Office of the Information and Privacy Commissioner of Alberta

DELIVERED BY EMAIL

May 31, 2024

Committee Clerk
Standing Committee on Resource Stewardship
Legislative Assembly of Alberta
RSCommittee.Admin@assembly.ab.ca

Dear Committee Clerk:

Re: Submission for Review of the *Personal Information Protection Act*

Attached is the Office of the Information and Privacy Commissioner of Alberta's submission for consideration by the Standing Committee on Resource Stewardship on its review of the *Personal Information Protection Act.*

Should you or the Committee have any questions in relation thereto, please contact my assistant, Edie Piroro, at 780-644-4894 or by email at epiroro@oipc.ab.ca, in regards to the same.

Sincerely,

[redacted]

Diane McLeod
Information and Privacy Commissioner of Alberta

Attachment

Office of the Information and Privacy Commissioner of Alberta

Personal Information Protection Act

Submission to the Standing Committee on Resource Stewardship

Submitted on May 31, 2024 by:
Diane McLeod, Information and Privacy Commissioner of Alberta

Contents

1. Commissioner's Message

On May 14, 2003, Bill 44, *Personal Information Protection Act* (PIPA) was tabled in the legislature.

During debate of the Bill, the kinds of concerns raised about the need to protect personal information (PI) were: the collection of phone numbers by retailers for any transaction including cash; the selling of customer lists between organizations; the rise of big data banks and risks associated with the compilation of PI,[1] the use of loyalty cards, [2] PI being stolen from trash bins outside of someone's home or through their garbage collection, and the risks from stolen identities.[3]

The state of technology and the amount of PI shared by individuals and accessible by organizations when PIPA was drafted in the early 2000s is vastly different than it is today.

In the early 2000s, less than 7% of the world was online.[4] Due to the expansion of broadband internet access, by 2020 over one-half of the global population had access to the internet.[5] The number of cell phones subscriptions increased from 740 million at the start of the 2000s to more than eight billion in 2020.[6] Technology was also becoming more personal and portable with the sale of the first iPod in 2001.[7] Just six years later the iPhone was introduced. This ushered in a whole new era of personal technology, which has led to a world in which technology touches everything we do.[8] In 2004, we began to see the rise of social media. MySpace was the first social media site to reach one million users.[9] Facebook, which did not launch publicly until 2006, had more than 2.26 billion users by 2018.[10] TikTok launched in 2016 and gained about 20 million new users per month, resulting in over half a billion users in just two years, and the list goes on.[11] The amount of users for 11 of the most popular social media platforms ranges from 238 million at the low end to over two billion at the high end.[12] Online shopping has increased exponentially over the past decade with a boom in 2020 due to the COVID pandemic, which forced many retailers and sellers online in order to survive. We now have numerous apps to do our daily activities, including banking, ordering food, watching movies and sports, video chatting, shopping, playing games, etc. Most people now have cell phones, providing us with ease of access to our apps. In addition, our phones now have the capability to record voice, video, and take photos, all of which can be edited at will, and easily uploaded to social media or other apps. This rise in technology and access to the internet has resulted in vast amounts of PI being shared by individuals and collected,

[1] Alberta Hansard, November 19, 2003 at pp. 1746 and 1747.
[2] *Ibid.,* at p. 1767.
[3] *Ibid.,* November 25, 2003, at p. 1851.
[4] World Economic Forum, How has technology changed – and changed us – in the past 20 years?, November 18, 2020, https://www.weforum.org/agenda/2020/11/heres-how-technology-has-changed-and-changed-us-over-the-past-20-years/.
[5] World Economic Forum, How has technology changed – and changed us – in the past 20 years?, November 18, 2020, https://www.weforum.org/agenda/2020/11/heres-how-technology-has-changed-and-changed-us-over-the-past-20-years/.
[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid.*
[9] Esteban Ortiz-Ospina (2019) - "The rise of social media" Published online at OurWorldInData.org. Retrieved from: 'https://ourworldindata.org/rise-of-social-media.
[10] *Supra 4.*
[11] *Supra 9.*
[12] *Ibid.*

used and disclosed by private sector organizations, mostly for profit. Profit is gained from PI directly by selling that information, or indirectly by serving ads for products based on profiling, leading to a higher chance of persuading a person to buy something or to hold their attention for longer.[13]More time on a platform equals more PI collected and more exposure to ads or other forms of influencing, resulting in more revenue. There is also a large market for influencing populations for special interest or political purposes.[14]

In more recent years, the development and use of Artificial Intelligence (AI) has increased. This technology is being harnessed by many organizations, social media and large technology corporations as an example, to analyze an individual's activity and to feed the individual personalized information based on an algorithm with the goal of selling goods, setting personalized prices,[15] and increasing profits. AI and the automated decision making it entails work seamlessly with the advertisement and influencing ecosystem that shape much of our online experiences. AI is also changing the way other industries work, such as education, and the expanding Education Technology (Ed-tech) ecosystem it fosters, means that even children are impacted by AI. AI enhances and enables processing of PI both in terms of the ease of collecting PI via technology, such as through facial recognition, and the increased ability to derive insight and meaning from raw data collected from various sources.[16] These examples stress that, as a society, more and more of our life is digitalized and our actions produce more data than ever before. This data is or will become subject to AI processing. This fundamental development must be taken into account when reviewing our privacy laws and ensuring our fundamental rights including the right to privacy are upheld.

In 2022, the world was introduced to generative AI and it took the Internet by storm: within three months of publicly launching ChatGPT, the platform had gained 100 million monthly active users, which had never happened before.[17] We are on the doorstep of the wide spread use of AI by all three sectors: private, public and health. AI is described by some as having immense potential benefit for societies, particularly in the areas of health care and public services. However, some also describe it as having great potential for harm. We are also on the verge of quantum computing, which will give us the power to harness big data more readily than before and to power AI and other novel technologies in development. It also has the potential, due to its processing power, to significantly disrupt the encryption technology that we all rely on for safe online transactions, including for banking.

Globally, nation states are being challenged to update their privacy laws in the face of this tremendously rapid advancement of technology and data driven world. The laws that have been modernized are designed to better protect citizens from the harms that could flow from inappropriate collections, uses

[13] The Markup, How Your Attention Is Auctioned Off to Advertisers, 23 June 2023, https://themarkup.org/privacy/2023/06/23/how-your-attention-is-auctioned-off-to-advertisers and https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you

[14] See e.g., Center for Strategic and International Studies, A Short Discussion of the Internet's Effect on Politics, January 29, 2021 https://www.csis.org/analysis/short-discussion-internets-effect-politics.

[15] See Woodcock, Ramsi A., "Personalized Pricing as Monopolization" (2019). Connecticut Law Review https://digitalcommons.lib.uconn.edu/cgi/viewcontent.cgi?article=1418&context=law_review.

[16] https://themarkup.org/machine-learning/2023/11/30/he-wanted-privacy-his-college-gave-him-none.

[17] Timeline of LLM Developments and Privacy Leaks, https://llmprivacy.ca/timeline

or disclosures of PI for profit by private sector organizations and the opaque nature of technology in the processing of this information. The laws that are discussed in this submission include enhanced measures to control the collection, uses or disclosures of PI by organizations, rights associated with the processing of PI using AI, increased security requirements, better privacy governance requirements, and protections to deter harmful practices, such as through the use of administrative monetary penalties. These laws recognize that use of technology by an organization today, more than ever before, can have a significantly negative impact on human rights, including privacy rights. This is due in part to the ever-growing power of technology, together with the vast amount of PI accessible in the marketplace. As a result, most modernized privacy laws are embedding these rights expressly within their laws, in recognition that even though there is value in having organizations participate effectively, including through the use of AI and other novel technology, in a worldwide digital economy, human rights and the right to fair data processing must be adequately protected in this environment.

The review of PIPA by the Standing Committee on Resource Stewardship (Committee) comes at a crucial time. PIPA needs to be amended to protect Albertans' privacy in our information based society[18], while enabling commerce, especially where this relates to the development and deployment of innovative technologies. Alberta also needs a modernized private sector privacy law that aligns with leading global privacy laws to accommodate the free flow of information vital to commerce.

In the pages that follow, we have outlined the relevant issues and trends that have been or are being addressed nationally and internationally in modern privacy laws to achieve a proper balance between protecting privacy and enabling the use of technology by businesses to prosper. Our recommendations to amend PIPA set out herein are designed to ensure that PIPA remains fit for purpose such that Alberta businesses will be able to prosper as the digital economy evolves while ensuring the privacy rights of Albertans remain adequate in this environment.

2. Explanatory Note

The comments and recommendations in this document have been prepared by the Office of the Information and Privacy Commissioner of Alberta (OIPC), for consideration by the Standing Committee on Resource Stewardship for amendments to PIPA.

All section references in this submission are to PIPA unless otherwise stated. See Appendix A for a Glossary of the terms used herein.

[18] Information society (sometimes also called network society) is a development coined by Manuel Castells. It indicates a society that operates through a constant flow of information through digital information technology. Information technology in such a society impacts most important forms of social organization, including education, economy, healthcare and government. See e.g., https://www.researchgate.net/publication/325582810_Manuel_Castells'_theory_of_information_society_as_media_theory for more information.

3. Summary of Recommendations

Section 5. Purpose of the Act

1. That the committee consider whether to expressly recognize in the purpose statement of PIPA that the protection of personal information privacy is a fundamental human right.

Section 6. Scope of the Act

Section 6.1. Political parties

2. That PIPA be amended to make the Act apply fully to political parties.

Section 6.2. Non-profit Organizations

3. That PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year transition period.

Section 7. Enhancing the Privacy Rights of Albertans

Section 7.1. Right of Access

4. That PIPA be amended to grant Albertans a *right* to access their own personal information.

Section 7.2. Right to Be Forgotten

5. That PIPA be amended to codify the 'right to be forgotten' by:
    a. giving individuals the right to request that their PI be de-indexed where the collection, use or disclosure of their PI or the dissemination of their PI constitutes a violation of PIPA or where these activities cause them harm, the latter of which would be subject to a harms test;
    b. giving individuals a right to request the disposal or deletion of their PI:
        i. when the PI is no longer necessary to meet the purpose for which it was collected;
        ii. when an individual has withdrawn consent for further uses or disclosures of their PI,
        iii. when PI was collected, used or disclosed in contravention of PIPA; and
        iv. if the PI was about a minor when it was collected, regardless of who provided it or who gave consent for the collection, use or disclosure of that PI;
    c. subjecting this right to limited and specific exceptions:
        i. for compliance by the organization with a legal obligation;
        ii. exercise of legal rights by the organization or to establish and defend it from legal claims against it; or
        iii. for reasons of public interest, i.e., related to public health or safety.

6. That PIPA be amended to require organizations to take into account any factors surrounding the request, including the individual's reasons and circumstances associated with the request, and

whether the subject individual associated with the request is a child or part of a vulnerable population.

7. That PIPA be amended to require organizations to notify the individual whose request is refused at the time of refusal that they may make a complaint to the Commissioner about the refusal.

Section 7.3. Right to Data Mobility and Portability

8. That PIPA be amended to codify the 'right to portability and data mobility' by including therein:
    a. the right of an individual to obtain their PI from an organization in a structured, commonly-used machine readable format; and
    b. the right of an individual to have their PI directly transferred to another organization in a structured, commonly-used machine readable format.

Section 7.4. Automated Decision Making

9. That PIPA be amended to grant individuals the right to:
    a. contest automated decision making; and
    b. be notified in plain language about the use of an automated decision making system to make the decision before it is made.

10. That PIPA be amended to require organizations that make a profile, prediction, recommendation or decision about an individual using an automated decision making system that either assists or replaces human judgment to:
    a. include in its publically available policies and procedures a plain language general account of the organization's use of automated decision making systems, an individual's privacy rights associated therewith, and how an individual can exercise these rights;
    b. before or at the time of collecting PI directly from the individual, require that individuals be notified about its use of automated decision making, the significance or consequences of the same, the related rights of the individual, and the name of a person or position in the organization who can answer questions on behalf of the organization about the use of automated decision making system;
    c. if indirectly collected PI is used, the same as under 10. b. applies plus an obligation to disclose where the indirectly collected PI was obtained, and under what authority it is being used;
    d. inform the individual about the PI being used to make a profile, prediction, recommendation or decision, the source of the information, and the reasons and criteria used that led to the profile, prediction, recommendation or decision;
    e. establish a process to enable the individual to:
        i. review the accuracy of its PI used for automated decision making;
        ii. contest the use of automated decision making to create a profile, prediction, recommendation or decision about them; and
        iii. to request reconsideration by a human after the profile, prediction, recommendation or decision is made.

11. That PIPA be amended to require organizations that use an automated system to make a profile, prediction, recommendation or decision that may lead to harm or unfairness to an individual or group to:
    a. report statistics associated with the use of the automated system in a form determined by the Commissioner or by regulation;
    b. regularly evaluate the outputs of the system to protect against harm and unfairness;
    c. submit a PIA and/or AIA to the Commissioner for review and comment prior to using the automated system; and
    d. permit the Commissioner to establish how AIAs are to be conducted and their content and form.

12. Where an organization plans to use an automated system to make a profile, prediction, recommendation or decision that may lead to harm or unfairness to an individual or group, that PIPA be amended to authorize the Commissioner to:
    a. audit the use of an automated decision making system to ensure the system in its design or use minimizes, to the degree possible, any harm or unfairness that may flow to an individual as a result of the use of the system;
    b. review and comment on PIAs or AIAs submitted by an organization;
    c. order an organization to stop using a system that may cause, has caused or is causing harm to an individual or group.

Section 7.5. Children's Privacy

13. That PIPA be amended to offer specific protection for children's PI such by including similar protections for children as set out in Bill C-27 (CPPA), the GDPR, and Quebec's Law 25 or by requiring organizations to adopt a code of practice similar to that of the UK's Children's Code.

Section 8. Duties That Promote Accountability and Public Trust

Section 8.1. Privacy Management Programs

14. That PIPA be amended to:
    a. require organizations to have a privacy management program in place;
    b. set out the components of a privacy management program similar to those set out in *Getting Accountability Right with a Privacy Management Program*, or as set out in Bill C-27 (CPPA) or Quebec's Law 25;
    c. require organizations to make publicly available relevant sections of their privacy management program including policies, procedures (access, complaints), practices (security, information management), and privacy contact information; and
    d. require that organizations provide information about their privacy management program to the Commissioner upon request.

15. That PIPA be amended to authorize the commissioner to:
    a. audit an organization's privacy management program including its components; and
    b. review and comment on an organization's privacy management program.

Section 8.2. Privacy Impact Assessments

16. That PIPA be amended to require organizations to:
    a. conduct PIAs in certain circumstances, such as undertaking activities that involve:
        i. processing sensitive PI;
        ii. profiling and data-linking or data-matching activities; and
        iii. any significant change to an existing program that involves the above-listed information or activity;
    b. submit those PIAs for review and comment by the Commissioner prior to undertaking those activities listed; and
    c. permit the Commissioner to establish the content and form of PIAs.

17. That PIPA be amended to:
    a. authorize the Commissioner to require an organization to provide a PIA to the Commissioner for review where the Commissioner has a reasonable belief that the processing activity creates risks to the privacy rights of Albertans;
    b. authorize the Commissioner to review all PIAs submitted by organizations and comment on any privacy risks associated with the proposed activity and provide recommendations; and
    c. require organizations to respond to any recommendations made by the Commissioner in response to a PIA submitted within 30 days of receipt.

18. That PIPA be amended to require organizations that develop information systems intended for use by custodians in Alberta's health sector to process health information governed by the HIA, to submit a PIA to the OIPC for review against the requirements of the HIA before deploying the information system to a custodian.

19. That the Committee recommend to the Minister of Health:
    a. that HIA be amended to relieve the duty of a custodian to prepare and submit a PIA for submission to the OIPC:
        i. for use of an IT system where a PIA was submitted to the OIPC by the organization as required by PIPA;
        ii. the OIPC has reviewed the system against the HIA requirements and any recommendations made by the OIPC for the IT system have been implemented to the satisfaction of the OIPC by the organization;
        iii. the organization provides documented evidence of the OIPC review to the custodian and compliance with any recommendations made by the OIPC; and
        iv. the custodian does not make any modifications that affect privacy risk to the IT system, such as through changes or customization that require further review against the HIA because they were not before the OIPC during its review of the PIA.
    b. that the HIA be amended to require a custodian who has made modifications to the IT system as indicated in 19. a. iv. above, to submit, prior to using the IT system, for review and comment by the OIPC, an addendum to the PIA that was submitted by the

organization as required by PIPA, setting out the modifications and how the same will comply with the HIA.

Section 8.3. Mandatory Breach Notification

20. That section 34.1 of PIPA be amended to require organizations to:
    a. without unreasonable delay, directly notify individuals about the Breach where there is a RROSH to the individuals as a result of the Breach;
    b. provide the information in the notice to the individuals in plain language that individuals would reasonably be able to understand; and
    c. provide the notice to the Commissioner at the same time the notice is sent to the affected individuals.

21. That PIPA be amended to:
    a. include a provision requiring an organization that is unable to directly notify one or more affected individuals as required by section 34.1, to request permission from the Commissioner for indirect notification;
    b. authorize the Commissioner to permit indirect notification on any terms and conditions specified by the Commissioner; and
    c. require the organization to adhere to any terms and conditions for indirect notification established by the Commissioner.

22. That PIPA be amended to include authority for an organization that is required to notify affected individuals of a Breach, to provide the prescribed information in phases, where necessary, to avoid undue delay in notification.

23. That PIPA be amended to include a definition for "significant harm" and include factors for use by an organization in determining whether a RROSH exists. A definition or list of factors should clarify that the determination is based on the risks to affected individuals and not risk of harm to the organization or its employees.

24. That PIPA be amended to require Service Providers:
    a. to notify any organization that contracted the service provider's services about a Breach of PI in the Service Provider's custody immediately upon discovering the breach;
    b. to cooperate with the organization's investigation into the Breach and to make any information accessible to the organization as may be required for the organization to carry out its duties under section 34.1; and
    c. to cooperate with the Commissioner's review of a Breach notice submitted by, or on behalf of the organization.

25. That the PIPA Reg be amended to require organizations to provide information to the Commissioner about the relationship with Service Provider when a Service Provider is involved in a Breach.

26. That section 37.1(1) of PIPA be amended to reflect the proposed amendment to the Breach notice requirement in section 34.1. Such amendments should include the Commissioner's authority to:
    a. require an organization to notify any individual to whom the Commissioner determines ought to have been notified under section 34.1 but was not notified; and
    b. require an organization to re-notify affected individuals who received notice of a Breach under section 34.1 when the notice does not contain all the information required by the PIPA Reg.

27. That the Breach reporting provisions in PIPA be amended to:
    a. grant the Commissioner authority to review the cause of the Breach and to require organizations to take steps that are necessary to mitigate the risk of recurrence - as part of this authority, the Commissioner should be authorized to obtain any information that is necessary to undertake this review; and
    b. require organizations and Service Providers, as applicable, to cooperate with the Commissioner's review of the cause of a Breach and to provide any information requested by the Commissioner to conduct the review.

28. That PIPA be amended to require organizations to:
    a. keep and maintain a record of every breach of security safeguards that impacts PI under its custody or control;
    b. include in the record the facts of the breach, the factors considered in the assessment of harm, and the remedial actions taken; and
    c. on request, provide the Commissioner with access to, or a copy of, the record notwithstanding any other enactment, solicitor-client privilege, or any privilege of the law of evidence.

Section 8.4. Service Providers

29. That PIPA be amended to bind Service Providers and any downstream Service Providers to comply with PIPA similar to that of Bill C-27 (CPPA) and the GDPR, including:
    a. requiring an organization to ensure, by contract, that a Service Provider provides the same or better privacy protection as the organization is required to provide under PIPA;
    b. prohibiting a Service Provider from collecting, use or disclosing PI on behalf of an organization except as permitted by the contract with the organization;
    c. binding the Service Provider to comply with PIPA for any PI collected or in its custody as a result of providing the services, or making the Service Provider subject to PIPA if it fails to comply with the contract;
    d. provisions that will ensure that downstream Service Providers are subject to PIPA the same as Service Providers;
    e. developing regulations about what the contracts should contain, such as:
        i. a requirement to specify the purposes for which the Service Provider is providing the service;

ii. the purposes for which the Service Provider may collect, use or disclose PI on behalf of the organization to deliver the services;
iii. that the organization maintains control of PI that is in the custody of the Service Provider for the purposes of providing the service;
iv. how the PI will be secured by the Service Provider such that the security will be in accordance with the requirements of PIPA;
v. a requirement to cooperate with the organization with respect to the exercise of any right under PIPA by an individual or any duty of the organization (e.g., PIAs);
vi. a requirement that the Service Provider notify the organization in the case of a Breach and cooperate with the organization to ensure the organization can meet its obligation with respect to Breaches under PIPA;
vii. a requirement that the Service Provider notify the organization if it intends to retain the services of a downstream Service Provider and a requirement to inform the organization about the nature of the services to be provided by that Service Provider where such services may involve the collection, use, disclosure, security or management of PI; and
viii. when the agreement comes to an end, whether the Service Provider will be required to return or destroy the PI in its custody and how it will occur.

