Office of the Deputy Minister
29th flr, ATB Place, South Tower
10020 – 100 Street
Edmonton, Alberta T5J 0N3
Canada
www.alberta.ca/technology-and-innovation.aspx

AR11315

Garth Rowswell, MLA
Chair, Standing Committee on Resource Stewardship
c/o RSCommittee.Admin@assembly.ab.ca

Dear MLA Rowswell:

On behalf of the Ministry of Technology and Innovation, I want to thank you for the opportunity for department officials to provide a technical briefing on the *Personal Information Protection Act* (PIPA) to the Standing Committee on Resource Stewardship on April 25, 2024. We are also pleased to provide a written submission for the Committee to consider in its review of PIPA.

Technology and Innovation is committed to fostering robust privacy legislation that balances individual rights with technological advancements. The digital age poses new challenges to both the business needs of organizations and the rights of individuals to protect the privacy of their personal information.

In 2021, Alberta's government conducted public engagement to obtain feedback from a broad spectrum of stakeholders regarding priorities, concerns, and recommendations for modernizing Alberta's privacy protections. From this engagement, it was clear that there was widespread agreement that Alberta's privacy legislation is out of date and requires modernization. However, modernization of privacy laws needs to strike a balance between providing effective privacy protection for Albertans while also enabling Albertans to enjoy the social and economic benefits of data use.

The need to modernize PIPA is more critical than ever as a result of rapid technological advancement and outdated provisions that do not allow the private sector to harness innovative new systems and technologies that could benefit Albertans. Amendments to PIPA are needed to ensure Alberta has the strongest privacy protections in Canada, give Albertans more control over their personal information, increase transparency and accountability regarding automated decision making, and support the private sector in attracting investment, diversifying the economy, and improving the lives of Albertans.

…/2

The supplementary information attached outlines key considerations and recommendations for consideration by the Committee as part of its review of PIPA. These topics have been identified by our department as areas that merit exploration from the Committee based on previous reviews of the Act, internal analysis, and trends and best practices observed in other jurisdictions. It is important to note that there are trade-offs and economic implications associated with each consideration.

Furthermore, should the Committee wish, the department would be willing to return to provide an additional oral presentation at the request of the Committee to facilitate a comprehensive understanding of the issues at hand.

Thank you again for the opportunity to participate in this important work.

Sincerely,

Maureen.Towle

Digitally signed by Maureen.Towle
Date: 2024.06.04 15:50:58 -06'00'

Maureen Towle
Acting Deputy Minister

Attachment – Written Submission to Standing Committee

cc: Hilary Faulkner, Acting Assistant Deputy Minister
Innovation, Privacy and Policy, Technology and Innovation

Key Considerations and Recommendations for the Review of the *Personal Information Protection Act* (PIPA)

1. Harmonization of Legislation with Other Jurisdictions

The privacy legislative landscape, both within Canada and internationally, is constantly evolving as a result of changing technology. Given this dynamic environment, it is essential for Alberta's PIPA legislation to remain responsive and adaptable.

To understand the current benchmarks in privacy legislation, it is important to look at the European Union's (EU) General Data Protection Regulation (GDPR), enacted in May 2018, which is considered the global standard. The purpose of the GDPR is to protect data belonging to individuals located in the EU. The GDPR harmonizes data privacy laws across Europe, gives improved privacy protection and rights to individuals, and extends the reach of personal data protection beyond the borders of the EU. This international framework highlights the importance of robust and adaptive privacy laws.

Similarly, within Canada, provinces are taking steps to modernize its privacy legislation. British Columbia (B.C.)'s Special Committee to Review the *Personal Information Protection Act* (PIPA) reported to the Legislative Assembly of B.C. in December 2021, stressing the importance of harmonization with the changing federal, provincial, and international privacy landscape. Members also focused on new provisions for the rapidly changing digital economy and recommended changes to B.C.'s PIPA to reflect modern information processing practices and their impacts on privacy. Changes to B.C.'s PIPA in response to the Committee's recommendations have yet to be made.

