses that operate across Canada and ensure that limited resources are focused on containing the incident and reducing harm, IBC supports harmonizing incident reporting requirements across Canada.

10. Administrative Monetary Penalty

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

Regulators increasingly use administrative monetary penalties (AMPs) to enforce compliance with their regulatory regimes. However, we contend that using AMPs as a deterrent rather than as a means of punitive penalty would be more effective and more consistent with the overall Canadian legislative framework. There should be reasonable maximum amounts for AMPs that are proportionate to the infraction. It is also important to avoid levying AMPs in different provinces for the same privacy incident. Data may flow from one province to another, and it would be unreasonable to have multiple AMPs levied against an organization for the same incident. In this regard, there should be a coordinated approach by the privacy regulators across the country.

Conclusion

IBC's member companies are strongly committed to protecting the personal information of their customers and other individuals with whom they deal. We would be pleased to answer any questions that the Standing Committee might have regarding our comments and recommendations in this submission.

Aaron Sutherland,
Vice-President, Western
Insurance Bureau of Canada