Section 8.5. Safeguards

30. That PIPA be amended to require an organization to make security arrangements to protect PI in its custody or control through a combination of physical, organizational and technological security safeguards.
    a. These safeguards should ensure the confidentiality, integrity and availability of the PI and allow for the prompt restoration of information systems following an incident.
    b. The level of safeguards should be commensurate with the information security risks the organization faces, sensitivity of the PI, the purposes for which the PI is to be used, and the quantity and distribution of the PI and the medium on which it is stored.
    c. At a minimum, the security provision in PIPA should include an obligation for security due care (certain minimal steps an organization should take), including the obligation to train its staff.

31. That consideration be given to including in the PIPA Reg specific security requirements that an organization is required to adhere to so as to make the law more responsive to mitigating the risks to security of PI from emerging and significant information security issues.

Section 8.6. Plain Language Requirements

32. That PIPA be amended to:
    a. require organizations to provide comprehensive, specific, clear and plain notice of all purposes for which individuals' PI will be collected, used and disclosed, such that it is

reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting;

b. clarify that consent is not valid if these requirements are not met; and
c. require that this notice be given separately from other legal terms.

33. That PIPA be amended to require an organization to communicate in plain language to an individual or the general public, as applicable, in its policies, procedures, notices, or other correspondence, including responding to access requests, such that the communication that the individual is reviewing or receiving would be understandable to them.

Section 8.7. Ethical Obligations and Duties

34. That the Committee considers whether to codify in PIPA a duty of loyalty, fiduciary duties or CoC, similar to that of other jurisdictions, to promote ethical conduct by organizations handling Albertans' PI.

Section 9. Privacy and Innovative Technology

Section 9.1. De-identification and Anonymization

35. That PIPA be amended to:
    a. define "de-identified PI" and the following should be included in the Act, regulations or standards set by regulation:
        i. standards as to what constitutes de-identified PI;
        ii. permission for organizations to use PI to create de-identified PI for legitimate purposes such as using de-identification as a security safeguard and for those purposes set out in Bill C-27 (CPPA);[19]
        iii. a prohibition on organizations:
            1. creation of de-identified PI except in accordance with the established standards;
            2. use of the term "de-identified PI" or the like to claim that no PI is being used, etc., or to infer privacy protection, unless the process of de-identification of the PI meets the established standards; and
            3. selling de-identified PI;
        iv. a requirement that organizations:
            1. keep information that can be used to re-identify an individual separate from the de-identified PI and that this information be subject to technical and organizational controls for that purpose;
            2. leveraging de-identification, conduct regular re-identification risk assessments to account for developments in the state of technology and available information;

[19] Bill C-27 (CPPA), sections 21, 22, 39.

3. maintain documentation on the de-identified PI held[20], the manner of de-identification used, and the risk assessments conducted by the public body;
4. maintain a record of disclosure of de-identified PI including to whom it was disclosed;

v. a general prohibition for *any person* to re-identify PI or attempt the same except for the purposes of testing the de-identified status of this information which would enable security researchers to attempt to re-identify this data in the public interest following a code of conduct in doing so (e.g., similar to the responsible security vulnerability disclosure process);

vi. a requirement that an organization notify the Commissioner without undue delay on learning, following the disclosure of de-identified PI to any person, that the information has been or may be re-identified;

vii. a requirement that *any person* that has received de-identified PI from an organization to notify the organization that the PI may be or has been re-identified;

b. make re-identification of de-identified PI an offence outside of a limited set of circumstances (public interest, preventing individual harm, security research);
c. provide the Commissioner authority to issue administrative monetary penalties (see section 10.2 herein) for non-compliance with the de-identification provisions as described in this section; and
d. make de-identified PI fully subject to the Act including for oversight.

Section 9.2. Anonymization

36. That PIPA be amended to define anonymization and include:
    a. standards as to what constitutes anonymized data or otherwise incorporated these into regulation, which must include reasonable technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;
    b. permission for organizations to use PI to create anonymized data;
    c. define "anonymized data" and the following should be included in the Act, regulations or standards set by regulation:
        i. standards as to what constitutes anonymized data;
        ii. a prohibition on organizations:
            1. creation of anonymized data except in accordance with the established standards;

[20] Similar to proposed requirements in Quebec regulation (the proposed de-identification regulation under their public and private sector acts), organizations must keep track of these data-sets, and how they where made. If there is a problem with a technique used to create de-identified information, a breach can be prevented/contained as much as possible by recalling the data and reprocessing (de-identifying) according to new techniques. The risk assessment is an annual or bi-annual exercise to ensure ongoing security/de-identification strength of the data-sets.

2. use of the term “anonymized data” or the like to claim that no PI is being used, etc., or to infer privacy protection, unless the process of anonymization of the PI meets the established standards;

iii. a requirement that organizations:
   1. leveraging anonymization, conduct regular re-identification risk assessments to account for developments in the state of technology and available information;
   2. maintain documentation on the anonymized data held, the manner of anonymization used, and the risk assessments conducted by the public body;
   3. maintain a record of disclosure of anonymized data including to whom it was disclosed;

iv. a general prohibition for *any person* to re-identify PI or attempt the same except for the purposes of testing the anonymized status of this information which would enable security researchers to attempt to re-identify this data in the public interest following a code of conduct in doing so (e.g., similar to the responsible security vulnerability disclosure process);

v. a requirement that an organization notify the Commissioner without undue delay on learning, following the disclosure of anonymized data to any person, that the information has been or may be re-identified;

vi. a requirement that *any person* that has received anonymized data from an organization to notify the organization that the PI may be or has been re-identified;

d. make re-identification of anonymized data an offence outside of a limited set of circumstances (public interest, preventing individual harm, security research);

e. provide the Commissioner authority to issue administrative monetary penalties (see section 10.2 herein) for non-compliance with the anonymization provisions as described in this section;

f. a clause that clarifies that if, for whatever reason, one or more individuals can or may be identifiable from the anonymized data that the information is fully subject to PIPA.

Section 9.3. Synthetic Data

37. That the Committee consider whether to permit organizations to use PI to create synthetic data and include additional provisions regarding the creation and use of this data by organizations. Such provisions should include establishing a standard for the creation of synthetic data, and the assignment of a body responsible for maintaining the standard and assuring the quality (i.e., privacy preserving properties) of synthetic data in practice.

Section 9.4. Defining Sensitive Personal Information

38. That PIPA be amended to include definitions of sensitive and biometric information, and set out the prohibitions, permissions, obligations, and limitations on the collection, use, disclosure and retention of such PI that reflect the level of sensitivity and potential for harm. Specifically:

a. requiring explicit consent from individuals and specific data handling practices with respect to biometric data;
b. having specific retention rules around biometric information; namely a requirement to destroy biometric information when the purpose for its collection is fulfilled;
c. requiring notice to the Commissioner of any system that uses biometric information 60 days prior to its use; and
d. requiring security practices and controls to be commensurate to the sensitivity of the PI processed by the organization.

Section 9.5. Multi-sectoral Information Sharing

39. That PIPA be amended to:
    a. prohibit an organization from using or disclosing personal or health information, including de-identified information, for its own purposes where that information has been shared with the organization for developing InnoTech. This prohibition should be accompanied by an offence provision to ensure compliance; and
    b. include a requirement in PIPA's mandatory Breach reporting provisions for organizations involved in a Breach of personal or health information in their custody that was shared with them by a public body or custodian for developing InnoTech to report the Breach, without unreasonable delay, to the Commissioner in a form and manner determined by the Commissioner.

40. That the Committee recommend that the Minister of Service Alberta and Red Tape Reduction and the Minister of Health ensure appropriate controls are contained in the FOIP Act and HIA for the sharing of personal and health information for InnoTech purposes. Such controls should include:
    a. mandatory PIAs and AIAs and a requirement to provide the assessments to the Commissioner for review and comment;
    b. anonymization assessments prior to the use of anonymized information for the purposes of InnoTech and a requirement to provide the assessments to the Commissioner for review and comment;
    c. a requirement to provide the Commissioner with a copy of any agreement entered into with an organization for development of InnoTech or for any other InnoTech related purpose prior to the transfer of personal or health information to the organization; and
    d. a requirement to conduct an ethical review and provide a copy of the review to the Commissioner for review and comment.

Section 9.6. Artificial Intelligence

41. That the Committee recommend that the Government of Alberta take steps to ensure proper regulation of the use of AI in Alberta to mitigate the risks of harm to the public that may occur as a result of using AI to deliver programs and services to Albertans.

Section 9.7. Regulatory Sandboxes

42. That the Committee consider including provisions in PIPA for the creation and use of a regulatory sandbox operated by the OIPC.

Section 10. Enforcement of the Act

Section 10.1. Offence Fines

43. That PIPA be amended to update the fine structure to bring Alberta in line with other Canadian jurisdictions.

44. That PIPA be amended to add a provision to permit the Court to direct that fines imposed on convictions for offences under PIPA be used for a program or activity that supports or promotes the purposes of PIPA.

Section 10.2. Administrative Monetary Penalties

45. That PIPA be amended to grant the Commissioner power to impose AMPs for non-compliance with PIPA.

46. That the Committee consider offence fines together with AMPs when making recommendations to amend PIPA.

Section 10.3. Commissioner's Orders and Oversight

47. That section 52(3) of PIPA be amended to allow the Commissioner to make an order that the Commissioner considers appropriate if, in the circumstances, an order currently listed in section 52(3) would not be applicable.

4. Introduction

Our submission for the PIPA Review and the recommendations that follow are aimed at modernizing PIPA to:

- Ensure the purpose of the Act adequately balances the right to the protection of PI against the needs of organizations to collect, use and disclose PI in the digital economy and expanded uses of innovative technologies by organizations.
- Ensure there are no gaps in the protection of PI in Alberta that may create unacceptable risks to Albertans.
- Enhance the protection of PI rights for Albertans to ensure adequate protection now and into the future.
- Enable commerce by increasing the accountability measures in PIPA such that it will promote a foundation of trust on which to effectively grow the digital economy in Alberta.
- Enhance the protection of PI by regulating the use or disclosure of non-PI and sensitive PI and the sharing of this information for use by organizations and researchers to innovate or for cross-sectoral initiatives.

- Ensure effective enforcement of PIPA to incentivize compliance.

In formulating our recommendations, we have taken into account the evolution of technology and the amassing of PI that has occurred in the marketplace over the past two decades as described in section 1 of this submission as well as the following, more current developments and trends.

- An increasing share of the economy is part of the service sector and a decreasing share is part of the industrial and agricultural sector.[21] The technology sector in particular has expanded and much of the service sector has started leveraging, or is more intensively utilizing, technologies that process PI.[22]

- Anticipation that technological advances can improve Canada's lagging per capita productivity growth.[23]

- The flow of technology from the technology sector, where it is developed and deployed, to other private sector industries, and to the public and health sectors.

- Increased stress on resources such as health services and certain government sectors, such as social services, due to demographic changes, i.e., an aging population and the highest influx in 50 years of both international and interprovincial migrants into Alberta.[24] The increased use of AI in these sectors to alleviate pressures and improve outcomes.

- The risks to the public, including harm, from the use of AI without proper guardrails.

- The increasing reliance by the education sector on Ed-tech for use by children in schools and the risks of harm to children that may flow from increased exposure to online platforms without proper guardrails, and the development and deployment of this technology.

- The Ministry of Technology and Innovation was established in October of 2022. It leads the Government's efforts under the Alberta Technology and Innovation Strategy to ensure Alberta is the destination of choice for entrepreneurs, innovators and investors, and encourages the commercialization of new technologies in Alberta, with the goal of creating more technology jobs, attracting more technology investment, and diversifying Alberta's economy.

- A strong foundation of research and development of AI in the province as a result of Government funding, several institutions undertaking research and development in AI, a highly trained technology workforce in the province, and various leading AI businesses located in Alberta work as a catalyst for (future) growth.

[21] https://www.businesscouncilab.com/wp-content/uploads/2021/12/Albertas-Economy-Economic-Overview-FULL.pdf.
[22] E.g., the move to personalized insurance, finance, e-commerce, education, medicine etc.
[23] https://www150.statcan.gc.ca/n1/daily-quotidien/231206/dq231206b-eng.htm.
[24] https://www.alberta.ca/population-statistics.

5. Purpose of the Act

This section addresses whether PIPA should be amended to include in its purpose clause a declaration that "informational privacy" – one of the three key elements of the fundamental human right of privacy[25] – should be accorded protection commensurate with its status as a fundamental human right.

Such an amendment would align PIPA with a similar clause in the purpose provision of the proposed Bill C-27, *Consumer Privacy Protection Act* (Bill C-27 (CPPA)), which would have the effect of making it substantially similar with the federal Bill in this regard. It would also align PIPA more closely with the GDPR.

The amendment would also enhance the controls over, and protection of PI afforded by PIPA, by providing guidance, to both tribunals and courts interpreting PIPA's provisions, as to the primacy to be accorded to these statutory manifestations of this fundamental human right.

The discussion will begin with a review of International and Canadian human rights laws, and how privacy fits within these declaratory schemes.

It will then consider the Canadian and Alberta statutes that focus specifically on informational privacy, exploring the particular privacy rights and interests that are protected by the statutory controls and protections over PI. It will also consider Supreme Court of Canada decisions that have commented on these statutes.

The discussion will go on to review similar "foundational commitments" to informational privacy in Bill C-27 (CPPA), as well as in the *General Data Protection Regulation* (GDPR) and in Quebec's Law 25.

Finally, it will reiterate the potential benefits of including recognition of the status of informational privacy as a fundamental human right within PIPA's purpose clause.

The Right to Privacy in the Context of International and Canadian Human Rights Laws

Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Everyone is entitled to these rights, without discrimination. International human rights law lays down the obligations of governments to act in certain ways or to refrain from certain acts, in order to promote and protect human rights and fundamental freedoms of individuals or groups.

<u>UN Declaration on Human Rights</u>

[25] As cited by La Forest, J. in *Dagg v. Canada* (1997)[25], *Privacy and Computers*, the Report of the Task Force established jointly by the Department of Communications/Department of Justice (1972) "… classifies these claims to privacy as those involving territorial and spatial aspects, those related to the person, and those that arise in the information context". The third of these elements - 'Informational privacy' - is the element protected by the personal information protection statutes discussed within.

The UN Declaration on Human Rights was proclaimed by the United Nations General Assembly in Paris on December 10, 1948.[26] Canada became a member on November 9, 1945.

Included in the preamble to the Declaration is the following:

> Whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom,
>
> Whereas Member States have pledged themselves to achieve, in cooperation with the United Nations, the promotion of universal respect for and observance of human rights and fundamental freedoms … .

The General Assembly proclaimed the "Universal Declaration of Human Rights as a common standard of achievement for all peoples and all nations, to the end that every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States themselves and among the peoples of territories under their jurisdiction".

There are 30 Articles specifying the human rights that member states are to recognize and uphold. Among them are the rights to:

- equality and dignity;[27]
- nondiscrimination,[28]
- life, liberty and security of the person,[29]
- protection against arbitrary interference with one's privacy including attacks on reputation or honour,[30]
- freedom of movement,[31]
- freedom of thought, conscience and religion,[32]
- freedom of opinion and expression,[33]
- freedom of peaceful assembly and association,[34]
- free participation in the cultural life of the community… [35]

In addition to the fourth bullet which expressly protects privacy, many of these rights are integrally associated with the values and goals of informational privacy, as will be discussed further below.

---

[26] https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Everyone%20is%20entitled%20to%20all,property%2C%20birth%20or%20other%20status.
[27] Article 1.
[28] Article 2.
[29] Article 3.
[30] Article 12.
[31] Article 13.
[32] Article 18.
[33] Article 19.
[34] Article 20.
[35] Article 27.

Canadian Charter of Rights and Freedoms (Charter)

The Charter came into force in Canada on April 17, 1982, with section 15 coming into force later on April 17, 1985. The intent of the Charter is to protect an individual against state action by governments that infringe on the rights afforded to individuals therein. Among the rights protected by the Charter are:

> Fundamental freedoms – freedom of conscience and religion; freedom of thought, belief, opinion, and expression; freedom of peaceful assembly; and freedom of association.
>
> Legal rights – the right to life liberty and security of the person and the right to be secure against unreasonable search or seizure. Included in the latter right is the reasonable expectation of privacy against state intrusion.

Again, these constitutionally-enshrined freedoms and rights support and are supported by informational privacy.

The Charter does not generally apply to private sector organizations.

Statutory Protection for Informational Privacy in Canada

Private sector privacy laws emerged in Canada in 2000 with the enactment of PIPEDA. PIPEDA applies to organizations who in the course of engaging in commercial activity, collect, use or disclose PI of individuals in Canada. In 2004, Alberta enacted PIPA after PIPEDA's reach extended into Alberta. PIPA was declared substantially similar to PIPEDA. Therefore, PIPEDA does not apply to organizations when they collect, use or disclose PI in Alberta.

Both PIPEDA and PIPA protect an individual's informational privacy rights by codifying the ability of an individual to control their own PI by withholding consent, and by limiting collection, use and disclosure in the absence of consent to specified circumstances, according to the scheme of each law. The purposes in both laws stress balance between an individual's right to control and protection of their own PI, and an organization's need to collect, use or disclose this information for business purposes.

In order to adequately understand the rights that PIPEDA and PIPA are designed to protect, it is important to understand that 'privacy' in the sense of not being observable or subject to intrusion, and 'personal information protection', are not synonymous. The values underlying informational privacy support protection for both private and non-private personal information, such as credit. As noted earlier, informational privacy is an element of the broader concept of "privacy", which is a value, interest, claim, social convention, or moral or human "right'. Both PIPEDA and PIPA confer control and protection for one's PI, whether that information is private in the conventional sense mentioned above, or not.

The interests in and values of privacy that PIPEDA and PIPA protect have a number of dimensions.

First, laws conferring control over PI protect individuals' *preference for privacy* – the desire most people have to keep particular information to themselves or to share it on a limited basis. Such preferences

exist for limitless numbers of particular reasons such as shyness, modesty, safety, protection of intimacy, avoidance of disapproval, or to project a chosen image.

Second, the ability to protect one's own PI is directly linked to *individual autonomy*. American scholar Helen Nissenbaum has explained the "enabling connection between privacy and autonomy" as follows:

> ... freedom from scrutiny and zones of "relative insularity" are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide venues in which people are free to experiment, act, and decide without giving account to others or being fearful of retribution. Uninhibited by what others might say, how they will react, and how they will judge, unhindered by the constraints and expectations of tradition and convention, people are freer to formulate for themselves the reasons behind significant life choices, preferences, and commitments. In defending robust broad protections for informational privacy, Cohen reminds us that autonomy touches many dimensions of peoples' lives, including tastes, behaviors, beliefs, preferences, moral commitments, associations, decisions, and choices that define who we are.[19] [Citations omitted] [Emphasis added]

These related values are often described in terms such as preservation of human dignity and integrity. For example the Supreme Court of Canada, in *R. v. Dyment,* LaForest J. articulated the concept of informational privacy as follows:

> Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual."[20]

Third, the control conferred by PIPEDA and PIPA enables individuals to *avoid or prevent harms* that may arise when information about them is collected, used and disclosed by organizations.

The potential for such harms has been greatly increased by the proliferation of technology that makes the collection and dissemination of PI infinitely easier, broader, deeper and more lasting (viz. "Google Glass"[36]). As well, the advent of facial recognition software and image geolocation techniques makes PI searchable even in the absence of identifying text. [37]

As organizations become more sophisticated in their collection and use of PI for their own purposes, protections must be extended to the individuals whose PI becomes correspondingly vulnerable and, in the wrong hands, potentially harmful. PIPEDA and PIPA provide that protection.

When PIPEDA and PIPA were enacted, the ability of organizations to amass PI about individuals was considerably less given the state of technology at the time and the limited purposes for which PI was collected by organizations. Generally, organizations were not in the position to significantly impact the lives of Canadians through their business activities. However, over time this has changed. Today, organizations have the capability to wield significant power over individuals and can impact their lives and cause them harm through their use of PI for business activities designed in large part to generate profit.

---

[36] Rose Eveleth, Google Glass Wasn't a Failure. It Raised Crucial Concerns, Wired, 2018. https://www.wired.com/story/google-glass-reasonable-expectation-of-privacy/

[37] This happens for good and for bad by means such as Open Source Investigation Techniques. For an example see Anatomy of a Killing', BBC Africa Eye, 2018.

Supreme Court of Canada Commentary on Statutes Protecting Personal Information

Our Supreme Court of Canada has described informational privacy rights as follows.