Quebec's government recently amended Quebec's *Loi sur la protection des renseignements personnels dans le secteur prive/An Act Respecting the Protection of Personal Information in the Private Sector* (QPSA), with changes coming into force in phases between 2021 and 2024. Key amendments to the QPSA include:

- establishing within an enterprise a designated person in charge of protecting personal information;
- requiring enterprises to ensure that any technological products or services they use provide the highest level of confidentiality by default;
- mandating that individuals whose information is included in nominative lists must give consent to be contacted for commercial and philanthropic purposes; and
- granting individuals the right to de-indexation, or the removal of their personal information from search engine results.

In June 2022, the Government of Canada also introduced Bill C-27, to modernize Canada's private sector privacy framework through the proposed *Consumer Privacy Protection Act*, which would partially replace the current federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*. If passed, the *Consumer Privacy Protection Act* may impact the "substantially similar" status of Alberta's PIPA to *Personal Information Protection and Electronic Documents Act*. However, potential impacts for Alberta will not be known until Bill C-27 is passed.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should continue to monitor developments regarding Bill C-27 to ensure Alberta retains a "substantially similar" status to federal legislation.**
- **The Committee should explore opportunities to harmonize PIPA with global standards like the GDPR and leading Canadian jurisdictions such as B.C. and Quebec in areas such as breach notification requirements, privacy protection mechanisms, and individual data rights.**

2. Harmonization of Alberta Legislation

The review of PIPA presents an opportunity to increase alignment with Alberta's other pieces of privacy legislation, the *Freedom of Information and Protection of Privacy Act* and the *Health Information Act*. This could include establishing common definitions and enhancing interoperability between the three different sectors covered by these laws. By aligning provisions where possible, Alberta could streamline compliance efforts and promote consistency in privacy practices across the private, public, and health sectors.

Harmonized privacy standards would empower businesses and organizations in Alberta to operate efficiently across different regions, while ensuring that consistent privacy protections are maintained regardless of geographic boundaries. This would also align with feedback received during the 2021 engagement, in which there was a strong recommendation across focus groups to harmonize Alberta's legislation with other jurisdictions.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider areas to increase alignment between PIPA, *Freedom of Information and Protection of Privacy*, and *Health Information Act*, including common definitions and interoperability of privacy provisions to facilitate the seamless exchange of data and information within the private sector.**

3. New Categories of Data

As greater amounts of personal information are collected and used by organizations, a key tool for protecting privacy involves creating new categories of data in which personal information is removed or anonymized. This allows organizations to work with raw data while mitigating the risk of individuals being identified, thus bolstering privacy protection. These categories typically include non-identifying data[1], anonymized data[2], and synthetic data[3]:

Quebec's QPSA regulates the use of de-identified and anonymized information in the private sector, establishing that personal information may be used without the consent of the person concerned for the specific purposes of research or for the production of statistics, and if the information is de-identified. B.C.'s review of the province's PIPA legislation included examinations of pseudonymized information, anonymized information, and de-identified

[1] Non-identifying data is data derived from personal information that has been altered so the identity of the individual who is subject of the data cannot be readily learned. This means that information cannot be directly attributed to an individual, although there is an inherent risk that the data could potentially be used to re-identify an individual.

[2] Anonymized data refers to a data or dataset that has been stripped of any personally identifiable information to ensure that no individual can be identified from the information, whether directly or indirectly, by any means. This allows for the broader use of the non-identifying data for research or innovation purposes while ensuring the privacy of personal information is protected.

[3] Synthetic data is data that mimics the structure and pattern of real-world data while removing any links to identifiable individuals in the original data. It offers the opportunity to test new ideas and develop new products without putting personal information at risk.

information; however, no amendments have yet been made. In Ontario and New Brunswick privacy legislation, de-identification involves assessing whether there is other data available that, when used in combination with the de-identified data, could potentially lead to identification of an individual.

