RS-2024-029

Alberta Standing Committee on Resource Stewardship

Review of the Personal Information Protection Act (PIPA)

PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC

Submission of the Public Interest Advocacy Centre

31 May 2024

Introduction

1. PIAC is pleased to submit this submission in response to the Alberta Standing Committee on Resource Stewardship call for submissions on the review of *Alberta's Personal Information Protection Act (PIPA)*.

2. PIAC is a national not-for-profit corporation and a federally registered charity that protects consumer interest in regulated industries such as telecommunications, energy, financial services, privacy and transportation.

3. PIAC's comments are focused on the right to logic for automated decision making, the right to be forgotten, breach notifications and children's privacy. PIAC believes this Committee has a vital opportunity to ensure updates to PIPA increase individual agency by strengthening protections for personal data and increasing corporate accountability.

PIPA should include a framework to regulate the design, development, and/or use of artificial intelligence systems within Alberta, including a right to logic for automated decision making.

4. In contrast with PIPA, the European Union's General Data Protection Regulation (GDPR), Canada's Consumer Privacy Protection Act (CPPA) and Quebec's Act Respecting The Protection Of Personal Information In The Private Sector (QPSA) all include a right to logic behind automated decision systems at varying degrees. As the use of automated decision-making is on the rise, privacy legislation needs to adapt to ensure individuals protection of personal data is not at even greater risk.

5. Under the GDPR, Article 14(2)(g) includes an express right to transparency and explainability of automated decisions. The controller shall provide the data subject with "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[1]

6. These transparency and explainability obligations are limited to only those decisions based solely on automated processing, including profiling, which produces legal effects concerning an individual.[2] Such use of automated decision making in the EU is only authorized if the decision based on the algorithm is necessary to enter into or to perform a contract with the individual whose data is being processed, a particular EU or

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 14(2)(g), https://gdpr-info.eu/art-14-gdpr//.

[2] *Ibid* at Article 22

national law allows the use of algorithms and provides appropriate safeguards, or the individual has explicitly given consent.[3]

7. In 2020, Canada's Office of the Privacy Commissioner (OPC) launched a public consultation on the appropriate regulation of AI. Out of the consultation, one of the OPC's recommendations on appropriate law for AI was the creation of provisions specific to automated decision making to ensure transparency, accuracy and fairness. Unlike the GDPR, the OPC recommended that PIPEDA should broaden the definition of automated decision making not limiting it to decisions made "solely" by AI. Currently, automated decision making in Bill C-27 "means 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."[4]

8. PIPEDA also includes an obligation on an organization to make available "a general account of the organization's use of any automated decision system to make predictions, recommendations or decisions about individuals that could have a significant impact on them".[5] The OPC report included recommendations for PIPEDA to provide individuals with rights to obtain a meaningful explanation and to contest the decision. Bill C-27 prescribes organizations, who have used an automated decision making system about the individual, to provide them with an explanation of the prediction, recommendation or decision upon request by said individual.[6] However, it does not currently include an explicit right for individuals to contest the decision. The GDPR however, does include a right to contest under Article 22(3) where in certain circumstances an individual has "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.[7]

9. Automated decisions are often used for decisions such as immigration, public health, employment, and more. Information collected about individuals is often highly person and sensitive. Decisions using such information can have serious impacts on the lives of individuals and therefore if it is not properly monitored nor accessible by the individuals whose data it contains, it runs the risk of serious breaches. For this reason, the EU's recent legislation on AI adds extra protects to "high-risk" systems such as employment, law enforcement, access to essential services and more.[8]

---

[3] *Ibid.*

[4] 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 (Bill C-27), 1st Sess, 44th Parliament, 70-71, June 16, 2022, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

[5] *Ibid* at Article 62(2)(c).

[6] Ibid at Article 63(3).

[7] *Supra* note 1 at Article 22(3).