In *Dagg v. Canada* (1997)[38], LaForest J., writing for the dissent in a split decision of the Court (5 to 4) had the following to say about the protection afforded by the Federal *Privacy Act*.[39] In reference to the first purpose of that Act, "to protect the privacy of individuals with respect to their personal information", he stated:

> The protection of privacy is a fundamental value in modern, democratic states; An expression of an individual's unique personality or personhood, privacy is grounded on physical and moral autonomy -- the freedom to engage in one's own thoughts, actions and decisions.
>
> Privacy is also recognized in Canada as worthy of constitutional protection, at least in so far as it is encompassed by the right to be free from unreasonable searches and seizures under s. 8 of the *Canadian Charter of Rights and Freedoms*. Certain privacy interests may also inhere in the s. 7 right to life, liberty and security of the person.
>
> Privacy is a broad and somewhat evanescent concept, however. It is thus necessary to describe the particular privacy interests protected by the *Privacy Act* with greater precision. In *Dyment*, I referred to *Privacy and Computers*, the Report of the Task Force established jointly by the Department of Communications/Department of Justice (1972), especially at pp. 428-30. That "report classifies these claims to privacy as those involving territorial and spatial aspects, those related to the person, and those that arise in the information context". It is the latter type of privacy interest that is of concern in the present appeal. As I put it in *Dyment*, at pp. 429-30:
>
> > Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained; see, for example, the *Privacy Act*. . . .
>
> See also: *R. v. Duarte*, "privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself"; Westin, "[p]rivacy is the claim of individuals . . . to determine for themselves when, how, and to what extent information

[38] 1997 CanLII 358 (SCC).

[39] This Act was the first privacy law in Canada. It went into effect on July 1, 1983. The Act was designed to regulate the protection of personal information by a Federal government institutions.

about them is communicated to others"; Charles Fried, "[p]rivacy . . . is control over knowledge about oneself").[40]

[Citations omitted]

In *R. v. Tessling* (2004), Binnie J., writing for the court stated:[41]

> Informational privacy has been defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others": A. F. Westin, *Privacy and Freedom* (1970), at p. 7. Its protection is predicated on the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain . . . as he sees fit. [Citation removed]

In 2013, the Supreme Court of Canada in *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*[42] had occasion to consider PIPA. The appeal involved a decision by an OIPC Adjudicator wherein they found that the United Food and Commercial Workers, Local 401, violated its provisions when it recorded and photographed individuals crossing its picket line for use in its labour dispute.[43]

The following are excerpts from the decision wherein the Supreme Court of Canada commented about PIPA and its protections.

> There is no dispute that *PIPA* has a pressing and substantial objective…
>
> The focus is on providing an individual with some measure of control over his or her personal information: Gratton, at pp. 6 ff. The ability of individuals to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These are fundamental values that lie at the heart of a democracy. As this Court has previously recognized, legislation which aims to protect control over personal information should be characterized as "quasi-constitutional" because of the fundamental role privacy plays in the preservation of a free and democratic society.[44]
>
> > *PIPA*'s objective is increasingly significant in the modern context, where new technologies give organizations an almost unlimited capacity to collect personal information, analyze it, use it and communicate it to others for their own purposes. There is also no serious question that *PIPA* is rationally connected to this important objective.[45]
>
> The beneficial effects of *PIPA*'s goal are demonstrable. *PIPA* seeks to enhance an individual's control over his or her personal information by restricting who can collect, use and disclose personal information without that individual's consent and the scope of such collection, use and disclosure. *PIPA* and

---

[40] *Supra* 36, at paras 65 to 67.
[41] *R v. Tessling*, 2004 SCC 67, at para. 23
[42] 2013 SCC 62 (CanLII).
[43] This decision resulted in PIPA being found unconstitutional because it violated the Union's freedom of expression during a labour dispute, which could not be justified by section 1 of the Charter. Following this decision, PIPA was amended to expressly except from its provisions the collection of personal information by a trade union for the purpose relating to a labour relations dispute (see section 14.1 of PIPA).
[44] *Ibid.,* at para 19.
[45] *Ibid.,* at para 20.

> legislation like it reflect an emerging recognition that the list of those who may access and use personal information has expanded dramatically and now includes many private sector actors. *PIPA* seeks to regulate the use of personal information and thereby to protect informational privacy, the foundational principle of which is that "all information about a person is in a fundamental way his own, for him to communicate or retain . . . as he sees fit".[46]
>
> Insofar as *PIPA* seeks to safeguard informational privacy, it is "quasi-constitutional" in nature.[47]
>
> *PIPA* also seeks to avoid the potential harm that flows from the permanent storage or unlimited dissemination of personal information through the Internet or other forms of technology without an individual's consent.[48]
>
> Finally, as discussed above, the objective of providing an individual with some measure of control over his or her personal information is intimately connected to individual autonomy, dignity and privacy, self-evidently significant social values. [49]

Statutory Recognition of Privacy as a Fundamental Right: Bill C-27 (CPPA) and the GDPR

Bill C-27 (CPPA)

Bill C-27 was tabled on June 16, 2022. Included in the preamble to the Bill is the following:

> Whereas the protection of the privacy interests of individuals with respect to their personal information is essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada;

During second reading of the Bill, MP Ryan Williams (Bay of Quinte, CPC), stated the following about privacy as a fundamental human right in the context of the CPPA which is contained within the Bill:

> Let us be clear. We need new privacy laws. In fact, it is essential to Canadians in this new digital era and to a growing digital future, but Bill C-27 needs massive rewrites and amendments to properly protect privacy, which should be a fundamental right of Canadians. The bill needs to be a balance between the fundamental right to privacy and privacy protection and the ability of business to responsibly collect and use data.[50]

It was noted during second reading by several MPs that the wording used in the preamble falls short of recognizing privacy as a fundamental human right and that in any event, the preamble is not part of the CPPA and the words used therein are not applicable (or non-binding) to the interpretation of the provisions therein.

The Privacy Commissioner of Canada made submissions on the Bill and recommended therein that the Bill should recognize privacy as a fundamental right. In reference to the preamble above noted, the Commissioner stated:

---

[46] *Ibid.,* at para 21.
[47] *Ibid.,* at para 22.
[48] *Ibid.,* at para 23.
[49] *Ibid.,* at para 24.
[50] November 4, 2022, at p. 1235.

> The new English version of the preamble recognizes that the protection of privacy "interests" is "essential to individual autonomy and dignity and to the full enjoyment of fundamental rights and freedoms in Canada." In contrast, the French version of the preamble uses the phrase "droit à la vie privée des individus" (privacy rights of individuals). The preamble ought to use terminology that highlights the fact that we are dealing with "rights", rather than "interests", in both official languages.
>
> A stronger recognition in the law of the importance of the fundamental right to privacy is necessary to foster greater consumer confidence in the digital economy and encourage responsible use of personal information by organizations in a way that supports innovation and economic growth. The OPC believes that the law can achieve both commercial objectives and privacy protection in the pursuit of responsible innovation. However, in those rare circumstances where the two are in an unavoidable conflict, privacy rights should prevail.

In addition to recommending the preamble be amended to recognize that "the protection of the fundamental right to privacy of individuals with respect to their personal information is essential", the Privacy Commissioner also recommended that the purpose section of the CPPA be amended as follows:

> The purpose of this Act is to establish – in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information – rules to govern the protection of personal information in a manner <u>that recognizes the fundamental right to privacy of individuals</u>… [My emphasis]

The purpose statement in the CPPA states as follows:

> **5** The purpose of this Act is to establish — in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information — rules to govern the protection of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

In a letter to the Chair of the Standing Committee on Industry and Technology, which is responsible for reviewing the Bill, sent on or around October 3, 2023 (INDU Committee), the Honourable Francois-Philippe Champagne, Minister of Innovation, Science, and Industry, submitted proposed amendments to Bill C-27 (CPPA).[51] In support of amendments to strengthen the privacy rights of Canadians, among other things, the Minister stated:

> First, we heard directly from the Privacy Commissioner and from a number of others that the Bill needs a stronger foundational commitment to the privacy of Canadians. It is with this in mind that the Government would support a recommendation by the Committee to explicitly recognize a fundamental right to privacy for Canadians. While there is already language in the preamble of the Bill, we believe this

51 https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12600809/12600809/MinisterOfInnovationScienceAndIndustry-2023-10-03-e.pdf.

could specifically be included in the purpose statement of the Bill itself, as echoed by many members of this Committee and others.[52]

The proposed amendment associated with this statement as set out in the Annex to the letter is as follows.[53]

Proposal	Details
Explicitly recognize a fundamental right to privacy for Canadians	To address concerns that the legislation does not explicitly recognize a *fundamental* right to privacy, the Government would propose amending the preamble to the Bill as well as the purpose clause (Section 5) to qualify the right to privacy as a fundamental right. This will ensure that the privacy rights of Canadians are given due importance in the interpretation of the Act.

The Bill is still at the committee stage.

GDPR

In the European Union (EU), human dignity is recognized as an absolute fundamental right. In this notion of dignity, privacy or the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role. Privacy is not only an individual right but also a social value.[54]

The right to privacy in the EU is rooted in the 1950 *European Convention on Human Rights* (ECHR), which states, "[e]veryone has the right to respect for his private and family life, his home and his correspondence".[55]

In 1995, the European Data Protection Directive (Directive) was passed in response to the advent of the Internet and the progression of data driven technology. The Directive established minimum data privacy and security standards. In 2011, following legal challenges to the practices of tech giants, the EU began working on the GDPR. It went into effect in 2018. The GDPR codifies the informational privacy human rights set forth in the ECHR and which also stem from EU Treaties and in the EU Charter of Fundamental Rights (EUCFR).[56]

Article 1 of the GDPR sets out the subject-matter and objectives of the GDPR. It states:

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

[52] *Ibid.,* at p.2.
[53] *Ibid.,* at p.1 of the Annex.
[54] https://www.edps.europa.eu/data-protection/data-protection_en.
[55] https://gdpr.eu/what-is-gdpr/.
[56] https://gdpr.eu/what-is-gdpr/.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.[57]

Privacy as a fundamental right is set out in recitals 1 and 2 of GDPR, recital 1 states:[58]

> The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

The GDPR regulates data protection in the EU.

Data protection is about protecting any information relating to an identified or identifiable natural (living) person, including name, dates of birth, photographs, video footage, email addresses and telephone numbers. Other information such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered personal data.[59]

The notion of data protection originates from the right to privacy and both are instrumental in preserving and promoting fundamental values and rights; and to the exercise of other rights and freedoms - such as free speech or the right to assembly.[60]

Data protection has precise aims to ensure the fair processing (collection, use, storage) of personal data by both the public and private sectors.[61]

In order to maintain its adequacy status so as to continue to allow the free flow of information between the EU and Canada, including as it relates to trade, Canada's privacy laws must be updated such that they align more closely with the GDPR. It is likely these and the other factors mentioned above about the evolution of technology and the data driven marketplace have led the Government of Canada to include in the CPPA recognition of privacy as a fundamental human right.

Recognizing Privacy as a Fundamental Human Right in PIPA's Purpose Clause

While PIPA, through its scheme, is designed to protect informational privacy as described above, it is worth considering whether, given the current digital environment and the risks to the protection of PI in the digital economy, the time has come to expressly require organizations to take into account these and associated human rights of individuals when collecting, using or disclosing PI, as a measure to adequately protect these rights, as is the case in Bill C-27 (CPPA) and the GDPR.

[57] https://gdpr-info.eu/art-1-gdpr/.
[58] https://gdpr-info.eu/recitals/no-1/
[59] https://www.edps.europa.eu/data-protection/data-protection_en.
[60] https://www.edps.europa.eu/data-protection/data-protection_en.
[61] https://www.edps.europa.eu/data-protection/data-protection_en.

As indicated, PIPA will need to maintain its substantially similar status to the CPPA once enacted. In his letter to the Chair of the INDU Committee, Minister Champagne stated the following about the application of the substantially similar status of the CPPA in reference to Law 25.

> I was asked during my appearance about the application of the "substantially similar provision" under CPPA, for example, in the case of Quebec. I would like to reaffirm that the alignment and coordination of privacy regimes are key to effective enforcement nationwide and to maintaining trust and confidence in data flows across Canada. Currently, the Personal Information Protection and Electronic Documents Act (PIPEDA) sets national standards for privacy practices in the private sector, and the CPPA will continue this practice. A few provinces have privacy laws deemed substantially similar to PIPEDA. This means that, in many circumstances, the provincial law applies instead of the federal law. The CPPA, like PIPEDA, contains a clause that will allow the Governor in Council to make regulations to establish criteria to be applied in a determination of substantially similar status (clause 122(3)). The intent is that provinces that provide equal or greater privacy protection to the CPPA and provide for independent oversight and redress will continue to be deemed substantially similar. In the specific case of Quebec, it is anticipated that the designation of their provincial privacy regime as "substantially similar" would continue under the CPPA. [My emphasis]

Further, amending PIPA to recognize informational privacy as a fundamental human right within its purpose clause will influence the interpretation of the protective provisions by the Commissioner, other tribunals, and the Courts in a manner that enhances their operations and affirms their importance.[62]

Recommendation

1. That the Committee consider whether to expressly recognize in the purpose statement of PIPA that the protection of personal information privacy is a fundamental human right.

6. Scope of the Act

Alberta's digital economy will benefit from privacy laws that leave no gaps, where Albertans' privacy rights do not apply. For there to be a trusted ecosystem of privacy protection, enabling economic and social participation and information flow in the Province, all organizations handling PI need to be regulated.

6.1. Political Parties

Currently, only British Columbia's privacy legislation captures the PI collected, used and disclosed by political parties. This means that there are no legislative privacy protections for the collection, use, disclosure, and maintenance of sensitive PI of Albertans by political parties, including voting intentions and other information used to identify specific demographics groups.

[62] The interpretive value of purpose clauses is affirmed in *1704604 Ontario Ltd. V. Pointes Protection Association* 2020 SCC 22 (CanLII, [2022] 3 SCR 587.

PI revealing political opinions is categorized as prohibited information under GDPR,[63] and processing is only allowed for electoral activities, with appropriate processes and safeguards established. Regulators have fined offending parties.[64]

It is of great importance to ensure trust in the democratic process, and in the institutions that are linked to its operations and outcomes. Without elections perceived as fair and transparent, trust in elected officials will erode. Canadian's frustration with the lack of transparency and protection regarding this sensitive PI held by political parties has become evident in the past decade as seen by the increase in complaints and legal actions taken concerning this issue.[65]

In 2018, the Federal, Provincial and Territorial Privacy Commissioners in Canada issued a Joint Resolution[66] wherein they urged their respective governments to ensure Canadian law at all levels carries meaningful privacy obligations for political parties by passing legislation:

- Requiring political parties to comply with globally recognized privacy principles, including in regards to breach reporting;
- Empowering an independent body to verify and enforce privacy compliance by political parties through, among other means, investigation of individual complaints; and,
- Ensuring that Canadians have a right to access their personal information in the custody or control of political parties.

Currently, Albertans do not have the right to complain to the Commissioner about the improper collection, use, disclosure or security of their PI by a political party, or to ask the Commissioner to review a party's response to their request for access to their PI. Political parties are under no obligation to report breaches to the public or to the Commissioner. Consequently, the Commissioner cannot require the party to notify affected individuals of a privacy breach that presents a real risk of significant harm to the individuals.

The addition of political parties to PIPA's scope would help to secure the protection of Albertans' PI and trust in our electoral process.

Recommendation

2. That PIPA be amended to make the Act apply fully to political parties.

[63] See article 9(1) and recital 56

[64] https://iapp.org/news/a/ico-fines-political-party-10k-gbp-over-unlawful-emails/ note that the UK operates under the UK GDPR since Brexit, for all intents and purposes except jurisdiction a clone of the EU GDPR.

[65] See https://www.ctvnews.ca/politics/major-political-parties-under-competition-probe-over-harvesting-of-canadians-personal-info-1.4768501 , https://www.oipc.bc.ca/investigation-reports/2278, https://www.ctvnews.ca/politics/privacy-group-going-to-court-over-alleged-improper-use-of-voters-list-by-liberals-tories-and-ndp-1.5058556 and https://www.theglobeandmail.com/opinion/article-data-protection-laws-must-be-extended-to-political-parties/

[66] https://oipc.ab.ca/resource/joint-resolution-elections/

6.2. Non-profit Organizations

In its 2007 Final Report, the all-party MLA Select Special PIPA Review Committee recommended that PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year transition period (Recommendation #5).[67] The OIPC supported the Committee's recommendation.

In its submission to the Standing Committee on Alberta's Economic Future conducting the 2016 review of PIPA, the OIPC reiterated its long-held position that all not-for-profit organizations should be fully subject to PIPA, as they are in British Columbia.

As noted in the previous PIPA review, the definition of non-profit organization in PIPA "has resulted in different treatment of similar organizations under PIPA (i.e., not-for-profit organizations that fall within the definition and those that do not). This, in turn, has resulted in differences in the way these organizations treat the PI of their clients, employees, volunteers, and donors."[68]

The OIPC maintains its position that all not-for-profit organizations should be fully subject to PIPA.

Under PIPA, a non-profit organization is defined as an organization that is:

- incorporated under the *Societies Act* or the *Agricultural Societies Act*; or
- registered under Part 9 of the *Companies Act* (section 56).

Under the current regime, some not-for-profit organizations do not fall within the section 56 definition of "non-profit organization" and are therefore fully subject to PIPA. These include religious societies, housing cooperatives, unincorporated associations, federally incorporated not-for-profit organizations, and organizations incorporated by private Acts. These not-for-profit organizations have the same obligations under PIPA as other organizations and businesses in Alberta to protect the PI in their custody or under their control. Their clients, donors, volunteers and employees enjoy the same PI protection and rights as the customers, clients, and employees of businesses subject to the Act.

As of May 8, 2024, there are 17,653 active societies under the *Societies Act*, 170 active agricultural societies under the *Agricultural Societies Act*, and 2,203 active non-profit companies under Part 9 of the *Companies Act*. These organizations must comply with PIPA only with respect to PI collected, used or disclosed in connection with a commercial activity.

Having the obligations in PIPA apply only in connection with a commercial activity creates additional inconsistencies for both the organization and individuals when a section 56 non-profit organization undertakes both commercial and non-commercial activities. For example, selling a membership or a fundraising list is a commercial activity. If a section 56 non-profit organization sells the PI of its donors without their consent, the donors can submit a complaint to the Commissioner. However, the donors cannot complain if the organization publishes PI about the donor without consent on its website.

[67] Select Special Personal Information Protection Act Review Committee, Final Report (November 2007) at p. 10.
[68] *Ibid.*

Since PIPA was enacted, approximately 60 cases involving section 56 non-profit organizations have been brought to the OIPC; however, PIPA applied in only a handful of cases. In the remaining cases, the non-profit organization was not subject to PIPA because there was no commercial activity taking place. The Commissioner has not had jurisdiction in any of the self-reported privacy breaches sent to the OIPC by section 56 non-profit organizations. Yet, the privacy breaches suffered by these organizations are typical of those of other organizations, such as missing paperwork; computer system upgrades gone awry; and stolen unencrypted laptops containing PI about many individuals, including banking and credit card information, criminal record checks, and social insurance numbers.

The increased emphasis by government on information sharing initiatives highlights the need to include all not-for-profit organizations under PIPA. Information sharing initiatives are frequently cross-sectoral, with a network of public, health, private and non-profit groups exchanging PI for the delivery of services or programs. While public sector bodies, health custodians and private businesses are subject to privacy laws, the non-profit agencies will not be if they fall within PIPA's definition of a non-profit organization and are not carrying out a commercial activity. However, many of these non-profits handle very sensitive PI about their clients. This is particularly true for those organizations providing social services or health programs, such as emergency shelters, drug or alcohol addiction counselling, and assistance programs for seniors and persons with disabilities. Past Commissioners of the OIPC have consistently stated that the benefits of information sharing should not come at the expense of privacy rights. All parties involved in information sharing initiatives should be regulated by privacy legislation and subject to the Commissioner's independent oversight. If PI is worthy of protection then it must be protected no matter what entity holds the information.

The Alberta Government has also recently announced initiatives to combine expertise between fields, including non-profit and for-profit sectors, to support the use of technological innovation to commercialize research and build capacity in fields such as health care.

As we move towards better enabling multi-sector information sharing projects and socially beneficial innovations, it is important to ensure consistency in how privacy laws apply to the project partners involved. The lack of statutory privacy protection across all organizations in Alberta causes confusion and delays, and may result, for example, in hesitancy to share PI with or receive PI from non-profit organizations that are not subject to privacy law.

There may be concerns that making PIPA apply to those non-profit organizations that are not currently subject to PIPA would add to their administrative burden. PIPA was originally developed with small and medium-sized businesses in mind – to make informational privacy requirements easier to implement and comply with. If small and medium-sized non-profit organizations were fully subject to PIPA, their obligations would be the same as for small and medium-sized businesses. As was recommended in the previous PIPA review, implementation could be delayed one year to allow non-profit organizations to prepare for compliance. The OIPC is willing to work with Service Alberta and Red Tape Reduction to provide resources that would help non-profit organizations understand their obligations under the Act.

Recommendation

3. That PIPA be amended to make the Act apply fully to all not-for-profit organizations, subject to a one-year transition period.

7. Enhancing the Privacy Rights of Albertans

The key challenge of the digital economy and information society is the tension between the potential benefits[69] brought by technological innovation and information driven business models and the handling of negative external effects. These external effects include the shifting of privacy related risks and harms to certain groups of end users, which has the potential for downstream costs to the public and health sectors. This occurs while profits are maximized using PI without effective accountability for such harms, or 'skin in the game' for executives overseeing such business practices. Famous examples include the privacy violations committed by Cambridge Analytica[70] and Tim Hortons[71]. Among the users are children and teenagers who are being harmed as a result of targeted social media content and addictive product design.[72]

To ensure Albertans privacy rights are adequately protected in this context, PIPA needs to be amended to grant Albertans enhanced privacy rights. Doing so will help build trust in the digital economy, which is necessary for it to flourish.