Non-identifying data, anonymized data, and synthetic data can be powerful tools for research, as they allow organizations to identify trends, analyze interdependencies, and develop targeted initiatives without exposing individuals' personal information. While PIPA has some provisions related to non-identifying information, it does not provide an adequate framework for leveraging the potential of these new and emerging types of data to improve service delivery for the benefit of Albertans. Amendments should authorize the creation and use of these new data types and establish provisions regarding notification to individuals that their personal information may be used for multiple purposes, such as research using non-identifying, synthetic, or anonymized data. This will balance the potential to harness this information for research and innovation, while ensuring Albertans are aware of how their data is used and processed.

Given the risk that non-identifying data could potentially be used to re-identify an individual without consent, it is also necessary to establish new offences in the legislation for violations or misuse of this information. Establishing a monetary penalty for re-identification or attempted re-identification would help deter attempts to re-identify non-identifying data, increase accountability for organizations subject to PIPA, and enhance the trust of Albertans that their personal information is protected.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider whether to authorize and regulate the creation and use of non-identifying data, anonymized data, and synthetic data by organizations subject to PIPA, while ensuring alignment with Alberta's other privacy legislation and principles.**
- **The Committee should explore provisions regarding notification to individuals that their personal information may be used for multiple purposes; and consider creating specific offences and penalties related to the re-identification or attempted re-identification of non-identifying data.**

4. Individual Data Rights

While PIPA establishes certain rights for individuals regarding the collection, use, and disclosure of their personal information, it lacks provisions for several key rights recognized in other jurisdictions. These include the right to erasure[4], the right to data portability[5], and the right to object to specific data processing activities[6].

[4] The right to erasure enables individuals to request the deletion of their personal information under certain circumstances. This would grant individuals the power to manage the retention and disposal of their own personal information.

[5] The right to data portability facilitates the transfer of personal data between service providers. This is intended to facilitate easier and more seamless transitions of personal data, promoting individual autonomy, and fostering competition.

[6] The right to object to specific data processing activities allows individuals to express their objections to the use of their personal data for certain purposes, such as direct marketing or profiling. This would require organizations to

Aligning with individual data rights, such as the GDPR's "right to be forgotten," would empower Albertans to have greater control over their digital footprint. This would enhance privacy protections and address growing public concerns about data misuse. Additionally, it would facilitate smoother international data exchanges by harmonizing Alberta's regulations with those of the EU, streamlining compliance for companies operating across these jurisdictions and making Alberta a more attractive destination for global business operations and technological investments.

During the 2021 engagement, a significant majority of general public respondents reported that they felt they had very little or no control at all over how their personal information is being used by organizations. It is important that Albertans are confident that their personal information is safe. Allowing more control over one's personal information fosters trust and instills confidence that, if organizations break that trust, there will be consequences. Implementing individual data rights within PIPA would strengthen individuals' control over their data and align privacy protections with international standards like the GDPR. This would enhance transparency and accountability among organizations, while empowering Albertans to shape how their personal information is collected, used, and disclosed.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider whether to establish individual data rights within PIPA, including the right to erasure, the right to data portability, and the right to object to specific data processing activities.**

5. Sensitive and Children's Data

With the rapid evolution of technology, there is a growing concern around safeguarding sensitive data and protecting children's privacy. Sensitive data includes things like medical, biometric, or intimate personal information, and can also include children's data. These types of information have a higher expectation of privacy due to the potential to result in serious harm if compromised. As technological advancements continue to expand the scope of personal data collection and processing, it is critical to strengthen protections for such information under PIPA.

Jurisdictions around the world have recognized that children and minors may be impacted by technologies differently than adults. There is widespread agreement that governments must provide specialized privacy protections for children and minors due to their vulnerability and distinct online experiences. Many jurisdictions have incorporated dedicated provisions safeguarding children's personal information, including the requirement of parental consent. PIPA's current provisions treat children's personal information similarly to that of adults, lacking specific measures to protect children's personal information.