[8] EU AI Act : first regulation on artificial intelligence, European Parliament, June 8, 2023, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

10. Aligned with the above regulations and proposed legislative amendments, PIAC suggests that PIPA should require that organizations provide individuals with the logic behind automated decision making about that individual and mirror the GDPR to provide a right to contest an automated decision. This form of algorithmic transparency can help create a better understanding for individuals on how their data is being used leading to more agency. Elements from both the GDPR and Bill C-27's proposed amendments for PIPEDA provide a foundation on which PIPA can build a strong AI framework.

PIPA should include protections for an individual's right to have their data be removed or de-indexed.

11. PIPA currently has "no provisions whereby an individual may require an organization to erase, dispose or de-index the personal information it holds about that individual."[9] The right to access one's personal information is less meaningful if individuals cannot take steps to have their information removed, de-indexed

12. Article 17 of the GDPR includes the right to erasure, including de-indexing from an online search, with certain limitations and exceptions.

    "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" if one of a number of conditions applies. "Undue delay" is considered to be about a month. Steps must also be taken to verify the person requesting erasure is actually the data subject."[10]

13. Under the GDPR, an individual has a right to be forgotten when they no longer consent to processing, there are significant errors within the data or if they believe information is being stored unnecessarily.[11] However, this right is not absolute. The right to be forgotten is balanced with a companies' right to process someone's data in instances, such as data necessary for public health purposes and serves in the public interest. Additionally, an organization can request a "reasonable fee" or deny a request to erase personal data if the organization can justify that the request was unfounded or excessive.[12]

---

[9] Emerging Issues: The Personal Information Protection Act, Standing Committee on Resource Stewardship Legislative Assembly of Alberta, February 13, 2024, https://www.assembly.ab.ca/docs/default-source/committees/rs/pipa-emerging-issues.pdf?sfvrsn=fb63a400_1.
[10] Everything you need to know about the "Right to be forgotten", Ben Wolford, GDPR.EU, accessed on May 30, 2024, https://gdpr.eu/right-to-be-forgotten/#:~:text=Also%20known%20as%20the%20right,always%20have%20to%20do%20it.
[11] *Ibid.*
[12] *Ibid.*

14. PIAC believes the language of "unfounded or excessive" should instead be a standard of undue hardship. To be undue hardship, the hardship must be substantial in nature. This is already an established standard in Canada under the *Canadian Human Rights Act* and therefore it will remove the risk of attempting to define what is unfounded or excessive, leaving organizations more unregulated. It is also a high standard that will remove frivolous complaints by organizations attempting to evade the regulations.

15. In late 2023, the Canada's Federal Court of Appeal rejected an application by Google to have a 2021 Federal Court decision overturned that determined the company's search engine is covered by Canada's privacy law.[13] The case was started by an individual complaining searches of his name on Google were producing inaccurate and outdated sensitive information. The individual stated that as a result of this inaccurate information produced by searches, he suffered direct harm including physical assault, lost employment, and social stigma.[14] At the time of this case, Bill C-27 and its proposed right to erasure had not yet emerged.

16. Bill C-27 includes amending PIPEDA to include a right to erasure, with exceptions, in three instances. First, if the organization had no right to have or use the personal data in the first place. Second, is where an individual has withdrawn their consent. Third, an individual can request deletion of their personal data where the information is no longer necessary for the continued provision of a product or service requested by the individual.[15]

17. PIAC believes that PIPA should include a right to forgotten that provides individuals with more agency to control when they no longer wish to have their data collected or used. As online environments are utilized more and more, the amount of personal data collected and stored is rapidly increasing. Having a right to erasure can help with the removal of inaccurate or outdated data that can have potentially harmful effects on individuals. Adding these provisions will also align PIPA with the changes to PIPEDA, ensuring PIPA remains substantially similar.

18. Additionally, these provisions would prevents companies from having open-ended free access to personal, often sensitive, data. PIPA already includes provisions on retention of data under section 35(1) where an organization is required to destroy personal information records or render information non-identifying to an individual if it is no long

---

[13] Federal Court of Appeal rules against Google in privacy law case, The Canadian Press, CTV News, October 2, 2023, https://www.ctvnews.ca/business/federal-court-of-appeal-rules-against-google-in-privacy-law-case-1.6585907.