Discussed in this section is the need to embed the 'right of access' to one's own PI under PIPA and the need to enhance the privacy rights of Albertans in line with the rights afforded to citizens in the EU under the GDPR, to Canadians under Bill C-27 (CPPA), and to Quebecers under Quebec's Law 25: the right to be forgotten and right of disposal; the right to data mobility and portability; rights associated with automated decision making; and specific rights for children.

7.1. Right of Access

Under PIPA, any individual may request their own PI from an organization, which is a permissive authority. This permission is set out in section 24. On receiving an access request, an organization must provide access to the information subject to certain limited and specific exceptions.

> 24(1) An individual may, in accordance with section 26, request an organization
>
> > (a) to provide the individual with access to personal information about the individual, or
> >
> > (b) to provide the individual with information about the use or disclosure of personal information about the individual.

[69] E.g. Personalization, productivity gains and other efficiencies, inclusion and voice for marginalized groups, improved outcomes in certain fields such as healthcare and education.
[70] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
[71] https://oipc.ab.ca/wp-content/uploads/2022/06/P2022-IR-01.pdf.
[72] https://www.theguardian.com/technology/2021/sep/14/facebook-aware-instagram-harmful-effect-teenage-girls-leak-reveals and https://www.cbc.ca/news/canada/toronto/ontario-school-boards-sue-social-media-giants-1.7158033 and https://socialmediavictims.org/effects-of-social-media/.

(1.1) Subject to subsections (2) to (4), on the request of an applicant made under subsection (1)(a) and taking into consideration what is reasonable, an organization must provide the applicant with access to the applicant's personal information where that information is contained in a record that is in the custody or under the control of the organization.

Embedding in PIPA that an individual has the *right* to access their own PI would clarify for an organization that access to PI is a 'right' that it is bound to comply with. It would also have the benefit of informing the interpretation of the provisions that permit an organization to refuse access to PI requested in the circumstances listed under section 24(2) or (3) or to sever information from a record requested under section 24(4). Furthermore, including access as a right under PIPA would harmonize the right of access for Albertans across all three laws. Both the *Freedom of Information and Protection of Privacy Act* (FOIP Act) and the *Health Information Act* (HIA) include the right of access to one's own PI or health information in the case of the HIA.

FOIP Act

6 (1) An applicant has the right of access to any record in the custody or control of a public body, including a record containing personal information about the applicant.

HIA

7(1) An individual has a right of access to any record containing health information about the individual that is in the custody or under the control of a custodian.

Recommendation

4. That PIPA be amended to grant Albertans a *right* to access their own PI.

7.2. Right to Be Forgotten

The "right to be forgotten" emerged in the EU around 2014 following a landmark ruling from the European Court of Justice.[73] Since then, various jurisdictions have taken steps to give individuals some recourse when there is information about them that is disseminated – usually on the Internet – and causes them harm. Some jurisdictions have enacted laws that require organizations to de-index PI (i.e., removing hyperlinks to PI) and to no longer disseminate PI, such as Quebec's Law 25. By contrast, other jurisdictions focus on an individual's right to request that their PI be deleted, such as under California law[74] or the proposed scheme included in Bill C-27 (CPPA). Last, some laws, such as the GDPR include both rights.

In all cases, the rights that individuals have to request that their PI be de-indexed, not be further disseminated, or be disposed of are not absolute because there are exceptions that allow organizations to deny requests. In most instances, legislation gives special consideration to the exercise of this right when it comes to children's PI.

[73] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=ecli:ECLI:EU:C:2014:317.
[74] *California Consumer Privacy Act*, CPPA FAQ.

PIPA does not contemplate the 'right to be forgotten' for Albertans as they are relatively new concepts that were introduced in the GDPR (2018), which is well after the last significant amendments to PIPA in 2010. However, including these rights in PIPA is key to balancing the significant power that organizations, and in particular large technology companies, hold over the publication and dissemination of individuals' PI online. It is important to note that PIPA protects the privacy rights of any individual whose PI is collected in Alberta regardless of where the organization operates in the world.

It also worth noting that Alberta businesses are already subject to the extraterritorial scope of the GDPR when they collect PI of individuals who reside in the EU. As such, these businesses are already required to have procedures in place to address these rights in relation to individuals in the EU.

Recommendation

5. That PIPA be amended to codify the 'right to be forgotten' by:
    a. giving individuals the right to request that their PI be de-indexed where the collection, use or disclosure of their PI or the dissemination of their PI constitutes a violation of PIPA or where these activities cause them harm, the latter of which would be subject to a harms test;
    b. giving individuals a right to request the disposal or deletion of their PI:
        i. when the PI is no longer necessary to meet the purpose for which it was collected;
        ii. when an individual has withdrawn consent for further uses or disclosures of their PI,
        iii. when PI was collected, used or disclosed in contravention of PIPA; and
        iv. if the PI was about a minor when it was collected, regardless of who provided it or who gave consent for the collection, use or disclosure of that PI;
    c. subjecting this right to limited and specific exceptions:
        i. for compliance by the organization with a legal obligation;
        ii. exercise of legal rights by the organization or to establish and defend it from legal claims against it; or
        iii. for reasons of public interest, i.e., related to public health or safety.

6. That PIPA be amended to require organizations to take into account any factors surrounding the request, including the individual's reasons and circumstances associated with the request, and whether the subject individual associated with the request is a child or part of a vulnerable population.

7. That PIPA be amended to require organizations to notify the individual whose request is refused at the time of refusal that they may make a complaint to the Commissioner about the refusal.

7.3. Right to Data Mobility and Portability

The right to data portability generally is the right of an individual to obtain their digital PI from an organization or to have it directly transferred to another organization in a "structured, commonly-used machine readable format", subject to certain criteria and exceptions. This right is an important aspect of

an individual's ability to control their own PI, which, as indicated above, is a fundamental principle of informational privacy. The right to data portability is often associated with the right of access.

Another important aspect of data portability is that it enhances competition by facilitating the transfer of an individual's PI to another business. This right ensures that an individual is not locked into doing business with one organization because their digital PI cannot be transferred to or received by another organization offering a similar service. Additionally, it gives the consumer the enhanced ability to more easily switch service providers.

Alberta's PIPA currently does not include a right to data portability. Data portability is one of the new rights being included in modernized privacy legislation to enhance an individual's control over their own PI. This right is found in the GDPR and included in Bill C-27 (CPPA). The Special Committee to Review British Columbia's *Personal Information Protection Act* (BC PIPA Review Committee), recommended in its report "Modernizing British Columbia's Private Sector Privacy Law", issued December of 2021 (BC PIPA Review Report) [75], that the right to data portability be added to British Columbia's *Personal Information Protection Act* (BC PIPA).

Different jurisdictions have taken a variety of approaches with respect to specific features of a data portability requirement, such as whether an organization is only required to transfer an individual's PI directly to another service provider, called data mobility, or also, on request, to the individual themselves. Another consideration is whether the obligation applies to all of an individual's PI or only that which was directly provided by the individual to the organization; and whether there are any exceptions to the obligation.

Recommendation

8. That PIPA be amended to codify the 'right to portability and data mobility' by including therein:
    a. the right of an individual to obtain their PI from an organization in a structured, commonly-used machine readable format; and
    b. the right of an individual to have their PI directly transferred to another organization in a structured, commonly-used machine readable format.

7.4. Automated Decision Making

Using various techniques such as data analytics and AI, a system leveraging an algorithm may assist or fully replace human judgment in making a prediction, recommendation or decision about an individual. For example, a resume screening tool that creates an initial list of candidates for a job interview to which a human resources person is able to add or subtract candidates is an example of assisted decision-making where there is meaningful human involvement (a "human-in-the-loop"). However, a resume screening tool that solely establishes the list of interviewees without any human oversight or ability to influence the result is a fully automated system.

[75] BC PIPA Review Report.

Automated decision making systems can result in a number of benefits to organizations, such as reduced costs, enhanced efficiencies, process optimization, and more consistent decisions. While individuals too can benefit from the use of automated decision making (e.g., quicker and consistent decision-making). However, use of an automated system has the potential to impact individuals, sometimes negatively, in the following ways.

- An individual may not be aware that a prediction, recommendation or decision is being made about them by an automated system.
- An individual may not understand how a prediction, recommendation or decision is made, what information is being relied on, which inputs are the most influential, or the significance or consequences of the process.
- Inaccurate or discriminatory results may occur because outdated or incorrectly interpreted training data is being used or unintentional algorithmic bias[76] exists in the AI's programming logic.
- A prediction, recommendation or decision made by an automated system may directly impact on an individual's life by:
    - affecting their employment opportunities or financial circumstances (e.g., denial of credit, a loan being granted at a higher interest rate), or their ability to obtain certain products or services (e.g., denial of insurance, refusal of rental accommodation); or
    - influencing their behaviour, preferences or choices (e.g., targeted advertising, personalized news feeds).

The significance of the impact is partially dependent on the presence or absence of compensating controls such as:

- Transparency of the process. Clarity for individuals about the PI being used to make the decision, how it is measured or weighed, and how the outcomes are used. If an individual is clear about the PI being used, they will be able to check the accuracy of the PI that is being used to render the decision.
- The ability to object or appeal. The ability to have a human make the decision or to have them review the automated decision.

[76] Bias occurs when the AI algorithms produces results that are systematically unfair to certain group or groups of people. AI bias tends to reflect human bias and can unconsciously creep to the process as a result of the data chosen and assumptions made in training the models. For example, in 2018, Amazon scrapped its then existing AI tool that reviewed and ranked job applications because the tool was proven to be discriminatory against female applicants. Unintentional gender bias existed because the computer programs had been trained on resumes submitted to the company over the previous 10 years, which had mostly come from men, reflecting the male dominance in the tech industry at the time. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

- Accountability and oversight. When automated decision making is used to make decisions that may lead to harm or unfairness to an individual or a group, accountability is essential to mitigate against the risk of harm or unfairness. This can be achieved by requiring proactive reporting of statistics associated with the use of the automated system, requiring internal evaluation of the outputs of the system to protect against harm, requiring the organization to submit a privacy impact assessment (PIA) and/or algorithmic impact assessment (AIA) to the Commissioner. Oversight by the Commissioner of this type of PI processing (such as by giving the Commissioner the authority to audit the system, to review and comment on PIAs or AIAs, and to order an organization to stop using the system) is essential to promote public trust in the use of these kinds of technology.

Modernized privacy laws in other jurisdictions have recognized that additional privacy protections are needed to address the risks associated with use of automated decision making systems. The legislative approaches vary in their scope, such as whether the obligations should apply to only when the automated decision making has a material impact on the individual; whether partial as well as fully automated decision making should be captured; and whether human intervention can be requested.

The GDPR establishes a general prohibition for solely automated decision making, including profiling, when it produces legal or similarly significant effects on the concerned individual.[77] Some exceptions exist, and in those cases individuals have the right to obtain information about the process and to obtain human intervention and to express their point of view.[78] The GDPR gives individuals the right to object to profiling in specific circumstances.[79]

Quebec's Law 25 provides that an organization must inform individuals when it makes a decision based exclusively on an automated system. This is regardless of the significance of the impact of the decision on the individual. In addition, upon request, the organization is required to inform the individual about whom the decision was made the PI used to render the decision, and about the reasons and the principal factors and parameters that led to the decision. The individual has the right to have the PI used to render the decision corrected.[80] The law also allows for a level of human intervention - an individual must be given the opportunity to submit observations to an employee of the organization who is in a position to review the decision.[81] Finally, Quebec's Law 25 specifically addresses profiling and location tracking. An organization that collects PI using technology that includes functions that profile, locate, or identify individuals must inform the individuals, at the time of collection, of the use of the technology and the ability to choose to enable or not enable these functions.[82]

[77] Article 22.
[78] Article 22, Recital 71.
[79] Article 21. Article r defines "profiling" as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".
[80] Section 12.1, *An Act respecting the protection of personal information in the private sector*.
[81] Section 12.1.
[82] *Ibid.,* section 8.1.

Bill C-27 (CPPA) proposes certain obligations when an automated decision system[83] is used (either fully in place of or to assist a human) to make a prediction, recommendation or decision about an individual that could have a significant impact on the individual. The organization is required to include in their organizational policies and practices a plain language, general account of their use of automated decisions systems.[84] Upon request, the organization must provide individuals with an explanation of the prediction, recommendation or decision, including the type of PI used, the source of the information, and the reasons or principal factors that led to the prediction, recommendation, or decision.[85] Unlike the GDPR and Quebec's Law 25, Bill C-27 (CPPA) does not include the right of an individual to contest the decision or express their point of view to a human who can intervene.

In the BC PIPA Review Report, the Special Committee recommended that the BC Government "ensure that PIPA requires an organization to notify an individual that automated processes were used to make a significant decision about them and includes provisions to allow an individual to request human intervention in the decision making process."[86]

To ensure Albertan's are not adversely affected through the use of automated decision making systems, it will be necessary to include rights to mitigate against these risks such as those set out in the GDPR, Bill C-27 (CPPA), and Quebec's Law 25. Including these rights in PIPA will also ensure the privacy rights afforded to Albertans are appropriately balanced against an organizations use of this type of system to innovate in the delivery of services, where such service involves the use of PI. Given the adverse risks to individuals that may result from the use of these systems by organizations, including the risk of harm, there should be adequate oversight by the Commissioner.

Recommendation

9. That PIPA be amended to grant individuals the right to:
    a. contest automated decision making; and
    b. be notified in plain language about the use of an automated decision making system to make the decision before it is made.

10. That PIPA be amended to require organizations that make a profile, prediction, recommendation or decision about an individual using an automated decision making system that either assists or replaces human judgment to:
    a. include in its publically available policies and procedures a plain language general account of the organization's use of automated decision making systems, an individual's privacy rights associated therewith, and how an individual can exercise these rights;
    b. before or at the time of collecting PI directly from the individual, require that individuals be notified about its use of automated decision making, the significance or

[83] Automated decision system is defined as "any technology that assists or replaces the judgment of human decision makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique." (Section 2(1)).
[84] Section 62(2)(c).
[85] Section 63(3).
[86] *Supra* 74*,* at p. 23.

consequences of the same, the related rights of the individual, and the name of a person or position in the organization who can answer questions on behalf of the organization about the use of automated decision making system;

c. if indirectly collected PI is used, the same as under 10. b. applies plus an obligation to disclose where the indirectly collected PI was obtained, and under what authority it is being used;
d. inform the individual about the PI being used to make a profile, prediction, recommendation or decision, the source of the information, and the reasons and criteria used that led to the profile, prediction, recommendation or decision;
e. establish a process to enable the individual to:
    i. review the accuracy of its PI used for automated decision making;
    ii. contest the use of automated decision making to create a profile, prediction, recommendation or decision about them; and
    iii. to request reconsideration by a human after the profile, prediction, recommendation or decision is made.

11. That PIPA be amended to require organizations that use an automated system to make a profile, prediction, recommendation or decision that may lead to harm or unfairness to an individual or group to:
    a. report statistics associated with the use of the automated system in a form determined by the Commissioner or by regulation;
    b. regularly evaluate the outputs of the system to protect against harm and unfairness;
    c. submit a PIA and/or AIA to the Commissioner for review and comment prior to using the automated system; and
    d. permit the Commissioner to establish how AIAs are to be conducted and their content and form.

12. Where an organization plans to use an automated system to make a profile, prediction, recommendation or decision that may lead to harm or unfairness to an individual or group, that PIPA be amended to authorize the Commissioner to:
    a. audit the use of an automated decision making system to ensure the system in its design or use minimizes, to the degree possible, any harm or unfairness that may flow to an individual as a result of the use of the system;
    b. review and comment on PIAs or AIAs submitted by an organization;
    c. order an organization to stop using a system that may cause, has caused or is causing harm to an individual or group.

7.5. Children's Privacy

As the past few years have shown, the internet plays an increasingly important role in children's (which term herein includes youths) lives, from supporting their learning to offering them opportunities to

connect with each other or providing entertainment, among others. However, the pivotal role the internet plays in the lives of children[87] comes with a certain number of risks.

Privacy legislation in Alberta - in the public, health and private sectors – currently recognizes that there are situations in which an individual's rights under these laws may be exercised by another individual, such as a parent or legal guardian exercising the access and privacy rights of behalf of a child,[88] but does not otherwise offer specific protections for children. This approach may have been sufficient at the time PIPA was first enacted. However, the prevalence of internet use or web-enabled services among children in Alberta exposes them to serious risks that can be broadly classified as follows:[89]

- risks of inequalities and discrimination;
- risks to their physical and mental health; and
- risk of privacy violations.

There is mounting evidence that children should be afforded specific protection to help mitigate against these risks. Such protections are now being recognized in several jurisdictions around the world who have passed or are in the process of passing specific laws that target organizations whose business models partially or entirely depend on the collection, use or disclosure of the PI of children. In October 2023, Canadian privacy regulators issued a resolution that calls on all levels of government to consider the privacy of children.[90] With regard to legislative changes relevant to children's PI, we have considered the GDPR, Quebec's Law 25, the Children's code in the United Kingdom, and Bill C-27 (CPPA).

Both Quebec's Law 25 and the GDPR include provisions that require an organization seeking to collect, use or disclose a child's PI to obtain the consent of a child's parent or legal guardian in the case where a child is under a certain age. Quebec's Law 25 sets the threshold at 14, whereas the GDPR provides an age range between 13 and 16, allowing EU member states to make that determination. Bill C-27 (CPPA) provides that age must be factored into an organization's reliance on implied consent, but does not provide a specific age threshold, since the age of majority varies by province/territory, with some also factoring in the mature minor rule.[91]

In addition to age considerations, article 12 of the GDPR requires that information provided to individuals be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child". Bill C-27 (CPPA) includes a similar requirement in section 15(4), which requires that information to individuals be provided "in plain

[87] In this submission, 'minors' refers to all individuals under the age of 18.
[88] See section 61 of PIPA, https://canlii.ca/t/81qp#sec61.
[89] Livingstone and Stoilova. The 4Cs: Classifying Online Risk to Children, https://doi.org/10.21241/ssoar.71817.
[90] *Putting best interests of young people at the forefront of privacy and access to personal information.*
[91] The mature minor concept stems from the ability of a child to comprehend the nature risks and consequences associated with a medical procedure such that they are able to consent to the treatment. The determination of the child's ability to comprehend is undertaken by a regulated member of a health profession, such as a physician. In the context of privacy, this rule would enable a child who can understand the risks and consequences associated with the collection, use or disclosure of their own PI to consent to the same. The rule is codified in section 61(b) of PIPA. In the context of PIPA, presumably the ability to comprehend would be undertaken by an employee or some other delegate of an organization.

language that an individual to whom the organization's activities are directed would reasonably be expected to understand".

Regardless of consent, there is increasingly a consensus among academia, lawmakers and regulators that organizations in the private sector should be prohibited from using children's PI for certain purposes that may be harmful to them. For example,

- The Information Commissioner's Office in the United Kingdom has created a Children's code, which sets out how online services likely to be accessed by children (e.g., apps, online games, and social media) should protect children in the digital world.[92] Among other requirements, the Children's code prohibits profiling or data sharing for children below the age of 13.

- The US Federal Trade Commission (FTC) has proposed a blanket prohibition against Meta (formerly known as Facebook), to prohibit the organization from monetizing children's PI.[93]

- The EU includes a ban on online advertising to children in article 28 of the *Digital Services Act* (DSA).[94]

- California has introduced a Bill aimed at curbing the impact of the addictive design of social media that would include restrictions on the notifications children can receive from addictive social media.[95]

In order to adequately protect Alberta children from the harms that can flow to them from their participation in the digital world, PIPA should include similar prohibitions, restrictions, protections and enforcement mechanisms on the collection, use or disclosure of children's PI.

Bill C-27 (CPPA) takes the approach to define children's PI as "sensitive information" and then specifies that an organization ought to consider the sensitivity of PI as a factor to take into account. It needs to do so for the following:

- when developing a privacy management program;
- when collecting, using or disclosing PI;
- when relying on implied consent to collect PI;
- when determining retention periods;
- when implementing security safeguards; or
- when de-identifying PI.

Bill C-27 (CPPA) also proposes a mechanism for any entity (public or private) to apply to the Commissioner for approval of a Code of practice. Such a Code of practice could be created and guide the

[92] Information Commissioner's Office, *Children's code guidance and resources*, accessed in September 2023.
[93] FTC, *FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data*, accessed in September 2023.
[94] https://www.eu-digital-services-act.com/Digital_Services_Act_Article_28.html.
[95] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB976 .

practices of organizations whose services primarily cater to children, similar to what the Information Commissioner's Office did in the UK.

Lastly, the Canadian privacy regulators in a joint resolution issued last October called on their respective governments to put the best interest of young people first by taking immediate action as necessary to:

- protect young people from commercial exploitation and the use of their PI to negatively influence their behaviour or to cause them harm;
- promote the privacy rights of young people;
- review, amend or adopt relevant privacy legislation to be consistent with internationally recognized policy and legal instruments to ensure adequate protection of the privacy rights of young people; and
- require private sector organizations that collect, use and disclose the PI of young people to:
    - implement strong safeguards;
    - be transparent about these practices;
    - enhance access to effective remedies for young people.