Similarly, biometric information, such as facial images, iris scans, fingerprint access systems, or geolocation, is considered personal information under PIPA and is subject to the Act's general rules for collection, use, disclosure, and protection. However, these general

assess and respect these objections, unless they can demonstrate legitimate reasons that override an individual's interests.

rules do not account for the heightened vulnerability of this information in the modern digital age. In contrast, Quebec's definition of sensitive personal information includes medical and biometric information, and individuals must expressly consent to the use of this information. Where intimate data is concerned, the risks associated with the use of generative AI programs are even greater as deepfakes created by generative AI using intimate data can be used to harass, demean, intimidate, extort, and undermine individuals. The sensitivity of this information and the potential to result in harm if compromised warrant the strongest possible safeguards.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider whether to create a specific category of sensitive personal information under PIPA, which includes, but is not limited to, children's personal information, intimate personal information, and biometric data.**
- **The Committee should also consider introducing strict requirements regarding the collection, use, access, disclosure, and retention of the new category of sensitive personal information, such as requiring PIAs if sensitive data is collected.**

6. Privacy Protection Mechanisms

Protecting personal information from unauthorized access, use, or disclosure is critical to preserving individuals' privacy rights. During the 2021 stakeholder engagement, more than half of Albertans surveyed reported having had their personal information breached. As greater amounts of information are managed by private sector organizations, public concerns around the collection and use of personal information have correspondingly increased, particularly as a result of information being exploited or mishandled; so, to have public expectation for effective privacy rules or 'guardrails'.

In response to this, other jurisdictions have implemented a variety of mechanisms for safeguarding personal information, including, but not limited to, privacy management programs (PMPs)[7], privacy impact assessments (PIAs)[8], and breach notification requirements.

Alberta's PIPA currently has some similar elements including:

- requirements for organizations to develop and follow policies and practices to meet their obligations under the Act, which must be made available to the Office of the Information and Privacy Commissioner (OIPC) upon request; and
- requirements to notify the OIPC and the impacted individual without an unreasonable delay if a privacy breach poses a real risk of significant harm to an affected individual.

[7] PMPs are tools that ensure privacy is built into initiatives, programs, or services at every stage of their development, implementation, and operation. They are meant to provide transparency on privacy measures and keep public bodies accountable and transparent about the management of personal information in their custody or control. Common components of a PMP include: requiring the appointment of a "privacy officer" or designated privacy office; policies on how individuals can access or correct their personal information; policies on how personal information is retained or disposed; ensuring the use of risk management tools including PIAs; transparency on privacy training and education requirements for employees; breach reporting or response protocols; and regular review of policies related to privacy.
[8] PIAs are tools which help to identify, assess, and mitigate potential privacy risks that may occur in a project.

Introducing new requirements for organizations to develop and implement PMPs and PIAs would enhance privacy protections and increase accountability for organizations that are entrusted with Albertans' personal data. However, it is also important to consider the administrative and financial implications this could have on organizations. During the 2021 engagement, some concerns were raised regarding the cost and burden PMPs could place on smaller organizations, and the capacity of the OIPC to respond to new privacy management obligations. Therefore, any new PMP and PIA requirements should take into account the size and resources of different organizations, as well as the sensitivity of the data they hold, and allow them to be tailored accordingly. For example, requirements should vary depending on whether an organization holds basic contact information or sensitive financial data.

