cybera.ca | info@cybera.ca

# Legislative Assembly of Alberta, Standing Committee on Resource Stewardship: *The Personal Information Protection Act*

Submission from Cybera Inc.

May 31, 2024

Cybera Inc.
Calgary Office: Suite 200, 3512 - 33 St NW, Calgary, AB T2L 2A6 T: 403-210-5333
Edmonton Office: 10055 - 106 Street NW, Edmonton, AB T5J 2Y2
cybera.ca | info@cybera.ca

# Introduction

Cybera is the not-for-profit facilitator of Alberta's Research and Education Network, and is responsible for driving connections, collaborations, and skills growth in the province through the use of digital technology. We operate the Alberta portion of the National Research and Education Network (NREN) — the dedicated pipeline for Canada's unmetered, not-for-profit internet traffic. This network is used by post-secondary institutions, K-12 schools, municipalities, research institutions, and business incubators to connect to similar organizations across Canada, and around the world.

In addition, Cybera is a founding member of the Alberta Rural Connectivity Coalition (ARCC).[1] This coalition of individuals and public-sector organizations advocate for universal access to high-speed internet — at affordable rates — for all Albertans, including those living in rural, remote, First Nations, and Metis Settlements communities.

As the Committee acknowledged in its emerging issues document, this comprehensive review of the Personal Information and Privacy Act (PIPA) is taking place at a crucial moment for personal information protection.[2] Globally, two interrelated trends are developing: the proliferation of automated digital technologies (artificial intelligence, machine learning, and big data), and the development of new legislative and regulatory regimes to address the risks inherent to these technologies. In this new technological paradigm, significant volumes of data are continuously being collected, while the uses and purposes of this collection are determined through algorithmic processes that were largely unknown at the time of collection.

In addition to the pressures this paradigm will place on governments and individuals, the compliance burden for organizations operating in multiple jurisdictions will be significant, particularly if patchwork regulatory regimes continue to exist.[3] As new laws and regulations are developed, decision makers must place a high priority on cross-jurisdictional alignment, both inter-provincially and internationally.

Within this space, a number of new concepts and approaches for personal information protection are being developed and codified into law. Among these are *algorithmic transparency*, *data portability*, and *enhanced consent*. Taken together, these emerging concepts are an acknowledgment of the unique risks inherent within automated digital technologies, as well as the higher standard of trust citizens will require in order to utilize them. In particular, these developments indicate a transition away from personal information protection regulations that are

[1] https://abconnectivity.ca/
[2] https://www.assembly.ab.ca/docs/default-source/committees/rs/pipa-emerging-issues.pdf?sfvrsn=fb63a400_1
[3] https://brooklynworks.brooklaw.edu/bjil/vol46/iss1/8/

governed solely by strict rules around data collection and use. Rather, personal information protection policies must now be centered around a more fundamental understanding of the rights inherent to each data subject.

In Cybera's view, the committee's comprehensive review of PIPA should not only incorporate other jurisdictions' approaches. Rather, this review can be an important opportunity to position Alberta as a leading jurisdiction for digital investment and innovation. Notably, the government's 2022 Technology and Innovation Strategy and the Alberta Digital Strategy (now being developed) both identify a robust privacy protection regime as a key plank in this larger objective.[4] [5]

Cybera commends the committee for accepting comments on this important matter, and looks forward to reviewing the committee's recommendations at the conclusion of this process.

# The Changing Legislative Landscape in Canada and Internationally

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

As the committee is aware, Alberta is one of a handful of provinces in Canada that has its own personal information protection legislation, and is therefore not subject to the federal government's Personal Information Protection and Electronic Documents Act (PIPEDA). Since its enactment in 2004, the federal Office of the Privacy Commissioner (OPC) has deemed Alberta's PIPA to be "substantially similar" to its federal counterpart.[6] Until the federal government tabled Bill C-27, which, in part, replaces the federal PIPEDA with the Consumer Privacy Protection Act (CCPA), there have been no changes to PIPEDA significant enough to warrant a reexamination of Alberta's "substantially similar" designation, nor did PIPEDA define a process to formally do so.