Within the resolution are a number of recommendations for private sector organizations to adopt best practices and on governments to use these practices as a guide to inform legislative reform in the following areas:

- protecting children's privacy by design;
- ensuring transparency;
- requiring privacy by default and prohibiting tracking;
- prohibiting deceptive practices;
- limiting the disclosure of PI;
- enabling deletion and de-indexing, and limiting retention; and
- facilitating access to and correction of PI.

Recommendation

13. That PIPA be amended to offer specific protection for children's PI such by including similar protections for children as set out in Bill C-27 (CPPA), the GDPR, and Quebec's Law 25 or by requiring organizations to adopt a code of practice similar to that of the UK's Children's Code.

8. Duties That Promote Accountability and Public Trust

Organizations subject to PIPA are responsible for PI in their custody or under their control and are accountable for their compliance with PIPA. The "accountability principle" is one of the core privacy principles established by the Organization for Economic Co-operation and Development (OECD) in

1980.[96] These privacy principles are the foundation for Canada's privacy laws, including PIPA and PIPEDA.

PIPA was enacted with certain requirements to promote an organization's accountability. For example:

- organizations must designate one or more individuals to be responsible for ensuring the organization's compliance with the Act (section 5(3));
- organizations are required to develop and follow policies and practices that are reasonable to meet their obligations under the Act, and to make written information about those policies and procedures available upon request (section 6); and
- organizations must make reasonable security arrangements for PI in their custody or under their control (section 34).

As mentioned in section 1 herein, the privacy landscape has changed drastically since PIPA's enactment such that rapid advancements in technology cause large amounts of PI to be generated by individuals through their use of social networks, e-mail, web logs, cell phone GPS signals, call detail records, Internet search indexing, digital photographs, wearable devices, and through online purchase transactions. Businesses are now able to collect, store and analyze vast amounts of PI in ways never contemplated - to gather intelligence and identify trends, to respond with better customer service, improved products and increased marketing. Privacy breaches have proliferated, with incidents often involving the PI of thousands or even millions of individuals at a time. And identity theft has become a pervasive issue.

In this environment, individuals are becoming much more aware of their privacy rights and the importance of protecting them. They need and want to better understand how an organization is handling their PI and what measures are in place to protect their privacy. This understanding is more critical when their PI is being shared by partners in the private, public and health sectors for program or service delivery.

At the same time, organizations are more aware that PI is one of the most valuable assets of an organization and that their business relies on maintaining the trust and confidence of their customers and employees by properly managing PI. Organizations need a better understanding of how to build privacy and accountability into their operations, to help minimize risks, ensure compliance with obligations under PIPA, and strengthen public trust. Building privacy and accountability into an organization's operations will also better situate those organizations to use innovative technologies to improve their business and to compete in the marketplace.

The following sections discuss amendments to PIPA to require organizations to implement tools such as privacy management programs and PIAs in specified circumstances. These sections also discuss proposed changes to the current obligations set out in PIPA for organizations to make reasonable security arrangements to protect PI. These changes are intended to provide additional guidance to

[96] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

organizations in determining the level of security required to protect PI commensurate with the type and volume of PI that needs protection.

8.1. Privacy Management Programs

In their 2012 joint publication, *Getting Accountability Right with a Privacy Management Program*,[97] the Privacy Commissioners of Alberta, British Columbia and Canada provide guidance on what makes a strong privacy management program. The fundamentals include:

- appointing a person to be responsible for the development, implementation and maintenance of the privacy management program;
- developing and documenting internal policies that address the obligations under PIPA and PIPEDA;
- educating and training employees in privacy protection;
- conducting privacy risk assessments;
- managing PI handling by third party service providers;
- having systems in place to respond to individuals' requests for access to (and correction of) PI or complaints about the protection of their PI;
- having breach response and reporting protocols;
- informing individuals of their privacy rights and the organization's program controls; and
- monitoring, assessing and revising their privacy framework to ensure it remains relevant and effective.

The OECD has also recognized the importance of the responsibility for compliance and revised its privacy guidelines in 2013 to include new provisions for implementing accountability within an organization. These provisions require the establishment of a privacy management program that:

- gives effect to the OECD Guidelines for all personal data under its control;
- is tailored to the structure, scale, volume and sensitivity of its operations;
- provides for appropriate safeguards based on privacy risk assessment;
- is integrated into its governance structure and establishes internal oversight mechanisms;
- includes plans for responding to inquiries and incidents; and
- is updated in light of ongoing monitoring and periodic assessment.

An organization must also be prepared to demonstrate its privacy management program to a data privacy enforcement authority, upon request.[98]

[97] Getting Accountability Right with a Privacy Management Program, *https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf.*
[98] *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

In its review of BC PIPA, the BC PIPA Review Committee agreed "that accountability is of critical importance to the effective implementation of [BC] PIPA" and recommended that organizations be required to adopt privacy management programs.[99]

Bill C-27 (CPPA) includes a provision that would require every organization to implement and maintain a privacy management program that includes the policies, practice and procedures the organization has in place to fulfill its obligations under the Act. On the request of the Commissioner, an organization must provide the Commissioner with access to the policies, practices and procedures that are included in its privacy management program and provide guidance on or recommend that corrective measures to its privacy management program.[100] Similar provisions codifying privacy management program content and requirements are included in Quebec's Law 25,[101] and British Columbia's *Freedom of Information and Protection of Privacy Act* (BC FIPPA).[102]

Modernizing PIPA by expressly requiring that organizations have a privacy management program in place will strengthen organizations' ongoing compliance with PIPA and will ensure PIPA remains current and harmonized with developments in accountability in other jurisdictions. It will also contribute to public trust through an organization's ability to demonstrate compliance by having such a program in place. Lastly, it will contribute to responsible use of innovative technologies that involve processing of PI.

Currently, organizations under PIPA are required to develop privacy policies and practices, and to make written information about those policies and practice available upon request. A requirement to have a privacy management program builds upon this existing requirement.

The requirements of a privacy management program should be adaptable and scalable to the size of the organization and to the volume and sensitivity of the PI that is in an organization's custody or control.

Recommendation

14. That PIPA be amended to:
    a. require organizations to have a privacy management program in place;
    b. set out the components of a privacy management program similar to those set out in *Getting Accountability Right with a Privacy Management Program*, or as set out in Bill C-27 (CPPA) or Quebec's Law 25;
    c. require organizations to make publicly available relevant sections of their privacy management program including policies, procedures (access, complaints), practices (security, information management), and privacy contact information; and

[99] *Report of Special Committee to Review the Personal Information Protection Act*, February 2015, at p. 11. The programs are to be tailored to the structure, scale, volume, and sensitivity of the operations of the organization; make the privacy policies of the organizations publicly available; include employee training; and be regularly monitored and updated. In a separate recommendation, the Committee supported mandatory breach reporting by organizations.
[100] Sections 9 and 10.
[101] Section 3.2.
[102] Section 36.2.

d. require that organizations provide information about their privacy management program to the Commissioner upon request.

15. That PIPA be amended to authorize the commissioner to:
    a. audit an organization's privacy management program including its components; and
    b. review and comment on an organization's privacy management program.

8.2. Privacy Impact Assessments (PIAs)

PIAs are a tool that fall under the umbrella of privacy management programs. Preparing a PIA accomplishes a number of objectives, including:

- enabling an organization, through the identification of data flows, to identify the authority to collect, use or disclose PI;
- enabling process mapping which supports business design;
- clarification of accountability for PI;
- enabling the identification of risks to privacy and security;
- enabling risk mitigation including prioritization and timelines;
- facilitating the creation of policy and procedure to ensure adequate protection of the PI involved; and
- identifying those requiring privacy training, including what kind.

PIAs are currently required only under the HIA. However, private sector organizations often process PI that is just as sensitive as health information, noting that some private sector organizations do provide health care but are not custodians under the HIA, as such PIPA applies to this information. Despite this, there is no requirement in PIPA for organizations to complete PIAs when processing this type of PI.

A breach of sensitive PI can have devastating consequences to an individual and can cause them harm. As such, organizations subject to PIPA who process sensitive PI (see section 9.4 herein for the definition of sensitive PI) should be required to prepare PIAs and submit them to the Commissioner for review and comment prior to processing this information.

In addition, there are risks to individuals from profiling and data linking or data matching activities, this is because:

- Individuals are generally unaware when these activities occur and undertaking these activities results in a loss of control over one's own PI given that these activities generate new PI about an individual without their knowledge or consent.
- In some circumstances undertaking these activities can cause harm to an individual or a group.[103]

[103] "For example, the US Department of Health, Education and Welfare (US HEW) data matched its list of welfare recipients with a list of its own employees. This data matching resulted in 33,000 matches. After a year of investigation, US HEW determined there were really only 638 cases of possible fraud. Only 55 of these cases were actually taken to court. (Information technology

Most privacy laws that permit data matching or data linking already require a PIA to be prepared and reviewed by a privacy commissioner in relation to that activity.

Recommendation

16. That PIPA be amended to require organizations to:
    a. conduct PIAs in certain circumstances, such as undertaking activities that involve:
        i. processing sensitive PI;
        ii. profiling and data-linking or data-matching activities; and
        iii. any significant change to an existing program that involves the above-listed information or activity;
    b. submit those PIAs for review and comment by the Commissioner prior to undertaking those activities listed; and
    c. permit the Commissioner to establish the content and form of PIAs.

The proposed requirement by organizations to conduct PIAs is associated with the risks to Albertans from the kinds of processing activities identified above. Where an organization fails to comply with the requirement to submit a PIA to the Commissioner or where the Commissioner has reason to believe that the processing of PI by the organization warrants review against PIPA, the Commissioner should be granted authority to require the organization to submit a PIA to the Commissioner for review and comment. This would give an organization an opportunity to demonstrate to the Commissioner its efforts to comply with PIPA, without the Commissioner having to initiate an investigation.

Recommendation

17. That PIPA be amended to:
    a. authorize the Commissioner to require an organization to provide a PIA to the Commissioner for review where the Commissioner has a reasonable belief that the processing activity creates risks to the privacy rights of Albertans;
    b. authorize the Commissioner to review all PIAs submitted by organizations and comment on any privacy risks associated with the proposed activity and provide recommendations; and
    c. require organizations to respond to any recommendations made by the Commissioner in response to a PIA submitted within 30 days of receipt.

Development and deployment of information systems for use in the health sector

Many PIPA organizations develop information systems that are designed for use in the health sector in Alberta. Although built on PIPA requirements, whenever these systems process identifying health information, their use is often governed by the HIA. It is then up to custodians to submit a PIA to the OIPC that demonstrates compliance with the HIA. This scheme has proven to be problematic.

---

and dataveillance by Roger A. Clarke. Communications of the Association for Computing Machinery, Inc. May 1988. Page 498)" Source: https://oipc.sk.ca/assets/data-matching.pdf.

The duty for custodians to prepare PIAs for information systems is set out in section 64(1) of the HIA. It states:

> 64(1) …each custodian must prepare a [PIA] that describes how …information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is subject of the information.

Section 64(2) requires the custodian to submit the PIA to the Commissioner for review and comment before implementing the system.

Under the HIA, custodians are responsible for collecting, using and disclosing health information in accordance with the HIA. They are also responsible for protecting health information by implementing reasonable technical, physical and administrative controls. Custodians acquire information systems from private sector organizations, usually vendors, for use in the health sector.

The OIPC has encountered many instances where the IT system's design does not comply with the HIA because it was designed to comply with PIPA. This has proven to be significantly challenging for custodians when they submit a PIA to the OIPC for review of an IT system that they have already purchased, but the OIPC subsequently provides feedback that the IT system was not designed to be compliant with the HIA. The HIA's scheme differs significantly from PIPA's. A system designed for use under PIPA will likely not comply with the HIA.

Many custodians, such as primary care physicians, do not have the legal or technical expertise necessary to evaluate the information systems they purchase to operationalize health care delivery services against the HIA requirements. In practice, these custodians rely on vendors to complete and submit a PIA to the OIPC that demonstrates compliance with the HIA. As indicated, in many cases these PIAs do not meet the requirements of the HIA because they were designed to comply with PIPA.

To ensure Information systems designed by vendors comply with the HIA where it is the intent of the vendor to market the IT system to custodians, it is necessary to shift the burden of compliance onto the vendors to ensure the system is HIA compliant.

Where a vendor has submitted a PIA for an IT system intended to be used by custodians to process health information within the terms of the HIA, there is no added benefit to the custodian also submitting a PIA to the OIPC for the same IT system. By shifting the burden of preparing and submitting PIAs that demonstrate compliance with HIA to vendors, as indicated, will appropriately situate the burden where it belongs - on the vendors who profit from the sale of IT systems to Alberta custodians. Another significant benefit, is the shift will reduce extra cost and the administrative burden on the custodian thereby freeing up more time for them to focus on the important task of health care delivery.

Recommendation

18. That PIPA be amended to require organizations that develop information systems intended for use by custodians in Alberta's health sector to process health information governed by the HIA, to submit a PIA to the OIPC for review against the requirements of the HIA before deploying the information system to a custodian.

19. That the Committee recommend to the Minister of Health:
    a. that HIA be amended to relieve the duty of a custodian to prepare and submit a PIA for submission to the OIPC:
        i. for use of an IT system where a PIA was submitted to the OIPC by the organization as required by PIPA;
        ii. the OIPC has reviewed the system against the HIA requirements and any recommendations made by the OIPC for the IT system have been implemented to the satisfaction of the OIPC by the organization;
        iii. the organization provides documented evidence of the OIPC review to the custodian and compliance with any recommendations made by the OIPC; and
        iv. the custodian does not make any modifications that affect privacy risk to the IT system, such as through changes or customization that require further review against the HIA because they were not before the OIPC during its review of the PIA.
    b. that the HIA be amended to require a custodian who has made modifications to the IT system as indicated in 19. a. iv. above, to submit, prior to using the IT system, for review and comment by the OIPC, an addendum to the PIA that was submitted by the organization as required by PIPA, setting out the modifications and how the same will comply with the HIA.

8.3. Mandatory Breach Notification

The breach notification requirements in PIPA requires an organization with control of PI to provide notice of a breach involving the loss of or unauthorized access to or disclosure of PI (Breach) to the Commissioner where a reasonable person would consider that there exists a real risk of significant harm (RROSH) to an individual as a result of the Breach.[104]

The *Personal Information Protection Act Regulation* (PIPA Reg) sets out what must be included in the Breach notice.[105] The Commissioner has authority to require:

- an organization to notify individuals to whom there is a RROSH as a result of the Breach in a form and manner prescribed by the PIPA Reg and within a specified time period;
- an organization to provide any additional information considered necessary to determine whether to require an organization to notify the affected individuals; and
- the organization to satisfy any terms or conditions that the Commissioner considers appropriate regarding the notification.[106]

[104] Section 34.1 (1) and (2).
[105] Section 19 of the PIPA Reg.
[106] Section 37.1.

Organizations must comply with the Commissioner's requirements. PIPA specifies that the Commissioner has exclusive jurisdiction as it relates to the foregoing requirements and must establish an expedited process for determining whether notice is required.[107]

These provisions have served Albertans well over the past 13 years by ensuring that they receive notice about Breaches that may cause them significant harm. Since 2010, more than 2000 Breaches have been reported to the Commissioner by organizations. More than 70% of these were found to be Breaches that may cause a RROSH to affected individuals and notification was required by the Commissioner.

In 2009, breach reporting was new for most organizations in Alberta and in Canada. As a result, the scheme in PIPA reflected that organizations might require support in determining whether a RROSH existed due to a Breach and whether to notify affected individuals. Mandatory breach reporting is now common in most of Canada's privacy laws, including in the public, health and private sectors. Notification allows individuals to take steps to protect themselves from harm that may occur as a result of a breach.

While PIPA requires the Commissioner to establish an expedited process to review Breach notices, the reality is that the process to determine whether notification is required has caused delays in notifying individuals affected by a Breach. The cause of these delays are the result of volume and challenges faced by the OIPC in trying to obtain information required to make a determination about whether there is a RROSH caused by the Breach and whether to require notification. At the end of April 2024, there was a backlog of 204 Breach notices for review.

The sole purpose of Breach notification provisions in privacy laws is to allow individuals to receive timely notification about a Breach that may cause them significant harm, which enables them to take steps to protect themselves from the harm. Any delay in receiving notification increases the likelihood that they will suffer the harm.

Most modernized privacy laws in Canada now include mandatory breach reporting provisions. While there are differing breach reporting schemes in these laws, they all have in common the requirement for the body subject to the law to notify individuals directly and in a timely manner about a breach involving a risk of harm. PIPA's Breach reporting scheme does not contain this requirement. PIPA encourages, but does not require, organizations to notify individuals on its own initiative.

Modifying the mandatory Breach reporting provisions in PIPA as recommended will more closely align with breach reporting requirements across Canada and will create a more harmonized approach to breach reporting for businesses making it easier to report multi-jurisdictional breaches.

To more effectively serve the purpose of the Breach reporting provisions in PIPA, the following is recommended.

Recommendation

20. That section 34.1 of PIPA be amended to require organizations to:

[107] Section 37.1 (3) and (6).

a. without unreasonable delay, directly notify individuals about the Breach where there is a RROSH to the individuals as a result of the Breach;
b. provide the information in the notice to the individuals in plain language that individuals would reasonably be able to understand; and
c. provide the notice to the Commissioner at the same time the notice is sent to the affected individuals.

In recognition that there may be circumstances where an organization cannot directly notify individuals affected by a Breach, the following is recommended.

Recommendation

21. That PIPA be amended to:
    a. include a provision requiring an organization that is unable to directly notify one or more affected individuals as required by section 34.1, to request permission from the Commissioner for indirect notification;
    b. authorize the Commissioner to permit indirect notification on any terms and conditions specified by the Commissioner; and
    c. require the organization to adhere to any terms and conditions for indirect notification established by the Commissioner.

In the PIPA Reg, notice to individuals about a RROSH caused by a Breach requires organizations to, among other things, include a description of the circumstances of the Breach and the steps taken to reduce the risk of harm.[108] It is the experience of the OIPC[109] that it can take some time for organizations to fully understand the cause of the breach and take steps to reduce the risk. Legislation in other jurisdictions acknowledges that gathering all of the information to be included in a notice to individuals may delay that notification. For example, the GDPR states:

> Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

If organizations are required to provide prescribed information to individuals when notifying them of a Breach, PIPA should include a provision permitting organizations to provide the prescribed information in phases, to avoid undue delays.

Recommendation

22. That PIPA be amended to include authority for an organization that is required to notify affected individuals of a Breach, to provide the prescribed information in phases, where necessary, to avoid undue delay in notification.

More recent breach notification requirements in other jurisdictions provide guidance in the legislation for determining when there is a RROSH.

[108] Section 19.1 (1) of the PIPA Reg.
[109] https://oipc.ab.ca/wp-content/uploads/2022/07/PIPA-Breach-Report-2022.pdf see page 22.

Bill C-27 (CPPA) includes a definition of "significant harm", which includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. This proposed legislation also includes factors for determining when a breach represents a RROSH to individuals. Including similar definitions and guidance in PIPA could assist Alberta organizations in determining when its duty to notify individuals is triggered.

Further, it is the experience of the OIPC that some organizations factor in reputational or other harm that may be experienced by the organization or its employees, in its assessment of harm. This has resulted in the organization deciding not to notify individuals affected by a Breach. However, the determination of whether a Breach represents a RROSH to affected individuals should include only factors relating to the affected individuals; organizations cannot 'offset' the risk of harm to affected individuals with concerns about its own harm (or harm to its employees).

Recommendation

23. That PIPA be amended to include a definition for "significant harm" and include factors for use by an organization in determining whether a RROSH exists. A definition or list of factors should clarify that the determination is based on the risks to affected individuals and not risk of harm to the organization or its employees.

Breach reporting and the role of service providers

As discussed in the next section, the role of service providers has grown disproportionately in the past few decades due to the development of cloud services, software as a service, and other mainly technology driven developments. According to a recent survey, at least 29% of organizations suffered a data breach in 2023 caused by a third party.[110] In recognition that most organizations use service providers as part of their operations, many modernized privacy laws contain obligations that hold service providers directly accountable for compliance under these laws including for breach reporting.[111] A service provider under PIPA is defined as "an organization, including without limitation, a parent corporation, subsidiary, affiliate, contractor or subcontractor that, directly or indirectly, provide a service for or on behalf of another organization"[112] (Service Provider).

Under the current mandatory Breach reporting scheme in PIPA, an organization with control of PI is required to provide a Breach notice to the Commissioner. Because of the ubiquitous use of Service Providers by organizations, there are many instances where a Service Provider has custody of PI for its service to the organization (e.g., outsourced payroll services) but does not have control. Control of PI generally rests with the organization on whose behalf the Service Provider is providing the service.