Alberta's PIPA requires an organization that suffers a loss or unauthorized access to or disclosure of personal information (breach) to notify the OIPC without unreasonable delay if the breach poses a real risk of significant harm to affected individuals. If the Commissioner determines that the breach poses a real risk of significant harm, they may then require the organization to notify individuals affected by the breach and to do so within a specified period. Reviewing breach reporting requirements will enhance transparency and accountability for organizations handling personal information and help determine whether the current provisions are appropriate.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider whether to implement mandatory PMP and PIA requirements for organizations subject to PIPA, scaled to the size of the business and the sensitivity of the personal information contained.**
- **The Committee should review breach reporting requirements to assess factors such as harm thresholds, notification timelines, and the scope of information provided to affected individuals.**

7. Administrative Monetary Penalties to Deter Non-Compliance

Enforcement measures are essential to ensure compliance with privacy regulations and to deter non-compliance. Administrative monetary penalties (AMPs) are financial penalties imposed for the failure to comply with an Act or regulation. Other jurisdictions have introduced AMP provisions in their laws to address serious, repetitive, or long-term contraventions and to reinforce that individuals' privacy rights are protected and enforced.

Quebec's QPSA provides for the Commission d'accèss à l'information to impose AMPs and sets out the terms for recovering and claiming the amounts owing. AMPs of up to $50,000 may be imposed if the contravener is an individual. In the case of an organization, the greater of $10 million or two per cent of worldwide turnover for the preceding fiscal year may be levied.

According to the GDPR, AMPs should be "effective, proportionate, and dissuasive." The maximum fine for certain infringements is the greater of €20 million or up to four per cent of the total worldwide annual turnover of the preceding financial year. The maximum fine for lesser infringements is the greater of €10 million or up to two per cent of the total worldwide turnover of the preceding financial year.

During the 2021 engagement, almost all general public respondents indicated that it was somewhat or very important that private sector organizations be subject to penalties and administrative fines for not complying with privacy obligations. Currently, while PIPA contains criminal penalties for non-compliance with its regulations, there are no provisions allowing for the imposition of AMPs, which are imposed by regulatory agencies rather than through the criminal justice system. This limits the options available to the OIPC in enforcing the legislation's provisions.

While AMPs are intended to deter non-compliance, it is important to recognize that a flexible and risk-based approach must be considered to accommodate the various operational needs and resources of organizations in Alberta. While penalty amounts should be set at an appropriate level to deter non-compliance, care must be taken to ensure that AMPs do not have an outsized impact on small businesses or stifle innovation and competitiveness in the province.

The OIPC should also have the discretion to choose not to impose an AMP should an individual or organization take measures necessary to remedy the failure or mitigate its consequences.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider whether to enable the OIPC to impose AMPs for non-compliance with the Act, with specific consideration given to the severity of the violation, the size and resources of the organization, and the potential impact on affected individuals.**

6. Rights Associated with Automated Decision-Making and Artificial Intelligence

The rapid advancement of digital technologies, particularly the use of automated decision-making associated with artificial intelligence (AI), presents both opportunities and challenges for privacy legislation. Automated decision-making involves the use of algorithms and AI to analyze data and make decisions without direct human intervention. As accessibility of these AI tools become more widespread, it is imperative for Alberta to create a comprehensive plan for the responsible adoption and implementation of AI within the private sector to maximize opportunities while minimizing risks. Canadian and international jurisdictions are taking a multi-pronged approach to regulate AI, addressing privacy issues within privacy legislation and requirements for AI technology development in standalone policy instruments.

In Canada, Quebec's QPSA is the only legislation that imposes some obligations regarding automated decision systems (ADS). The purpose is to establish transparency and accountability requirements for applicable ADS processes. The provision only applies to ADS decisions that use personal information and are exclusively automated. QPSA requires organizations to:

- provide notice of the ADS process at the time the decision is made;
- provide a channel for individuals to submit questions, comments or complaints to a representative who can review the decision;

- allow individuals to request correction of the personal information used in the decision; and
- inform the individual, upon request of the personal information used in the decision, the reasons, principal factors, and parameters.

The Government of Canada has introduced the *Artificial Intelligence and Data Act* (AIDA) as part of Bill C-27. The purpose of AIDA is to:

- regulate international and interprovincial trade and commerce in AI systems by establishing common requirements, applicable across Canada, for the design, development, and use of those systems; and
- prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or harm to their interests.