In addition to fundamentally overhauling PIPEDA, the proposed CCPA also introduces new measures for the federal regulator to reconsider a province's existing "substantially similar" designation, which is an entirely new power.[7] This addition reads:

> *Regulations — substantially similar provincial legislation*
> *(3) The Governor in Council may make regulations establishing*

[4] https://www.alberta.ca/alberta-technology-and-innovation-strategy
[5] https://www.alberta.ca/digital-strategy-engagement
[6] https://oipc.ab.ca/pipa-sustantially-similar/
[7] https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading - Section 122 (3)

> *(a) criteria that are to be applied in making a determination under paragraph (2)(b) that provincial legislation is substantially similar to this Act, or in reconsidering that determination; and*
> *(b) the process for making or* ***reconsidering that determination***

As such, a key focus of modernizing PIPA should be cross-jurisdictional alignment. Notably, the matter of *where* provincial or federal legislation has ultimate jurisdiction is being challenged by the expanded powers given to the new regulatory body (the Personal Information and Data Protection Tribunal) — including the power to levy administrative monetary penalties. As such, it is unlikely that a provincial privacy regime in Alberta will be sustainable if both its overarching policy principles, and its enforcement regime, remain fundamentally unchanged. Alberta's PIPA notably lacks a robust, rights-based approach to personal information protection, and does not give Alberta's privacy regulator — the Office of Information and Privacy Protection (OIPC) — any significant punitive powers. Cybera recommends that a modernized PIPA must include both of these additions.

We believe these gaps can be addressed by viewing the European Union's General Data Protection Regulation (GDPR) — itself a strong inspiration for the federal government's approach to C-27 — as a model. Enacted in 2016, the GDPR is widely considered to be the global "gold standard" for data protection legislation, and has had significant implications for the development of privacy regulation across the world. In Cybera's experience, many public sector organizations who do not operate in Europe, and were not subject to GDPR, still voluntarily adopted many of GDPR's overarching practices. This was done with the understanding that compliance with GDPR could be reasonably assumed to guarantee compliance with all other privacy legislation, whereas the opposite was not true.

While the question of how Alberta can specifically align its privacy legislation with other jurisdictions is detailed later on in this submission, Cybera notes that many jurisdictions are also in the process of modernizing their existing personal information protection laws. In addition to the federal government's C-27, a number of US states, including California and New York, have recently enacted new privacy legislation with a particular focus on artificial intelligence systems.[8] Within Canada, Quebec passed Law 25 in 2023, while BC is currently reviewing its provincial privacy act.[9] Both of these can be seen as attempts to align provincial and federal privacy legislation in light of C-27.

In reviewing the priorities outlined by other jurisdictions, it is clear that the centering of individual rights in privacy legislation will become the standard framework. As such, while consent is, and should remain, a key concept in privacy legislation, it will be in the interest of both individuals and

[8] https://digitalcommons.law.uw.edu/wjlta/vol19/iss1/3/?utm_source=digitalcommons.law.uw.edu
[9] https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1304&context=cjlt

organizations operating in Alberta for PIPA to go beyond this. The revised PIPA should clearly define a system of individual rights that address modern privacy concerns. These rights will be detailed in other sections of this submission.

# Artificial Intelligence

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

The question of whether PIPA should explicitly regulate artificial intelligence systems, and in exactly what manner, is a complicated one. The federal government's C-27 addresses general personal information protection and artificial intelligence systems in two separate pieces of legislation — the CCPA and the Artificial Intelligence and Data Act (AIDA). Both are being governed by separate regulators.

Under AIDA, AI systems will fall under the purview of a proposed Artificial Intelligence and Data Commissioner.[10] This regulator will be guided by principles that significantly overlap with personal information protection policies, but will have a formally distinct mandate. The European Union has taken a similar approach by handling AI in its AI Act, rather than including these provisions in GDPR. Notably, the federal government's proposed privacy legislation will, once enacted, still remain essentially technology-neutral, as PIPA currently is.