There is no requirement in PIPA for a Service Provider to report a Breach to the organization. Absent a contractual agreement specifying this requirement, there is nothing requiring the Service Provider to

[110] See Global Third-Party Cybersecurity Breach Report, Security Scorecard Feb. 2024 https://securityscorecard.com/wp-content/uploads/2024/02/Global-Third-Party-Cybersecurity-Breaches-Final-1.pdf.
[111] See jurisdictional scan for an overview of PIPA, GDPR, ADPPA and CPPA on these topics.
[112] Section 1(1)(m.3).

notify the organization about the Breach. Failure by a Service Provider to notify an organization about a Breach can cause the organization to violate their Breach notice requirements and can result in individuals affected by a breach where there is a RROSH not to be notified in a timely manner or at all.

Adding these duties for Service Providers will help to protect the reputation of Alberta organizations and better protect Albertans from suffering harm caused by a Breach.

Recommendation

24. That PIPA be amended to require Service Providers:
    a. to notify any organization that contracted the service provider's services about a Breach of PI in the Service Provider's custody immediately upon discovering the breach;
    b. to cooperate with the organization's investigation into the Breach and to make any information accessible to the organization as may be required for the organization to carry out its duties under section 34.1; and
    c. to cooperate with the Commissioner's review of a Breach notice submitted by, or on behalf of the organization.

25. That the PIPA Reg be amended to require organizations to provide information to the Commissioner about the relationship with a Service Provider when a Service Provider is involved in a Breach.

In the early years of mandatory Breach reporting under PIPA, organizations had already notified affected individuals of a Breach by the time the Commissioner was notified in approximately 55% of cases. More recently, that number has increased to 80% of cases. Even given the willingness of organizations to notify individuals, the OIPC has identified cases in which not all affected individuals were properly notified, where the notification did not include the prescribed information, or where the Commissioner found a RROSH to exist when the organization had not.

Given this, the OIPC's oversight role for Breach notification remains essential. Any amendments to the Breach notification provisions in PIPA should be accompanied by appropriate amendments to the Commissioner's oversight authority.

Recommendation

26. That section 37.1(1) of PIPA be amended to reflect the proposed amendment to the Breach notice requirement in section 34.1. Such amendments should include the Commissioner's authority to:
    a. require an organization to notify any individual to whom the Commissioner determines ought to have been notified under section 34.1 but was not notified; and
    b. require an organization to re-notify affected individuals who received notice of a Breach under section 34.1 when the notice does not contain all the information required by the PIPA Reg.

As indicated, notifying affected individuals of a Breach allows those individuals to take necessary steps to protect themselves. However, it does not diminish the likelihood of a similar incident occurring in the

future. The Commissioner currently has authority to conduct investigations to ensure compliance with the Act. Rather than opening an investigation to examine the cause of a Breach, granting the Commissioner review authority within the Breach reporting provisions may be more appropriate as the process of review is a proactive measure that aligns more closely with the activity of reviewing to mitigate the risk of recurrence of a Breach.

Recommendation

27. That the Breach reporting provisions in PIPA be amended to:
    a. grant the Commissioner authority to review the cause of the Breach and to require organizations to take steps that are necessary to mitigate the risk of recurrence - as part of this authority, the Commissioner should be authorized to obtain any information that is necessary to undertake this review; and
    b. require organizations and Service Providers, as applicable, to cooperate with the Commissioner's review of the cause of a Breach and to provide any information requested by the Commissioner to conduct the review.

Bill C-27 (CPPA) includes a requirement for organizations to keep records of breaches of any security safeguards involving PI and to, on request, provide the Commissioner with the record.[113] This duty already exists in the *Personal Information Protection and Electronic Documents Act* and Quebec's Law 25. A duty to record keep for management of Breaches and mitigation to prevent recurrence is an effective way for organizations to demonstrate accountability for the protection of PI and garner public trust.

Recommendation

28. That PIPA be amended to require organizations to:
    a. keep and maintain a record of every breach of security safeguards that impacts PI under its custody or control;
    b. include in the record the facts of the breach, the factors considered in the assessment of harm, and the remedial actions taken; and
    c. on request, provide the Commissioner with access to, or a copy of, the record notwithstanding any other enactment, solicitor-client privilege, or any privilege of the law of evidence.

8.4. Service Providers

As indicated in the previous section, a Service Provider is "an organization, including without limitation, a parent corporation, subsidiary, affiliate, contractor or subcontractor that, directly or indirectly, provide a service for or on behalf of another organization". It is common for organizations to use Service Providers to help conduct their daily business; for example, customer account management, helpdesk or sales systems, information management and technology systems and solutions, etc.

[113] Sections 60 (1) and (2).

Impact of Service Providers on Albertans and Alberta businesses

Many organizations contract with large multi-national companies to provide services such as cloud storage, data processing or other services. When dealing with large companies, organizations often do not have negotiating power, and must accept the terms of service in order to obtain or use the service. In these situations, an organization is in a difficult position to try to ensure that the practices of its Service Provider is compliant with PIPA.

Additionally, it is increasingly common to have complex chains of Service Providers involved in creating the eventual product for an organization. This is particularly true for products leveraging AI, as foundational models are at the core of many privacy concerns. Foundational models are customizable models, such as OpenAI's GPT or Meta's Llama. Implementations of these models are used by other organizations to create customized products that are then delivered to yet other organizations that use these in business processes and in interaction with Albertans. This way, organizations such as those mentioned and products such as the GPT language models can have a disproportionate large downstream effect on privacy.

Current PIPA obligations on organizations and Service Providers

PIPA places the responsibility of a Service Provider's compliance with the Act on the organization engaging the services of a Service Provider. [114] This means that where an organization engages a Service Provider to handle the organization's helpdesk calls, for example, the organization is responsible for ensuring that the Service Provider complies with PIPA with respect to the collection, use and disclosure of PI that occurs in the course of providing the helpdesk service.

Currently there are no explicit requirements placed on the Service Provider under PIPA, although Service Providers *may* be subject to all requirements of PIPA under section 5(6). The lack of clarity around Service Provider accountability under PIPA has created significant confusion for both organizations and its Service Providers. It has also been challenging for the OIPC when investigating any alleged non-compliance involving an organization and its Service Provider in determining accountability under the Act.

It is essential to the protection of PI rights of Albertans that there are adequate provisions included in PIPA that bind Service Providers, along with any downstream Service Providers, to the requirements of PIPA so that they can be held accountable for non-compliance either through the complaint mechanism in the Act or by the Commissioner through their power to investigate any potential non-compliance with the Act. Establishing direct accountability for Service Providers to comply with PIPA will provide more confidence to organization's that the privacy rights of its customers' and clients' will be protected by PIPA when engaging the services of Service Providers.

Modernized obligations for Service Providers

[114] Sections 5(1) and (2).

In recognition of the foregoing challenges regarding service providers, many jurisdictions have opted to expressly place responsibility for complying with requirements of privacy legislation directly on the service provider.

Bill C-27 (CPPA) requires an organization to ensure, by contract or otherwise, that a service provider provides the same or better privacy protection as the organization is required to provide under that Act.

Both Bill C-27 (CPPA) and the GDPR limit the ability of a service provider to collect, use or disclose PI to only activities set out in a contract with the organization who contracts with the service provider.[115] If the service provider fails to comply with the contract, it becomes fully subject to the Act.[116] Importantly, binding a service provider by contract to the organization's obligations under the GDPR is mandatory therein. In the GDPR there are provisions that obligate the service provider to notify the organization with whom the service provider has contracted about breaches and to cooperate in access requests and for the exercise of any other individual rights thereunder.

Lastly, some jurisdictions also require service providers to either give notice to or obtain authorization from the organization before retaining the services of another service provider to provide the service.[117]

Recommendation

29. That PIPA be amended to bind Service Providers and any downstream Service Providers to comply with PIPA similar to that of Bill C-27 (CPPA) and the GDPR, including:
    a. requiring an organization to ensure, by contract, that a Service Provider provides the same or better privacy protection as the organization is required to provide under PIPA;
    b. prohibiting a Service Provider from collecting, use or disclosing PI on behalf of an organization except as permitted by the contract with the organization;
    c. binding the Service Provider to comply with PIPA for any PI collected or in its custody as a result of providing the services, or making the Service Provider subject to PIPA if it fails to comply with the contract;
    d. provisions that will ensure that downstream Service Providers are subject to PIPA the same as Service Providers;
    e. developing regulations about what the contracts should contain, such as:
        i. a requirement to specify the purposes for which the Service Provider is providing the service;
        ii. the purposes for which the Service Provider may collect, use or disclose PI on behalf of the organization to deliver the services;
        iii. that the organization maintains control of PI that is in the custody of the Service Provider for the purposes of providing the service;
        iv. how the PI will be secured by the Service Provider such that the security will be in accordance with the requirements of PIPA;

[115] E.g. GDPR Art. 28, CPPA 11(2).
[116] GDPR Art. 28(10).
[117] See e.g. GDPR, Art. 28(2), 28(3)(d). and ADPPA S302(a)(4).

v. a requirement to cooperate with the organization with respect to the exercise of any right under PIPA by an individual or any duty of the organization (e.g., PIAs);
vi. a requirement that the Service Provider notify the organization in the case of a Breach and cooperate with the organization to ensure the organization can meet its obligation with respect to Breaches under PIPA;
vii. a requirement that the Service Provider notify the organization if it intends to retain the services of a downstream Service Provider and a requirement to inform the organization about the nature of the services to be provided by that Service Provider where such services may involve the collection, use, disclosure, security or management of PI; and
viii. when the agreement comes to an end, whether the Service Provider will be required to return or destroy the PI in its custody and how it will occur.

8.5. Safeguards

Not a day goes by without a headline that a government, municipality, hospital or business experiences an issue with its computer systems, whether they experience an outage or suffer a cyber attack such as ransomware.[118] Regardless of the cause, loss of access to information systems or PI has a detrimental impact on both businesses, whose operations are disrupted, and on individuals, whose PI may be held for ransom, sold on the dark web, used to perpetrate fraud or all of the above.

Historically, private sector organizations have had a duty to protect PI from foreseeable risks. However, these requirements under PIPA and similar privacy laws have been relatively limited. With the dramatic increase in cybercrime, there are legislative reform efforts underway across the world to require more of organizations when it comes to protecting both PI and information systems holding that PI.[119] The EU through the GDPR and Quebec through its Law 25 have already introduced more stringent information security requirements in their respective privacy laws. Similarly, Bill C-27 (CPPA) in its current form proposes increased requirements for organizations.

Given the risks to the privacy of Albertans' PI as described above, it is necessary that PIPA be amended to reflect the heightened importance of adequately protecting the PI of Albertans. For reasons previously stated, it is important to keep PIPA aligned on the laws of Alberta's trade partners nationally and internationally. Information security is a broad topic, other aspects of which are addressed elsewhere in this submission. The focus in this section is solely on security arrangements.

Currently, section 34 of PIPA reads as follows:

[118] Ransomware is a type of malicious software that infects an organization's computer systems and encrypts files on these systems, rendering them inaccessible; cyber criminals who created that software then require that organizations pay them a ransom in exchange of the key to decrypt data.
[119] The latter is not within the scope of this submission.

> An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

This provision is the only requirement on organizations to secure PI. The general requirement to "make reasonable security arrangements" is open to interpretation and does not convey to organizations the critical importance of adequate security arrangements. Privacy laws in other jurisdictions are both more prescriptive and more detailed, and direct organizations to take specific steps in order to protect the PI they are responsible for.

For example, when it comes to the kind of "security arrangements" an organization ought to make, both the EU's GDPR and Bill C-27 (CPPA)[120] require that organizations protect PI through a combination of physical, organizational and technological security safeguards. It should be noted this is already a requirement in HIA and is standard in most modern privacy laws in Canada.

PIPA's standard as to what is reasonable[121] may not suffice when it comes to security arrangements, given the increasing difficulty to adequately secure PI and the expertise it requires.

In line with the security standard in other jurisdictions and across Canada, PIPA should require an organization to protect PI in its custody or control by having in place physical, technical and organizational safeguards that ensure:

- Confidentiality – confidentiality parameters should provide the highest level of confidentiality by default, without any intervention of individuals.
- Integrity – PI should be protected against unauthorized modification or destruction, and could be restored to earlier state if integrity of information is not guaranteed.
- Availability – PI should be available to the organization, the individual, or both, when they need it and where they need it.

When it comes to availability, specifically, as noted at the beginning of this section, it is widely accepted that system outages can occur for any number of reasons, such as natural disasters, component failure, cyber attacks or human error. One should also keep in mind that the interconnected nature of operations across the public and private sectors means that an organization who experiences a system failure could affect the ability of government or health care providers to operate and vice versa. For example, in 2013, an electrical fire in a Calgary data centre operated by a private company crippled multiple public services, including the issuance of fishing licences, registry services and to some extent, access to Alberta's electronic health record, Alberta Netcare.[122] As such, PIPA should be amended to require that an organization be able to restore the availability of information systems and thus access to PI in a timely manner in the event of a physical or technical incident.

---

[120] As of August 2023.
[121] The standard under section 2 of PIPA is "what a reasonable person would consider appropriate in the circumstance".
[122] OIPC Investigation Report F2013-IR-03/P2013-IR-01/H2013-IR-02, *Business continuity planning following a system outage*, available at https://oipc.ab.ca/wp-content/uploads/2022/01/F2013-IR-03-P2013-IR-01-H2013-IR-02.pdf.

The level of safeguards an organization is required to have in order to adequately protect the PI will depend on the following considerations:

- information security risks the organization faces;
- the sensitivity of PI;
- purposes for which the PI is to be used;
- quantity and distribution of the PI; and
- the medium on which it is stored.

These considerations will provide much needed clarity for organizations, help ensure adequate information security and align Alberta's legislated requirements with those of other jurisdictions. In addition, this would avoid placing an unreasonable compliance burden on smaller Alberta-based organizations, since most hold less PI than large corporations.

Lastly, specific information security requirements could be outlined in the PIPA Reg – which is not currently the case – and thus make that aspect of the law more responsive to addressing emerging and significant information security issues. Other privacy legislation[123] includes requirements for due care, that is a continuous effort on the part of organizations to maintain their information security posture by ensuring activities such as vulnerability management and patching take place. Another trend is to include an obligation to ensure employees receive information security training[124], as this is the single most effective way to prevent privacy and security incidents.

Recommendation

30. That PIPA be amended to require that an organization to make security arrangements to protect PI in its custody or control through a combination of physical, organizational and technological security safeguards.
    a. These safeguards should ensure the confidentiality, integrity and availability of the PI and allow for the prompt restoration of information systems following an incident.
    b. The level of safeguards should be commensurate with the information security risks the organization faces, sensitivity of the PI, the purposes for which the PI is to be used, and the quantity and distribution of the PI and the medium on which it is stored.
    c. At a minimum, the security provision in PIPA should include an obligation for security due care (certain minimal steps an organization should take), including the obligation to train its staff.

31. That consideration be given to including in the PIPA Reg specific security requirements that an organization is required to adhere to so as to make the law more responsive to mitigating the risks to security of PI from emerging and significant information security issues.

[123] As set out in i.e. GDPR 32.1(d) and proposed ADPPA s208(b).
[124] Explicitly required under the proposed ADPPA s208(b)(5), CCPA 1798.130(a)(6) and indirectly under GDPR via corporate rules, CoC and DPO requirements.

8.6. Plain Language Requirements

Any person who has signed up for a new digital service likely has experienced the process of scrolling through lengthy, technical, and possibly incomprehensible notices before clicking a box, agreeing to terms and conditions they may or may not have understood.

PIPA requires organizations to provide information to individuals in various circumstances. For example, organizations are required to notify individuals of the purpose for collecting, using and disclosing PI when that PI is collected from the individual with consent. Organizations are also required to provide information about their privacy policies and practices, upon request. Lastly, in response to an access request under PIPA, organizations are required to inform applicants whether the requested information will be provided and if not, why not, as well as to provide information on request as to how the organization has used their PI and to whom it has been disclosed.

PIPA does not set out requirements with respect to the intelligibility or clarity of such notices. In contrast, the proposed Bill C-27 (CPPA) requires that an organizations provides:

- information about its policies and practices in plain language,
- responses to access requests in plain language; and
- information about automated decision systems to individuals in plain language.

Bill C-27 (CPPA) requires specified information to be provided to an individual in order for the individual's consent to the collection, use or disclosure of their PI to be valid, including the purposes for which the information is collected. Bill C-27 (CPPA) further requires that this information be provided "in plain language that an individual to whom the organization's activities are directed would reasonably be expected to understand." This requirement ensures that organizations take into account the circumstances of their audience when obtaining consent. An example would be obtaining consent from youth: in many jurisdictions they are above the age threshold for parental consent, which varies by jurisdiction, but they would still need to be addressed in language that is appropriate for their cognitive abilities to obtain valid consent. Another factor to consider is the increasing complexity of the processing of PI, e.g., by AI or other technology that will need to be explained in understandable terms.

Similarly, Quebec's Law 25 requires that information provided to individuals when obtaining consent must be "in clear and simple language".

Like other private-sector privacy legislation in Canada, PIPA's default position is to require consent to collect, use and disclose PI, with specified exceptions. However, consent is not meaningful if it is not informed; likewise, providing information to individuals is not meaningful if the information is not clear and comprehensible.

In his submission to the BC PIPA Review Committee, the former Information and Privacy Commissioner for British Columbia, Michael McEvoy, recommended the following amendments in support of plain language requirements for obtaining consent for the collection, use or disclosure of PI by organizations under that Act:

Amend PIPA to:

- Require organizations to give notice in writing to ensure that individuals understand what their personal information will be used for, unless consent is implied.
- Require organizations to provide comprehensive, specific, clear and plain notice of all purposes for which individuals' personal information will be collected, used and disclosed, such that it is reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.
- Require organizations to provide notice separate from other legal terms, and to assist any individual to understand what they are being asked to agree to if the individual asks.[125]

In order to ensure that organizations obtain meaningful consent for any PI collected, used or disclosed from Albertans going forward, it is necessary to amend PIPA to clarify that in order for organizations to rely on an individual's consent to collect, use or disclose their personal information, the consent must be informed and that information must be presented in plain language that recipients of the information can understand. Such an amendment would bring PIPA into alignment with the amendments proposed to privacy laws in other jurisdictions, including Bill C-27 (CPPA), as it relates to the plain language requirements.

Recommendation

32. That PIPA be amended to:
    a. require organizations to provide comprehensive, specific, clear and plain notice of all purposes for which individuals' PI will be collected, used and disclosed, such that it is reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting;
    b. clarify that consent is not valid if these requirements are not met; and
    c. require that this notice be given separately from other legal terms.

In order for individuals to more effectively understand and exercise their rights under PIPA when dealing with an organization, the following is further recommended.

Recommendation

33. That PIPA be amended to require an organization to communicate in plain language to an individual or the general public, as applicable, in its policies, procedures, notices, or other correspondence, including responding to access requests, such that the communication that the individual is reviewing or receiving would be understandable to them.

8.7. Ethical Obligations and Duties

Various solutions have been proposed to address the problem that the interests of organizations that are in custody or control of PI (Data Holders) and individuals (Data Subjects) are often misaligned, and are the root cause for much of the privacy harms occurring today. As a result of past social and

[125] https://www.oipc.bc.ca/documents/legislative-submissions/2321.

economic developments, corporate social responsibility has been partially codified into laws such as labor laws and environmental laws that were created to protect society against the adverse effects of corporate interests. Corporate social responsibility implies that corporations have a responsibility to the society that exists around them.[126] The ethical aspects of corporate social responsibility ensure that organizations operate in fair and ethical manner in their treatment of all stakeholders, including their customers.[127]

As indicated in section 1 of this submission, due to the amassing of PI by organizations and technological ability, organizations now have the capability to wield significant power over individuals and can impact their lives, including in harmful ways. This has created a power imbalance that has led academics and lawmakers to try and address.

Loyalty duties have been proposed by scholars as a way to improve privacy laws.[128] Narrowly defined, loyalty duties are defined in section 102 of the proposed *American Data Privacy and Protection Act* (USA ADPPA), but have not made it into the newer proposed *American Privacy Rights Act* (APRA). GDPR takes a somewhat different approach. Article 40 encourages the creation of Codes of Conduct (CoC) to further regulate the relationship of Data subject and Data holders and operationalize what constitutes fair and transparent processing of PI. One active CoC under article 40 is the EU Cloud CoC,[129] which specifies the expected conduct of Cloud Service Providers subject to GDPR. Bill C-27 (CPPA) takes a similar route and proposes the use of codes of practice and certification programs, approved by the OPC, to mitigate the risk of harm to individuals and to address some of the power imbalance.[130]

In order to mitigate the risk of harm to Albertans in the digital economy and correct some of the power imbalance between organizations and individuals, the following is recommended.

Recommendation

34. That the Committee considers whether to codify in PIPA a duty of loyalty, fiduciary duties or CoC, similar to that of other jurisdictions, to promote ethical conduct by organizations handling Albertans' PI.

9. Privacy and Innovative Technology

Alberta is leading the way in Canada in the use of innovative technologies. There are a number of institutes and organizations in the province that are dedicated to this work.

Organizations operating in Alberta are already using innovative technologies and it is anticipated that their use will increase steadily in the coming years. The landscape is ripe for research and development opportunities for technologies that will improve or enhance the delivery of public and health services.