One of the key components to AIDA is the creation of an Artificial Intelligence and Data Commissioner within the department responsible for the Act. It would also authorize the Minister to order the production of records related to AI systems, and to establish an advisory committee and produce reports on compliance within the Act.

As we continue to monitor developments at the federal level, Alberta should consider how best to accommodate the evolving landscape of AI while ensuring robust privacy protections. Creating regulations prematurely could lead to policy misalignment with the rest of Canada, potentially discouraging organizations from operating in Alberta due to the lack of harmonization. Furthermore, industry has expressed caution in additional AI legislation and its impact on innovation and competitiveness.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider establishing individual rights and privacy protections within PIPA regarding automated decision-making and AI systems such as:**
  - **requiring organizations to inform individuals of the use of automated decision-making before using their personal information in this manner;**
  - **enabling individuals to request a human review of decisions;**
  - **implementing processes to safeguard the security of personal information used in AI systems and the logic involved in automated decisions; and**
  - **requiring organizations to conduct audits or ensure the accuracy of data processing, with provisions for individuals to request corrections.**
- **The Committee should consider whether to grant the Minister power to regulate AI standards and guidelines, similar to AIDA, to ensure organizations would be subject to government oversight for the ethical use of AI technologies.**

7. Altered Content

Modern technologies have enabled the manipulation of content to create convincing images, audio, and videos of an individual or an event. Commonly referred to as “deepfakes”, this type of content has become increasingly prevalent in recent years and has raised significant concerns regarding their potential to deceive or manipulate audiences. While some alterations are done by AI or generative tools, deepfakes can also be created using more traditional computer software like Adobe Photoshop. When used maliciously, they can

harass, demean, intimidate, extort, and undermine individuals, organizations, and/or the democratic process.

Some Canadian jurisdictions have recently taken steps to address altered content. In 2022, Saskatchewan updated its *Privacy Act* to provide victims of non-consensual sharing of intimate images with the power to reclaim their images and have them removed from the internet. In 2024, B.C. enacted the *Intimate Images Protection Act*, which empowers individuals to request the removal of intimate images, regardless of whether they are real or fake, and pursue legal action against both perpetrators and internet platforms for any damages incurred. In January 2024, the Government of Canada introduced Bill C-63, the *Online Harms Act*, to combat sexually explicit deepfakes. The bill, still in draft, aims to regulate online content, addressing the non-consensual sharing of intimate images.

In 2017, Alberta passed the *Protecting Victims of Non-Consensual Distribution of Intimate Images Act*. However, a lack of legal proceedings relating to deepfakes has limited the courts' ability to determine if they are within the legislation's scope. A 2021 decision made by the Court of Queen's Bench of Alberta (ES v Shillington) recognized the "public disclosure of private facts" tort for the first time. The case pertained to an individual who posted their partner's intimate images on the internet without consent. This decision resulted in the individual being ordered to remove the images and pay damages to their partner. Alberta was the first western Canadian province to recognize the tort—this recognition is significant, as it makes it possible for Albertans to seek damages for injuries (physical, emotional, financial) when private information is publicly disclosed without their consent.

Provisions in Alberta's PIPA apply to the collection, use, access, and disclosure of personal information by private sector organizations, or individuals operating in a commercial capacity. These provisions may apply to the creation and/or dissemination of altered content if generated for a commercial purpose; however, this is currently not specified within the legislation. Amendments could explicitly clarify that the scope of PIPA's collection, use, and disclosure provisions also apply to the creation and/or dissemination of altered content.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider clarifying that provisions in PIPA that apply to the collection, use, access, and disclosure of personal information by private sector organizations also apply to the creation and/or dissemination of altered content.**

8. Consent Requirements

Consent is a fundamental principle of private sector privacy legislation, enabling individuals to exercise control over their personal information. Under PIPA, there are three types of consent, including express consent[9], implied or deemed consent[10], and opt out consent[11].