Specifically referencing artificial intelligence systems in PIPA would therefore be a significant shift from its technology-neutral nature, which could require the OIPC to assume new responsibilities, or could precipitate Alberta similarly creating a new regulator. While Cybera is not in a position to comment on the feasibility of this approach within Alberta, incorporating some provisions relevant to AI governance into existing personal information protection legislation has its benefits, and is an approach currently being pursued by Quebec in its Law 25.[11]

Notably, Quebec's approach to regulating artificial intelligence systems, enacted in 2023, predates the federal government's approach and appears significantly influenced by GDPR. Its Law 25 explicitly references "automated processing" and "processing by technological means" as a distinct form of personal information processing, and subsequently outlines the limits to its use. Perhaps more significantly, Law 25 also outlines a number of rights inherently held by an individual with specific applicability to automated decision making, including algorithmic transparency, and consent to automated processing.[12] This approach is notably similar to that enshrined by GDPR, and

[10] https://digitalcommons.law.uw.edu/wjlta/vol19/iss1/3/
[11] https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1304&context=cjlt
[12] https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1

effectively creates a "Privacy Bill of Rights" that features prominently in the legislation's overall tenor and framing.

In Cybera's view, incorporating AI references into PIPA is broadly in keeping with the act's existing framework, and should be well within the regulator's ability to enforce. While specific rights and amendments relevant to AI governance are outlined in other sections of this submission, Cybera recommends that, in keeping with other modern privacy legislation's references to automation, PIPA should be amended to include a provision reflecting the following:

> *Any organization that uses personal information to render a decision based exclusively on an automated processing of such information must inform the person concerned accordingly, and provide opportunities for the person concerned to challenge and object to the result of that processing.*

# Application

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

Cybera sees no reason for non-profits to not be formally subject to all of the provisions of PIPA. As stated previously, the impact of personal information protection on t organizations (both commercial and non-profit) extends beyond simple compliance. In many ways, ambiguity around which privacy regulations apply to an organization is more burdensome than the rules themselves.

In many cases, organizations lack the in-house knowledge or resources to read and interpret regulatory rulings, particularly in Alberta, where provincial legislation governs commercial activities. As such, rather than attempting to determine which of their activities apply to which privacy protection legislation, many public sector organizations find it simpler to adopt the spirit and restrictions of one particular personal information protection regime, with a strong tendency towards the more restrictive of these.

Stating clearly that these organizations are subject to PIPA would clarify any ambiguity that may exist in this regard, and would create a more straightforward relationship with the authorities that govern their activities. Formalizing privacy management programs, which is discussed in more detail in other sections of this submission, would be a significant improvement over the current system.

This change would also align Alberta with BC's PIPA, which explicitly applies to "unincorporated associations, trade unions, trust and not for profit organizations."[13]

# Consent Requirements

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

In Cybera's view, PIPA's provisions addressing consent are well in-line with traditional approaches and do not need significant changes. However, one drawback of the historical reliance on consent as a framework is that it creates an implied hierarchy for how organizations treat information that does not formally require consent. This is an issue that both C-27 and GDPR address through enshrining a higher consent standard.

Canada's C-27 includes the following provision:

> An organization may collect, use or disclose personal information only in a manner and for the purpose that a reasonable person would consider appropriate in the circumstances, **whether or not consent is required under this Act.**[14]

The bolded section is a new addition to the federal government's privacy legislation, and Cybera recommends an equivalent provision be included in PIPA.

# Individual Rights that are Not Included Under PIPA

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

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

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

[13] https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01
[14] https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading - Section 12(1)

In Cybera's view, each of the above rights would align PIPA with modern personal information protection principles, and should be included in PIPA, with some modifications as detailed below.