---

[126] Stobiersky, T., What is Corporate Social Responsibility, Business in Society, Strategy, Sustainable Business Strategy, Harvard Business School Online, April 8, 2021: https://online.hbs.edu/blog/post/types-of-corporate-social-responsibility.
[127] *Ibid.*
[128] https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4055&context=faculty_scholarship.
[129] https://eucoc.cloud/en/home.
[130] See sections 76 to 81 of Bill C-27 (CPPA), CPPA.

PI is increasingly valuable as new technological tools have created ways to use this information for new purposes. Large data repositories generate opportunities to create, combine, transfer, learn and infer in a way that has far-reaching impacts on service delivery, research and privacy protection. The challenge of this ongoing digital transformation is to ensure Albertans enjoy all the benefits of progress without eroding rights or becoming the subject of negative effects of such developments.

The Government of Alberta has included in its 20-year plan investments in the use of these technologies to support innovation. Included in this plan is the goal of breaking down silos between the various sectors to support innovation through data sharing.

In 2022, Government formed the Department of Innovation and Technology. Included in the Alberta Technology and Innovation Strategy[131] is a number of "research and commercialization priorities".[132] Among the priorities listed are "health and disease prevention" and "emerging technologies". Mentioned within these priorities are: increased application of digital technologies in health care and communities; advancing novel diagnostics, medical devices and therapeutics; advancing commercialization opportunities in areas of existing strength, including artificial intelligence, machine learning and quantum science; and harnessing the digital economy across sectors, including…big and open data, to encourage digital adoption.[133]

On August 23, 2023, Technology and Innovation Minister, Honourable Nate Glubish announced $13.6 million in grants for 19 projects through the Alberta Innovates Ecosystem Partnerships Program to help non-profit organizations and for-profit companies commercialize research, speed up development or build capacity.[134] As part of the announcement he said:

> My goal, at a high level, is to look for every opportunity to use technology to solve problems in new ways and to deliver better, faster, smarter services to Albertans in everything we do, including in health care.[135]
>
> …
>
> The good news is that when you do that, you have an added benefit of creating jobs, attracting investment, and growing and diversifying our economy.[136]

In response to a question about regulation in the health innovation sector, Minister Glubish was reported to have said:

> Privacy legislation in the province and around the world is out of date and has not kept pace with modern advances in technology.[137]

---

[131] Located at: https://open.alberta.ca/dataset/60b678e2-76d6-4231-a76b-914270ed1a3f/resource/955cd7da-a537-4c6f-a815-cb759d47d8fc/download/jei-alberta-technology-and-innovation-strategy-2022.pdf.
[132] Ibid., at p. 22.
[133] Ibid., at p.23.
[134] AB Today, August 23, 2023.
[135] *Ibid.*
[136] *Ibid*.
[137] *Ibid*.

…

> It will be important to have the strongest privacy protections that Albertans have ever seen while still creating conditions to encourage more innovation.[138]

Circumscribing the appropriate use and regulation of new and emerging technologies such as AI is an enormous undertaking that regulators have recently begun to address. In many ways, regulating these new technologies and industries is beyond the scope of PIPA and privacy law more generally. Nevertheless, these new technologies bring with them significant concerns about their impact on the privacy of individuals.

This section of the submission will address proposed amendments to PIPA to set necessary parameters around the use of these new technologies. It will also raise matters the Committee may wish to consider with respect to changes that may be necessary to other legislation or the creation of other laws in the province, in order to foster innovation while ensuring the highest privacy protections.

New technologies that allow for the storage, linking, and transferring of large amounts of data are enabling the sharing of PI between the public, health, and private sectors. These technologies can support innovation and increase efficiencies in the delivery of services in these sectors. In Alberta, each sector is governed by its own privacy legislation: the FOIP Act in the public sector; the HIA in the health sector, and of course PIPA in the private sector. Although all three pieces of legislation must be reviewed to ensure that appropriate data-sharing can occur across the sectors while maintaining a high degree of privacy protection, this section of the submission will focus solely on proposed changes to PIPA.

Employing de-identification and anonymization techniques are important to ensure in the safe enablement of using and sharing PI for research, development, and service delivery. Currently PIPA does not define or use these concepts. This section will begin with a discussion of these concepts.

9.1. De-Identification and Anonymization

The concepts of de-identifying and anonymizing PI commonly arise in conversations around technological innovation. The terms “pseudonymized”, “de-identified” and “anonymized” mean different things in different pieces of legislation. In practice, these concepts signify varying degrees on a scale. For the purpose of this document, we will use the following qualifications:

- Simple de-identified information - information easily linked to a unique individual;
- Strong de-identified information - information identifiable by a motivated individual;
- Simple anonymized information - information identifiable by a motivated, well-resourced organization or state-level actor; and

[138] *Ibid*.

- Strong anonymized information - information where it is impossible by state of the art knowledge to identify an individual.

It is important to note that information protected on the above scale is subject to decay of that protection over time. Re-identification either by means of breaking encryption or by advanced data-linking (e.g., pattern-of-life analysis, or geo-location) has become easier over time due to increased access to data, cryptographic advances, data analysis techniques, and computing power, and this trend will continue.

9.1.1 Simple de-identification

De-identification is a process that generally means either removing the ability to identify a unique individual from a dataset or the removal of a named individual from a dataset. The later example of de-identification can be done by pseudonymisation (simple de-identification)**,** that is replacing a name, email and other name-like direct identifiers with a substitute, or removing the data. Such de-identification is generally considered weak de-identification.

9.1.2 Strong de-identification

A higher degree of de-identification also addresses the ability to uniquely identify an individual**.** This means addressing (e.g., making abstract, removing or encrypting) indirect identifiers (such as phone number, postal code, place of employment, age) that can be combined to identify a unique individual from a dataset (e.g., via pattern-of-life analyses). An example of this type of de-identification can be found in the second part of the USA's *Health Insurance Portability and Accountability Act* (US HIPAA) Safe Harbor de-identification standard.[139] In practice, the HIPAA de-identification process has been undone by various motivated individuals.[140]

9.1.3 Simple anonymization

A process as set out in, e.g., the HIPAA Safe Harbor rule, can be taken further by privacy preserving techniques (PPT). PPT aims are to achieve differential privacy, which ensures privacy of an individual in a data-set without the loss of statistical relevance of the dataset. Techniques to achieve this include aggregating or otherwise abstracting information, implementing k-anonymity,[141] or using synthetic data.[142] If done according to specific standards that address and test the risk of re-identification, these processes can contribute to making de-identification stronger to the point it could be considered anonymized. The caveat being that it is considered anonymized at the time of processing, and according

[139] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard.
[140] https://www.forbes.com/sites/forbestechcouncil/2019/08/27/medical-data-de-identification-is-under-attack/?sh=5c1b81647782 and https://www.nature.com/articles/s41467-019-10933-3.
[141] Defined in Wikipedia as "*k*-anonymity is an attempt to solve the problem "Given person-specific field-structured data, produce a release of the data with scientific guarantees that the individuals who are the subjects of the data cannot be re-identified while the data remain practically useful." A release of data is said to have the *k*-anonymity property if the information for each person contained in the release cannot be distinguished from at least individuals whose information also appear in the release. Unfortunately, the guarantees provided by *k*-anonymity are aspirational, not mathematical".
[142] See https://journalofbigdata.springeropen.com/articles/10.1186/s40537-018-0141-8 for a primer into privacy preserving techniques.

to the current state of technology and publically available data (simple anonymized information). Over time, this anonymization will likely weaken to a de-identified category. With enough resources and determination or patience, such anonymization may still be (partially) undone.[143]

9.1.4 Strong anonymization

Anonymization can be strengthened by ensuring it is protected against advanced attacks, such as assuming an attacker has perfect knowledge of the steps, techniques and source code used to achieve anonymity.[144] Furthermore, requiring the anonymization to be robust against theoretical/future attacks such as advances in mathematics, quantum computing and failure/deprecation of cryptographic systems would also be required to achieve strong anonymized information.[145] This level of anonymization has practical uses for sensitive PI. There is evidence that malicious actors actively capture[146] such information that is currently too strongly encrypted/anonymized to be of immediate use, but they expect to be able to break the protections at a later point in time when more data for correlation is available, or when techniques to break protection have advanced. This is where strong anonymization would protect and simple anonymization would fall short.[147]

9.1.5 De-identification

GDPR

The GDPR uses the term pseudonymisation, which means (Art.4(5)):

> the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

It elaborates that (Recital 28):

> the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

Bill C-27 (CPPA)

Bill C-27 (CPPA) defines "de-identify" as follows:

[143] See the examples under 9.1.4 for some examples how some PPTs to achieve simple anonymization can be broken (i.e. how partial or full re-identification can take place).
[144] Similar to Kerckhoffs's principle for cryptography.
[145] For a good primer on these topics see: https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf : https://www.gdprsummary.com/anonymization-and-gdpr/ .
[146] https://techmonitor.ai/hardware/quantum/harvest-now-decrypt-later-cyberattack-quantum-computer.
[147] See https://www.cryptomathic.com/news-events/blog/how-to-protect-yourself-against-steal-now-decrypt-later for a primer on the subject.

> 2(1) de-identify means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains.

It also requires organizations to take proportional measures to de-identify PI.

> 74 An organization that de-identifies personal information must ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information.

Lastly, it prohibits re-identification with limited exceptions.

> 75 An organization must not use information that has been de-identified, alone or in combination with other information, to identify an individual except
>
> (a) to conduct testing of the effectiveness of security safeguards that it has put in place;
> (b) to comply with any requirements under this Act or under federal or provincial law;
> (c) to conduct testing of the fairness and accuracy of models, processes and systems that were developed using information that has been de-identified;
> (d) to conduct testing of the effectiveness of its de-identification processes;
> (e) for a purpose or situation authorized by the Commissioner under section 116; and
> (f) in any other prescribed circumstance.

Bill C-27 (CPPA)'s definition of "de-identify" is close to the GDPR definition of pseudonymised personal data.[148] It acknowledges the risks of re-identification and prohibits re-identification in most circumstances, but stops short of the GDPR where that law explicitly requires the same level of protection and obligations for pseudonymised PI as for PI. Instead, it has a proportionality requirement and sets out several circumstances in which de-identified PI is carved out of the Act.[149] Sections 20 and 21 specifically allow an organization to use PI to create de-identified PI and use that information for internal research, development and analysis without an individual's knowledge or consent. De-identified PI can be disclosed without consent to particular bodies under section 39(a) for socially beneficial purposes, which is defined in section 39(2).

In regards to PIPA, de-identified PI has an important role to play in advancing the digital economy. There has to be a clear definition of de-identified PI included in PIPA, and de-identified PI should not be carved out as, in contrast with anonymized information, re-identification is a real risk to privacy. Any permission of collection, use or disclosure of de-identified PI without consent must be balanced with safeguards, transparency, oversight and recourse. A clear standard for de-identification must apply. Such a standard should be more robust than e.g., HIPAA's Safe Harbor standard, and take into account continuous advances in technology used to re-identify, other information available that may be used to re-identify, and the availability of PPT.

Recommendation

35. That PIPA be amended to:

---

148 https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e1489-1-1.

149 Bill C-27 (CPPA), section 2(3).

a. define “de-identified PI” and the following should be included in the Act, regulations or standards set by regulation:
    i. standards as to what constitutes de-identified PI;
    ii. permission for organizations to use PI to create de-identified PI for legitimate purposes such as using de-identification as a security safeguard and for those purposes set out in Bill C-27 (CPPA);[150]
    iii. a prohibition on organizations:
        1. creation of de-identified PI except in accordance with the established standards;
        2. use of the term “de-identified PI” or the like to claim that no PI is being used, etc., or to infer privacy protection, unless the process of de-identification of the PI meets the established standards; and
        3. selling de-identified PI;
    iv. a requirement that organizations:
        1. keep information that can be used to re-identify an individual separate from the de-identified PI and that this information be subject to technical and organizational controls for that purpose;
        2. leveraging de-identification, conduct regular re-identification risk assessments to account for developments in the state of technology and available information;
        3. maintain documentation on the de-identified PI held[151], the manner of de-identification used, and the risk assessments conducted by the public body;
        4. maintain a record of disclosure of de-identified PI including to whom it was disclosed;
    v. a general prohibition for *any person* to re-identify PI or attempt the same except for the purposes of testing the de-identified status of this information which would enable security researchers to attempt to re-identify this data in the public interest following a code of conduct in doing so (e.g., similar to the responsible security vulnerability disclosure process);
    vi. a requirement that an organization notify the Commissioner without undue delay on learning, following the disclosure of de-identified PI to any person, that the information has been or may be re-identified;
    vii. a requirement that *any person* that has received de-identified PI from an organization to notify the organization that the PI may be or has been re-identified;

[150] Bill C-27 (CPPA), sections 21, 22, 39.

[151] Similar to proposed requirements in Quebec regulation (the proposed de-identification regulation under their public and private sector acts), organizations must keep track of these data-sets, and how they where made. If there is a problem with a technique used to create de-identified information, a breach can be prevented/contained as much as possible by recalling the data and reprocessing (de-identifying) according to new techniques. The risk assessment is an annual or bi-annual exercise to ensure ongoing security/de-identification strength of the data-sets.

b. make re-identification of de-identified PI an offence outside of a limited set of circumstances (public interest, preventing individual harm, security research);
c. provide the Commissioner authority to issue administrative monetary penalties (see section 10.2 herein) for non-compliance with the de-identification provisions as described in this section; and
d. make de-identified PI fully subject to the Act including for oversight.

9.2. Anonymization

Neither Bill C-27 (CPPA) nor the GDPR apply to anonymized data. US ADPPA does apply some conditions to the use of anonymized covered data.

Bill C-27 (CPPA) defines anonymized data as "to irreversibly and permanently modify PI, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means".

The GDPR asserts that anonymized data is information that does not relate to an identifiable individual. It includes information that was identifiable but that has been rendered anonymous.

In Quebec, a draft regulation under the *Act respecting the protection of personal information in the private sector (chapter P-39.1)*[152] proposes requirements for PI to be considered anonymized.[153] There are requirements in the regulation that:

- Require the anonymization to be for a purpose consistent with section 23 of the Act respecting the protection of PI in the private sector.
- The process of anonymization must be carried out under the supervision of a person qualified in the field.
- At the beginning of a process of anonymization, an organization must remove from the information it intends to anonymize all PI that allows the person concerned to be directly identified.
- The organization must then conduct a preliminary analysis of the re-identification risks according to criteria further explained in the regulation, as well as the risks of other information available, in particular in the public space, being used to identify a person directly or indirectly.
- Anonymization techniques subsequently applied must be appropriate given the re-identification risk, which must be consistent with generally accepted best practices. The organization must also establish protection and security measures to reduce re-identification risks and analyze such re-identification risk.

[152] https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2023A/106606.pdf.
[153] *Ibid.*

In terms of bullet four in the foregoing list, the standard that must eventually be achieved is as follows:[154]

> The results of the analysis must show that it is, at all times, reasonably foreseeable in the circumstances that the information produced further to a process of anonymization irreversibly no longer allows the person to be identified directly or indirectly.
>
> [For the analysis] it is not necessary to demonstrate that zero risk exists. However, taking into account the following elements, the results of the analysis must show that the residual risk of re-identification is very low:
>
> > (1) the circumstances related to the anonymization of personal information, in particular the purposes for which the body intends to use the anonymized information;
> >
> > (2) the nature of the information;
> >
> > (3) the individualization criterion, the correlation criterion and the inference criterion;
> >
> > (4) the risks of other information available, in particular in the public space, being used to identify a person directly or indirectly; and
> >
> > (5) the measures required to re-identify the persons, taking into account the efforts, resources and expertise required to implement those measures.

The organization then has a duty to regularly re-assess the re-identification risk and if the assessment no longer meets the standard, the information is no longer considered anonymized.

Lastly, there is an extensive documentation obligation for the organization regarding the anonymization purpose, process risk assessments and reassessments.

For the same reasons indicated under section 8.1 De-Identification, PIPA should include a definition of anonymization therein and establish standards and rules to ensure anonymized data remains as such.

Recommendation

36. That PIPA be amended to define anonymization and include:
    a. standards as to what constitutes anonymized data or otherwise incorporated these into regulation, which must include reasonable technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;
    b. permission for organizations to use PI to create anonymized data;
    c. define "anonymized data" and the following should be included in the Act, regulations or standards set by regulation:
        i. standards as to what constitutes anonymized data;
        ii. a prohibition on organizations:
            1. creation of anonymized data except in accordance with the established standards;

[154] *Ibid.,* at section 7.

2. use of the term “anonymized data” or the like to claim that no PI is being used, etc., or to infer privacy protection, unless the process of anonymization of the PI meets the established standards;

iii. a requirement that organizations:
    1. leveraging anonymization, conduct regular re-identification risk assessments to account for developments in the state of technology and available information;
    2. maintain documentation on the anonymized data held, the manner of anonymization used, and the risk assessments conducted by the public body;
    3. maintain a record of disclosure of anonymized data including to whom it was disclosed;

iv. a general prohibition for *any person* to re-identify PI or attempt the same except for the purposes of testing the anonymized status of this information which would enable security researchers to attempt to re-identify this data in the public interest following a code of conduct in doing so (e.g., similar to the responsible security vulnerability disclosure process);

v. a requirement that an organization notify the Commissioner without undue delay on learning, following the disclosure of anonymized data to any person, that the information has been or may be re-identified;

vi. a requirement that *any person* that has received anonymized data from an organization to notify the organization that the PI may be or has been re-identified;

d. make re-identification of anonymized data an offence outside of a limited set of circumstances (public interest, preventing individual harm, security research);

e. provide the Commissioner authority to issue administrative monetary penalties (see section 10.2 herein) for non-compliance with the anonymization provisions as described in this section;

f. a clause that clarifies that if, for whatever reason, one or more individuals can or may be identifiable from the anonymized data that the information is fully subject to PIPA.

9.3. Synthetic Data

Synthetic data is created when a dataset of PI is transformed into fictitious data, without losing statistical significance.[155] This technique is useful when PI is needed to derive insights from or to train AI, as doing so with PI could be prohibited, violate limitation principles, or create a security risk. Using synthetic data can strengthen de-identification or anonymization of PI. It is however, not a silver bullet for protecting PI, as forms of re-identification, such as membership-inference attacks,[156] remain possible.

[155] For more information see https://mostly.ai/synthetic-data/what-is-synthetic-data.
[156] https://arxiv.org/abs/2302.12580.

It could be useful to allow for the use of PI to create synthetic data under PIPA. If allowances are made, meaning synthetic data can be used in place of PI, the creation of synthetic data should be regulated and held to a standard that minimizes the risk of re-identification. It could be described as a de-identification technique and made a part of a de-identification/anonymization regulation or framework. The use of PPT should generally be encouraged and allowed.

Recommendation

37. That the Committee consider whether to permit organizations to use PI to create synthetic data and include additional provisions regarding the creation and use of this data by organizations. Such provisions should include establishing a standard for the creation of synthetic data, and the assignment of a body responsible for maintaining the standard and assuring the quality (i.e., privacy preserving properties) of synthetic data in practice.

9.4. Defining Sensitive Personal Information

PIPA applies to PI, which is defined as "information about an identifiable individual." PIPA often specifies that where a particular action is authorized, it is authorized to the extent reasonable for the purpose. Whether an action is reasonable in a particular circumstance may depend, in part, on the type of PI at issue. For example, an organization is required to adopt reasonable safeguards to protect PI; the type of safeguards that would be reasonable to protect names and contact information may not be sufficient to protect financial or medical information.

However, PIPA does not set out certain categories of PI to which additional protections or limitations apply.

In contrast, legislation in some jurisdictions specifies certain categories of PI, such as sensitive PI, biometric information and PI of children, to which additional protections or limitations apply. For example, Quebec's Law 25 includes a definition for "sensitive personal information"[157], which is defined as information that is "due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, it entails a high level of reasonable expectation of privacy".

The GDPR places greater limitations[158] on the processing of PI that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".[159] Australia's *Privacy Act* contains a similar definition of "sensitive information" and takes a similar approach to that information.

In 2021, the BC PIPA Review Committee in the BC PIPA Review Report recommended that BC's PIPA be amended to "[d]efine new sensitive categories of information in PIPA which would require explicit

[157] Law 25, S13(3) https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/latest/sq-2021-c-25.html
[158] In article 9(1) GDPR Prohibits this processing, except for certain purposes in 9(2).
[159] Article 9.

consent from individuals and specific data handling practices to include: biometric data, political views, religion, sexual orientation, medical information, and information related to children and youth".[160]

A specific subset of sensitive PI is biometric information. The GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data." Biometric data is significantly sensitive for two reasons. One, the information goes to the biological core of an individual (and can even reveal medical conditions[161]). Two, because it cannot, or cannot reasonably be changed if compromised.

The primary uses for biometric information are identification and authentication; for example, fingerprint recognition, voice biometrics, retina scans, and facial recognition.