[9] Express consent is when consent is provided in writing or verbally.
[10] Implied consent is when an individual does not actually give consent but volunteers information for an obvious purpose, and a reasonable person would think that it was appropriate in the situation to volunteer that information.
[11] Opt out consent is when an individual is given the choice to opt out of collection, use, or disclosure of their personal information. By not opting out, they have provided consent for the organization to collect, use, or disclose personal information for the specified purpose.

These provisions are intended to ensure that individuals' consent is informed, voluntary, and meaningful.

The 2021 engagement indicated that Albertans feel private sector organizations do not communicate use of information clearly. Almost all of the general public respondents agreed or strongly agreed that they should have the right to consent before an organization buys or sells their personal information, but very few respondents indicated that they know how private organizations use their information.

Drawing lessons from the GDPR and Quebec's QPSA, Alberta should consider updating consent requirements to enhance clarity and transparency. Under the GDPR, consent must be obtained in an intelligible and easily accessible form, using clear and plain language, while Quebec's legislation states consent must be clear, free, and informed, and must be requested in clear and simple language.

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider whether to implement requirements mandating plain language notices to ensure individuals have a clear understanding of how their personal information will be used and shared prior to providing consent.**

9. Scope of the Act

Currently, PIPA applies primarily to private sector organizations in Alberta. This includes, but is not limited to, corporations, businesses, professional regulatory associations, trade unions, partnerships, private schools, and any individual acting in a commercial capacity.

The application of Alberta's PIPA differs from some other jurisdictions in that:

- PIPA only applies in a limited way to certain non-profit organizations, only to the extent that they are involved in commercial activities; and
- PIPA does not apply to political parties.

In contrast, B.C.'s PIPA applies to both provincial and federal political parties operating in the province and Quebec's QPSA applies to personal information held by a political party, an independent member, or an independent candidate.

B.C.'s PIPA applies to not-for-profit organizations, including trade unions, charities, foundations, trusts, clubs, churches, and amateur sports organizations. Not-for-profit organizations in B.C. (regardless of the location of the organization's headquarters) are in the same position as for-profit organizations and subject to the legislation in respect of all their activities, not only to any potential "commercial activity." Quebec's QPSA applies to organizations engaging in economic activities even if that activity is not commercial in nature. However, the organization's primary purpose is an essential factor in QPSA's applicability.

Expanding the scope of PIPA to fully encompass non-profit organizations and political parties would enhance transparency, accountability, and privacy protection within these sectors. However, it will be important to examine the additional compliance burdens and operational challenges this may create. Clarifying the scope of PIPA's application to non-

profits and political parties will require thorough deliberation and consideration of the unique characteristics and functions of these organizations within the Alberta context. It may be more appropriate to update Alberta's *Election Act* to address issues regarding political parties, and instead focus PIPA amendments on expanding the scope of the Act to explicitly include non-profit organizations, with a focus on size and scale, and type of personal information collected.

During the 2016 review of PIPA, stakeholders expressed the challenges associated with the current definition of "commercial activity" in PIPA, which can make it difficult for some non-profit organizations to easily understand the legislation. The Committee's only recommendation in the review's final report was to amend Section 56 of PIPA to clarify the definition of commercial activity. This further exemplifies the need to review the scope of PIPA on non-profit organizations, whether clarifying this definition or including non-profit organizations fully within the scope. This would resolve the lack of clarity and would help non-profits better understand their obligations under the Act and reduce their risk of non-compliance due to ambiguity about the scope of "commercial activity."

SPECIFIC CONSIDERATIONS FOR THE COMMITTEE:

- **The Committee should consider extending PIPA's scope to include non-profit organizations, with a focus on size and scale, and type of personal information collected.**
- **The Committee should consider whether to revise the definition of "commercial activity" to explicitly outline which activities fall under the scope of PIPA.**
- **The Committee should consider whether to extend PIPA's scope to include political parties.**