## Right to the portability of data

While PIPA explicitly outlines the right for an individual to access and correct their personal information, the concept of data portability is relatively new, and does not exist in PIPA. The goal of the right to data portability is to ensure that dominant market participants whose business models rely heavily on users' personal information (in particular, social media platforms) cannot 'lock-in' their users by holding their data in unique or non-transferrable formats. A number of legal challenges have been undertaken to address this issue, most notably a proceeding initiated by Italy's competition regulator against Google in 2023.[15]

While ostensibly subtle, data portability indicates a significant conceptual shift in personal information protection governance. An individual's freedom to exercise their choices in the modern marketplace is not a right unique to personal information, and can be applied to a large number of regulatory areas, including consumer protection and antitrust cases. Effectively, data portability addresses a number of public policy objectives that are not unique to privacy. As stated, this kind of broad and holistic approach to data subject rights is becoming the new paradigm in personal information protection, and does not perfectly align with the "collection, use and disclosure" framework that has traditionally been its foundation. As such, Cybera proposes the right to data portability be enshrined in PIPA, in a manner similar to the following:

> *On the request of an individual, and taking into consideration what is reasonable, an organization must provide the personal data concerning the individual to another organization in a structured, commonly-used format, without hindrance or delay.*

## Right of Erasure/Right to be forgotten

While PIPA does require organizations to destroy any personal information that is no longer required to fill the purposes of the data's original collection, the right to be forgotten reframes this requirement in some significant ways. The right to be forgotten, in effect, allows an individual to retroactively withdraw their consent for the original collection of their data. The right to be forgotten is enshrined in both GDPR and C-27, and, in Cybera's view, should be included in PIPA, in a manner similar to the following:

> *The data subject shall have the right to obtain the erasure of personal data concerning them without undue delay, where one or more of the following circumstances apply:*

[15] https://www.reuters.com/technology/italys-antitrust-accepts-googles-proposals-end-data-portability-case-2023-07-31/

a. *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed*
b. *the data subject withdraws consent*
c. *the data subject objects to the processing*
d. *the personal data has been unlawfully processed*

### Right to object to automated processing

In Cybera's view, the wording of the amendment related to automated decision making should be significantly strengthened. Our key concern about automated decision making is the potential for inequity or profiling. For this reason, individuals should have the right not only to be informed of the logic behind automated decision making, but also the right to object to the results of automated decision making. As such, Cybera recommends including a provision in PIPA outlining these rights in a manner similar to the following:

1. *An individual shall have the right to object, at any time, the automated processing of personal data concerning them, including profiling.*

2. *An individual shall have the right not to be subject to a decision based solely on automated processing, including profiling.*

## Safeguarding Personal Information

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

In Cybera's view, PIPA should formalize privacy management programs (PMP) as a requirement for organizations to implement.

While the addition of PMPs to federal legislation is a new development in C-27, it has existed as an industry best practice for a number of years. The OIPC, in conjunction with other Canadian regulators, has published detailed guidelines that organizations can use to develop their own PMPs, as well as justifications for why they should voluntarily do so.[16] As it stands, Alberta's privacy regulator already possesses strong institutional understanding of PMPs, as well as existing intake and evaluation processes. The PMP guidelines document that is now being formalized in C-27 has created an important industry standard for privacy management. This legislative change will, in effect, codify these guidelines, either formally or in-practice, and should therefore be included in PIPA with similar wording.

[16] https://oipc.ab.ca/wp-content/uploads/2022/02/Accountability-2012.pdf

As a not-for-profit organization that is responsible for member organizations' data, Cybera's current formal obligations under PIPA extend only to its commercial activities. Nonetheless, Cybera sees value in enshrining a more proactive and preventative approach to privacy than currently exists in PIPA. Including PMPs within PIPA would incentivize organizations to fully understand their data management risks and opportunities, and develop data management practices that are in-line with the regulator's guidelines, well before a breach occurs.