Also in the BC PIPA Review Report, concerns were expressed about biometric information, noting that "once this type of information is compromised there is no way to secure it again."[162] The BC PIPA Review Committee recommended that the BC Government require organizations to reaffirm the consent of individuals to the collection, use or disclosure of their biometric information with reasonable frequency, and require organizations to delete biometric information at the request of an individual. As noted above, the BC PIPA Review Committee also recommended that biometric information be included as a category of sensitive personal information that requires explicit consent and data handling practices.

The GDPR, Quebec's Law 25, and Illinois' *Biometric Information Privacy Act* all classify or qualify biometric information as sensitive PI and have prohibitions and/or require additional controls, transparency, safeguards, limitations (such as requiring mandatory express consent for processing, and limiting retention) and sometimes special oversight on its processing.

Given the risks associated with the collection, use, disclosure and management of this type of information, which can be severe, PIPA should include measures to mitigate any impact its misuse or a Breach thereof.

Recommendation

38. That PIPA be amended to include definitions of sensitive and biometric information, and set out the prohibitions, permissions, obligations, and limitations on the collection, use, disclosure and retention of such PI that reflect the level of sensitivity and potential for harm. Specifically:
    a. requiring explicit consent from individuals and specific data handling practices with respect to biometric data;
    b. having specific retention rules around biometric information; namely a requirement to destroy biometric information when the purpose for its collection is fulfilled;
    c. requiring notice to the Commissioner of any system that uses biometric information 60 days prior to its use; and

[160] *Supra* 75.
[161] https://www.sciencedirect.com/science/article/pii/S1077314222000522
[162] *Supra* 75.

d. requiring security practices and controls to be commensurate to the sensitivity of the PI processed by the organization.

9.5. Multi-sectoral Information Sharing

Supporting the Government of Alberta's stated plan to invest in technologies to support innovation through data sharing will require the amassing of large data sets and the sharing of these and other datasets among the various sectors, public, health and private. For example, to improve the delivery of public services, information collected during the delivery of these services, which may include PI, may be used to train AI systems to partially or wholly automate services delivery. Another example is in relation to health care delivery innovation. To innovate in this sector will require access to health information. It is widely known in Canada that Alberta is the only province with one central health services agency, Alberta Health Services (AHS).[163] AHS delivers the majority of public health services to Albertans and is a single custodian of health information, holding health information for almost every Albertan, if not all of us. This data set is a treasure trove for developers of AI systems, which can be developed and used for the benefit of Albertans. Once developed, these systems can be commercialized and marketed and sold globally, creating significant opportunities to generate profit.

As indicated, Alberta has three laws that govern the privacy of Albertans' personal and health information. The FOIP Act is a complete governance scheme for the collection, use, disclosure and management, including security, of PI by public bodies. The FOIP Act is not consent-based legislation, meaning that consent is not the primary means of authority to collect, use or disclose PI. This is largely because of the power imbalance that exists between a public service entity and an individual who requires publicly funded services. Some services, such as taxation, are not voluntary. Consent, therefore, cannot meaningfully be obtained in this context. The FOIP Act generally allows a public body to collect, use or disclose PI as necessary in order to facilitate delivery of public services to *an individual*. It is on the basis of the governance scheme in the FOIP Act that public bodies are entrusted to act according to controls established in the law for any collection of PI and for any subsequent use or disclosure of this information.

Similarly, the HIA is a complete governance scheme for the collection, use, disclosure and management of health information by custodians. This law establishes a high standard for the protection of health information in recognition that this kind of information is highly sensitive. The HIA is designed to allow custodians to collect and use health information to deliver health services and to disclose it to other custodians or persons for ongoing care purposes. The scheme permits the sharing of health information without consent in what is referred to as the 'circle of care'. Albertans provide their health information to custodians for the specific purpose of receiving health care and, by virtue of the model designed to protect their health information, entrust those custodians to abide by the rules in the HIA.

In contrast, PIPA is consent-based legislation. PIPA's purposes recognize both the right of an individual to have his or her PI protected and the need of organizations to collect, use or disclose PI for purposes that are reasonable. PIPA is consent-based legislation, meaning that consent is the primary means of

[163] Noting here that at the time of writing this submission, Alberta's health system is undergoing restructuring.

individual control over PI by individuals. The consent model in PIPA recognizes that individuals have a choice about who they engage with in acquiring products and services in the private sector market and with whom they chose to share their PI to receive the same. PIPA organizations are prohibited from collecting, using or disclosing PI unless permitted by PIPA.

Innovation in the delivery of public and health services will involve all three sectors. As indicated, the plan of the Government of Alberta includes breaking down silos between the various sectors to support innovation through data sharing, which will likely include the sharing of PI collected in the public sector and health information collected in the health sector.

The Government of Alberta has earmarked $13 million dollars for 19 projects to help non-profit and for profit organizations commercialize research for innovative technologies, including AI (InnoTech). It is unclear if public bodies and health custodians have authority to share personal or health information for the purposes of developing InnoTech solutions for public services or health care delivery. However, this submission is not focused on the operation of the FOIP Act or HIA; the purpose of this submission is to address how any sharing of personal or health information by custodians or public bodies with private sector organizations can be controlled, including through PIPA, so as to mitigate the risks to Albertans as InnoTech advances in the province and until the FOIP Act and HIA are reviewed.

Alberta's privacy legislative framework must build in robust constraints to responsibly facilitate the use or disclosure of personal and health information for InnoTech purposes. One constraint is to ensure that a public body or custodian who shares personal or health information with a private sector organization, including non-profits, for InnoTech purposes maintains control over the information.

Where personal or health information has been shared with a PIPA organization by a public body or custodian for InnoTech purposes, the organization should be prohibited from using or disclosing personal or health information for its own purposes, including de-identified information. Given the sensitivity of information likely to be shared, there should be an offence for failing to comply with this prohibition.

The organization should also be required to submit to the Commissioner the documented anonymization assessment and decision prior to authorizing any use of anonymized information by the organization.

Organizations involved in a Breach of personal or health information in their custody that was shared for InnoTech purposes should be reported, without unreasonable delay, to the Commissioner in a form and manner determined by the Commissioner.

Recommendation

39. That PIPA be amended to:
    a. prohibit an organization from using or disclosing personal or health information, including de-identified information, for its own purposes where that information has been shared with the organization for developing InnoTech - this prohibition should be accompanied by an offence provision to ensure compliance; and

b. include a requirement in PIPA's mandatory Breach reporting provisions for organizations involved in a Breach of personal or health information in their custody that was shared with them by a public body or custodian for developing InnoTech to report the Breach, without unreasonable delay, to the Commissioner in a form and manner determined by the Commissioner.

40. That the Committee recommend that the Minister of Service Alberta and Red Tape Reduction and the Minister of Health ensure appropriate controls are contained in the FOIP Act and HIA for the sharing of personal and health information for InnoTech purposes. Such controls should include:
    a. mandatory PIAs and AIAs and a requirement to provide the assessments to the Commissioner for review and comment;
    b. anonymization assessments prior to the use of anonymized information for the purposes of InnoTech and a requirement to provide the assessments to the Commissioner for review and comment;
    c. a requirement to provide the Commissioner with a copy of any agreement entered into with an organization for development of InnoTech or for any other InnoTech related purpose prior to the transfer of personal or health information to the organization; and
    d. a requirement to conduct an ethical review and provide a copy of the review to the Commissioner for review and comment.

9.6. Artificial Intelligence (AI)

Although the regulation of new technologies such as AI go beyond the scope of PIPA, the use of AI represents significant privacy concerns. Generative AI such as ChatGPT interacts with individuals, collects PI and tailors it's response to the person using the system. Many if not most AI based business products are effective because they have the ability to personalize and profile the customers interacting with the AI system.[164]

Bill C-27 (CPPA) includes the creation of the *Artificial Intelligence and Data Act* (AIDA); the stated aim of this legislation is to:

- establish common requirements for the design, development, and use of AI systems, to be applied across Canada; and
- prohibit certain conduct that may result in serious harm to individuals or their interests.

Notably, the proposed AIDA will apply to international and interprovincial trade and commerce associated with AI systems. This leaves intraprovincial regulation of AI to the provinces.

[164] For examples see https://www.forbes.com/sites/jiawertz/2024/02/07/ai-and-personalization-in-the-age-of-automation/

Separate legislation may be required to regulate the use of AI systems in general in the province, where these systems are high risk[165] or where they may affect fundamental rights including regarding non-discrimination, fair process and outcomes, privacy, human rights and the rights of the child.[166] Such a regulatory scheme has been recently passed in the EU in its *AI Act*.

The province could benefit from a standalone law to regulate the use of AI systems across all sectors to ensure there is consistent and effective regulation to mitigate the harms and oversight for infractions, such as by the Commissioner wearing her Information Commissioner hat.

The OIPC would be pleased to discuss with the Government of Alberta how best to regulate the use of AI in Alberta.

Recommendation

41. That the Committee recommend that the Government of Alberta take steps to ensure proper regulation of the use of AI in Alberta to mitigate the risks of harm to the public that may occur as a result of using AI to deliver programs and services to Albertans.

9.7. Regulatory Sandboxes

Regulatory sandboxes are facilities created and controlled by regulators to allow for the testing and experimentation of new products or services before these become widely accessible. For the providers of services and products, sandboxes offers an opportunity to experiment with a limited scale test of their product or service, while gaining valuable feedback on what regulatory risks there are, and what compliance barriers need to be overcome if any before their product or service can go to market. Regulators have an opportunity to learn about innovations that are within their mandate. This is especially useful when the Acts and Regulations have not been written with such innovation in mind. Regulatory sandboxes have been in use for some time by financial regulators to test the workings and impact of new financial products and services. For example, the Alberta *Financial Innovation Act* allows for this type of testing in the financial sector already.

An example of how a sandbox works in relation to privacy law, is the regulatory sandbox conducted by the UK Information Commissioners Office and digital healthcare solutions provider Novartis.[167] In this case, the use of voice enabled record keeping and remote patient care were tested in the sandbox to see how GDPR would apply and what obligations needed to be met.

Impact on Albertans and Albertan businesses

A regulatory sandbox for PIPA would provide opportunities for providers of disruptive technology such as AI, blockchain technologies, etc., to safely test and experiment with their product or service and learn how it can become compliant with PIPA.

---

[165] The EU AI Act designates an AI system as high risk if either the criteria of article 6 apply or if the system performs a task or otherwise qualifies according to annex 3.

[166] The EU AI Act prohibits AI practices that are detrimental to fundamental rights in Article 5

[167] https://ico.org.uk/media/for-organizations/documents/2619244/novartis-sandbox-report.pdf.

As long as Alberta's legislation remains substantially similar to Federal private sector privacy law, and our Federal private sector privacy law retains equivalency status with the protected afforded to EU citizens under the GDPR, such a sandbox exercise could result in a competitive advantage when taking Alberta made products or services, national or global.

Benefits

For organizations, engaging in a sandbox with the OIPC in an early phase of disruptive technology product development would have the added benefit of:

- building compliance requirements and privacy protection in to design of new products and services;
- reducing development cost and time to market due to less chance on having to do costly adjustments in later stage design;
- preventing or reducing issues of non-compliance (such as breaches); and
- enhancing the trust of Alberta consumers and investors in the products and services provided.

Another added benefit of the sandbox is a more agile approach to regulating and oversight. As issues emerge in the sandbox environment, regulators can learn what the risks are and how to address and mitigate these before harm occurs industry wide (e.g., by issuing orders or providing guidance). Any risks that cannot be adequately addressed under the current regulator's mandate will be communicated to the legislature before adoption of disruptive technology takes off.

Recommendation

42. That the Committee consider including provisions in PIPA for the creation and use of a regulatory sandbox operated by the OIPC.

The following may inform these provisions.

- Alberta's innovation and PIPA's regulatory regime could benefit from the introduction of a regulatory sandbox where disruptive technology is involved.

- Participation in a regulatory sandbox should not completely exempt participants from liability under and compliance requirements with PIPA. Exemption from any one provision[168] should be, reasonable, necessary, limited, time bound, risk measured and monitored.

- During the sandbox stage, where possible, usage of non-PI related test data, anonymized, synthetic or de-identified PI should be required (in that order).

- Checks and balances must be built in to PIPA if its sandboxing includes exemptions of provisions (see e.g., sections 8(3), 9, 10(1)(c), and 10(4) of the Alberta *Financial Innovation Act*)

- Consideration should be given to the model of regulatory sandboxing:

[168] See e.g. 7(4) of the Alberta *Financial Innovation Act.*

- One modular sandbox for multiple regulators or authorities. Regulators participate depending on subject matter and impact. One authority coordinates the sandbox. For example, AI will often touch on fairness of process and decisions (Ombudsman), may involve human rights (Human Rights Commission), may include medical research or decisions (Research Ethics Boards), etc.

- A sandbox per regulator. Regulators involve other regulators according to need or as mandated by the applicable Act. (See e.g. Sec. 5 in the Alberta *Financial Innovation Act*).

10. Enforcement of the Act

Privacy regulation requires a variety of strategies to ensure compliance. The majority of organizations understand that consumer trust is paramount. Compliance with privacy laws builds trust and is good for business.

As seen around the world, however, some organizations require greater motivations to comply with the law. Currently, the Commissioner can sanction serious violations of Albertan's privacy rights only by ordering an organization to do what the law requires in the first place, that is, to comply with PIPA's requirements.

PIPA does not incentivize investing in information security as penalties for non-compliance are, especially for larger organizations, negligible in comparison to the costs associated with proper protection of PI. From a cost-benefit perspective, it makes sense to reserve a fraction of the costs of creating a strong information security framework for litigation and fines, as opposed to ensuring compliance.

Jurisdictions around the globe have strengthened the oversight and penalty regimes in public, health and private sector privacy laws. These strengthened measures include giving privacy regulators the ability to administer monetary penalties.

There are elements of privacy protection that are so fundamental that serious, repetitive or long-term infractions require significant penalties. A regime that includes administrative monetary penalties and significant penalties for offences would act as a sufficient deterrent that few penalties would be imposed.

Enforcement of PIPA also includes the Commissioner's oversight role. Modernizing the Act in harmony with other jurisdictions requires an update to the Commissioner's powers currently set out in PIPA.

10.1. Offence Fines

Fines for offences in Alberta are currently well below the proposed fine structures in Quebec's Law 25 and Bill C-27 (CPPA). Ensuring that privacy protections in Alberta are equal to those in other jurisdictions includes updating the fine structure in PIPA to be commensurate with those other jurisdictions.

Recommendation

43. That PIPA be amended to update the fine structure to bring Alberta in line with other Canadian jurisdictions.

In its 2007 Final Report, the all-party MLA Select Special PIPA Review Committee recommended that PIPA be amended to allow the courts the discretion to direct that a fine imposed under the Act be used for a program or activity that supports or promotes the purposes of the Act (Recommendation #46). This is also known as 'creative sentencing'. As noted in the OIPC's submission to the 2006-2007 Select Special PIPA Review Committee, similar provisions exist in other Alberta statutes, including the *Occupational Health and Safety Act* and the *Environmental Protection and Enhancement Act.* For example, the former includes a provision allowing the court to direct funds to programs that benefit the health and safety of workers, which courts have interpreted to include such things as college safety programs, or programs to airlift injured workers. The environmental legislation is even broader, and funds have been directed to charities, wetland reclamation projects, etc.

The OIPC maintains its position that PIPA should be amended to allow for creative sentencing.

Recommendation

44. That PIPA be amended to add a provision to permit the Court to direct that fines imposed on convictions for offences under PIPA be used for a program or activity that supports or promotes the purposes of PIPA.

10.2. Administrative Monetary Penalties

Administrative monetary penalties (AMPs) are an increasingly common regulatory compliance tool that can be imposed directly by a regulator (such as the Information and Privacy Commissioner). Unlike criminal or quasi-criminal fines, AMPs do not require prosecution by the crown and a finding of guilt by a court. The ability to impose AMPs may encourage and reinforce statutory compliance by organizations.

Although AMPs are relatively new in privacy law, many Alberta statutes include AMP regimes (see for example, Alberta's *Consumer Protection Act*). In the privacy realm, AMPs are present in the GDPR, Ontario's *Personal Health Information Protection Act* (ON PHIPA), Quebec's Law 25, Bill C-27 (CPPA) and has been recommended in 2020 by British Columbia's Information and Privacy Commissioner to the BC PIPA Review Committee for inclusion in BC PIPA.[169]

Generally Alberta statutes set out maximum fines, often but not always ranging from $10,000 to $100,000. However, AMPs under privacy statutes (both enacted and proposed), often consider percentages of revenue up to a maximum of millions. If Alberta's PIPA is to be considered substantially similar to Bill C-27 (CPPA), its enforcement provisions must be enhanced. Bill C-27 (CPPA) includes AMPs to a maximum of the higher of $10,000,000 or 3% of the previous year's global revenues, which is broadly consistent with both the GDPR, the United Kingdom's *Data Protection Act* 2018, and Quebec's Law 25.

[169] Recommendation 7: https://www.oipc.bc.ca/documents/legislative-submissions/2321.

An AMP regime would make clear that the privacy rights of Albertans are meaningful, well protected and incentivize investments in information security on the front end.

An amendment to include an AMP regime should contain due process requirements, as well as protections against multiple fines or penalties being imposed for the same contravention.

Recommendation

45. That PIPA be amended to grant the Commissioner power to impose AMPs for non-compliance with PIPA.

46. That the Committee consider offence fines together with AMPs when making recommendations to amend PIPA.

10.3. Commissioner's Orders and Oversight

After conducting an inquiry, the Commissioner is required to dispose of the issues by making an order.[170]

Section 52(2) lists the orders the Commissioner may make when the inquiry relates to the organization's decision on whether to give an individual *access* to their PI or to provide information about the use or disclosure of this information. Section 52(2) was amended after the previous PIPA review to allow the Commissioner to make an order that the Commissioner considers appropriate when none of the listed orders would be applicable in the circumstances of a particular case under section 52(2)(b).

Section 52(3) sets out the orders the Commissioner can make when the inquiry relates to a matter *other than an access request* referred to in section 52(2). However, there are instances where none of the enumerated orders in section 52(3) are applicable under the circumstances. For example, section 52(3)(a) allows the Commissioner to confirm that a duty owed under PIPA has been performed by the organization or to require the organization to perform the duty, but the inquiry might determine that there was no duty owed by the organization under the Act. In other situations, an issue might be moot so that there is no reason to make one of the specified orders.

In its submission to the Standing Committee on Alberta's Economic Future conducting the 2016 review of PIPA, the OIPC proposed a technical amendment to section 52(3): that section 52(3) be amended to include a provision similar to section 52(2)(b) to allow the Commissioner to make an order that the Commissioner considers appropriate when none of the orders currently listed in section 52(3) would be applicable.

Recommendation

47. That section 52(3) of PIPA be amended to allow the Commissioner to make an order that the Commissioner considers appropriate if, in the circumstances, an order currently listed in section 52(3) would not be applicable.

[170] Section 52(1).

APPENDIX A – Glossary of Abbreviations

AI	Artificial Intelligence
AIA	Algorithmic Impact Assessment
AIDA	*Artificial Intelligence and Data Act* (part of Bill C-27)
AMP	Administrative Monetary Penalty
BC PIPA	British Columbia's Personal Information Protection Act
BC PIPA Review Committee	The Special Committee to Review British Columbia's PIPA (2021)
BC PIPA Review Report	"Modernizing British Columbia's Private Sector Privacy Law", issued December of 2021, by the Special Committee to Review British Columbia's Personal Information Protection Act
Bill C-27	An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts
Breach of privacy under PIPA	The loss of or unauthorized access to or disclosure of PI (s.34.1(1))
California CPA	California *Consumer Privacy Act*
CoC	Codes of Conduct
Committee	The Standing Committee on Resource Stewardship who is responsible for the review of PIPA
Contracting Organization	an organization who engages the service of another organization to deliver products or services
CPPA	*Consumer Privacy Protection Act* (part of Bill C27)
Data Holders	an Organization that has PI in its custody or control
Data Subjects	an Individual whose PI is in the custody or control of an organization
Directive	European Data Protection Directive
DSA	EU *Digital Services Act*
DSA	EU's Digital Services Act
ECHR	European Convention on Human Rights
Ed-tech	Education Technology
EU	European Union
EUCFR	EU Charter of Fundamental Rights
FOIP Act	Freedom of Information and Protection of Privacy Act
FTC	United States Federal Trade Commission
GDPR	General Data Protection Regulation

GPT	Generative Pre-Trained Transformer
HIA	Health Information Act
INDU Committee	The Parliamentary Standing Committee on Industry and Technology, which is responsible for reviewing Bill C-27
InnoTech	Innovative technologies, including AI
IT	Information Technology
Llama	Large Language Model Meta AI
OECD	Organization for Economic Co-operation and Development
OIPC	Office of the Information and Privacy Commissioner
OPC	Office of the Privacy Commissioner of Canada
PI	Personal Information
PIA	Privacy Impact Assessment
PIPA	Personal Information Protection Act
PIPA Reg	*Personal Information Protection Act Regulation*
PPT	Privacy Preserving Techniques
RROSH	Real risk of significant harm
Service Provider	an organization, including without limitation, a parent corporation, subsidiary, affiliate, contractor or subcontractor, that, directly or indirectly, provides a service for or on behalf of another organization
USA ADPPA	*American Data Privacy and Protection Act*