[14] Google is covered by Canada's privacy law, Federal Court of Appeal rules, Howard Solomon, IT World Canada, September 30, 2023, https://www.itworldcanada.com/article/google-is-covered-by-canadas-privacy-law-federal-court-of-appeal-rules/547997.

[15] *Supra* note 4 at Article 55; https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=358:bill-c-27-and-the-erasable-right-of-erasure#:~:text=In%20its%20basic%20form%2C%20this,addressed%20in%20Bill%20C%2D27.

reasonably necessary for the organization to possess. Therefore a right to be forgotten or de-indexed is not a completely new burdensome process for organizations. Rather, it adds a layer of protection for individuals and encourages organizations to comply with their existing retention and destruction of personal information responsibilities.

The provisions for notifications of breaches to the Commissioner and individuals under PIPA can be improved.

19. Currently under PIPA, notifications are only required to the Commissioner if there is a real risk of significant harm to the individual. It is then up to the Commission to determine whether the individual should be notified.

20. Under PIPEDA, an organization is required to report to the Commissioner any breach involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. This threshold is not as strong as the reasonable person standard included in PIPA. It runs a higher risk of organizations storing privacy breaches internally that are never reviewed by the Commissioner.

21. PIPA's reasonable person standard can be kept the same. Alternatively, PIPA could require organizations to report every breach to the Commissioner with a statement describing their view on whether the breach meets or does not meet the standard. It will then be up to Commissioner's office to decide whether a breach created a real risk of significant harm and if an individual should be notified. This will reduce the risk of data breaches going unreported and individuals remaining unaware that their personal information has been compromised.

22. Further, and importantly, PIAC urges the Committee to be wary of claims by companies that data breach notifications are too onerous. Breach notifications are integral to ensuring corporate accountability and informing Canadians when their information is at risk.

Provisions should be added to enhance the protection of children's personal information.

23. In the digital age, protection of personal information for children is of utmost importance. The threats that exist in online environments are designed to directly target young users using their viewing habits and personal data. Children also have increased unsupervised access to online sites increasing the frequency at which serious breaches can occur.

24. PIAC has previously commented on children's privacy. In 2008, PIAC released a report titled "All In The Data Family: Children's Privacy Online"[16] which recommended a tiered system for age verification and consent quoted below.

    "First, there should be a general prohibition on the collection, use and disclosure of all personal information from children under the age of 13. This age marks a rough threshold for children to be considered capable of making decisions about themselves (what is known in medical law, for example, as being a "mature minor").

    Second, for young teens aged 13-15, websites should be permitted to collect and use personal information, with the consent of the teen and the explicit consent of a parent for the benefit of the child and solely in relation to that website or service and should not be permitted to further disclose their personal information.

    Third, for older teens aged 16 to legal majority (18 or 19), websites should be permitted to collect and use personal information, with the consent of the teen. Such websites should be permitted to disclose the personal information of the teen only with the opt-in consent of the teen and explicit consent of a parent.

    Once children reach 18 years of age…websites that have collected and used personal information (or that have been transferred the child's personal information with explicit consent during this period) should no longer be permitted to retain the information gathered during the child's "legal minority" and should be required to remove the information immediately (a privacy "get out of information jail free card") unless the newly adult person gives his or her explicit consent to the continued collection, use, and (should they agree) possible future disclosure of their personal information gathered during their minority."

25. The approach is designed to avoid encouraging children offer up their personal data until they are capable of appreciating, to a reasonable degree, that they are ready for the responsibility. PIAC still supports this approach and urges the committee to implement provisions on protecting children's privacy.

Conclusion

26. PIAC supports the Committee in its efforts to update PIPA and safeguard individuals and their right to protection of personal data. PIAC cautions the Committee to not entertain organizations' arguments that current and newly proposed provisions in PIPA will be too burdensome. Individual agency over personal data should be the primary focus.

---

[16] All in the Data Family: Children's Privacy Online, John Lawford and Mani Taheri, The Public Interest Advocacy Centre (PIAC), September 2008, at pages 4-5, https://www.piac.ca/wp-content/uploads/2014/11/children_final_small_fixed.pdf.

End of Document