Notably, C-27 includes two important provisions related to this that should be mirrored in PIPA:

- *Section 110(1)(e): on request by an organization, provide guidance on — and, if the Commissioner considers it appropriate, recommend corrective measures in relation to — its privacy management program.*

This provision, which allows an organization to engage with its privacy regulator to evaluate and recommend improvements to its PMP, would be of significant benefit. It would allow organizations to remove any uncertainty in their approach to privacy management, and fully adjust their policies to both the letter and interpretation of privacy rules, as determined by the regulator.

- *Section 111: The Commissioner must not use the information the Commissioner receives under section 10 or paragraph 110(1)(e) as grounds to initiate a complaint under subsection 82(2) or to carry out an audit under section 97 unless the Commissioner considers that the organization has wilfully disregarded the corrective measures that were recommended in relation to its privacy management program.*

This above provision, which offers protections to organizations who submit privacy management programs to the Commissioner, is also a significant benefit to organizations, and should be included in PIPA. Many organizations are concerned about how potential deficiencies in their privacy management programs, including ones resulting from a lack of knowledge about rules and regulations, could cause them to be singled out for increased scrutiny by the regulator. Implementing privacy management programs successfully will require assurance that safeguards are in place to prevent this from happening.

To successfully implement PMP's in law, the OIPC will need to provide specific and unambiguous guidance to organizations on content and format requirements, in a simple language. Here, Cybera recommends the OIPC leverage its existing privacy impact assessment processes to create an easy to use questionnaire template for organizations to develop their PMPs.

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

In Cybera's view, new provisions specifically regulating de-identified and/or anonymized data should be included in PIPA. For jurisdictions where privacy legislation doesn't explicitly reference or govern "de-identification" or "anonymization" — as is the case in both PIPA and PIPEDA — the implication has been that the definition of personal information as applying to an "identifiable person" excludes these circumstances in practice.[17] On its face, this is technically true. However, such an approach has significant drawbacks. If "de-identification" and "anonymization" of personal information aren't explicitly defined or separately governed, it is not clear that the elicit "re-identification" of this information can exist as a distinct infraction or could be individually deterred.

Automated decision making and artificial intelligence systems will significantly increase the opportunities and the incentives for these types of infractions, and rules for governing these instances should be enhanced in PIPA and applied at OIPC's discretion. However, given the significant value that de-identified and anonymized data can have for public interest uses — including scholarly and commercial interests — the overarching framework for these instances (i.e. requiring lower consent standards) should remain in place.

Here, C-27 outlines a framework for addressing these instances that should serve as a model for PIPA. The C-27 bill enshrines the following definitions in the Consumer Privacy Protection Act:

> ***anonymize*** *means to irreversibly and permanently modify personal information, 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.*
>
> ***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.*

Because de-identified data is implied to carry a higher risk to the individual, clear definitions and rules must be outlined to govern their use. Cybera recommends that PIPA use the above definition as a template, and subsequently empower the regulator to set penalties to address any infractions in relevant instances.

Conversely, Cybera is of the view that true anonymization of data should be sufficient to exempt this information from being considered a form of personal information, and therefore should not be

[17] https://informationethics.ca/index.php/irie/article/view/379/385

subject to PIPA. This is in keeping with both C-27 and GDPR, and explicitly defining this within PIPA would provide helpful clarification.

# Conclusion

Cybera once again thanks the committee for accepting comments on its comprehensive review of PIPA. In this submission, Cybera made the following recommendations:

1. Maintain a broad alignment with C-27 and GDPR.
2. Align PIPA with other modern personal information protection legislation by adopting a rights-centered approach, including:
    a. Right of data portability
    b. Right of algorithmic transparency
    c. Right of erasure
3. Maintain PIPA's existing consent regime while acknowledging organizations' obligations in instances where consent is not required.
4. Outline rules with respect to automated decision making in a manner that maintains PIPA's technology-neutral nature.
5. Enshrine privacy management programs in PIPA, with the right for organizations to request guidance from the regulator and subsequently be safeguarded from audits resulting from this process.
6. Define and create rules governing anonymized and de-identified data.
7. Include non-profits in organizations subject to PIPA.