

20260710 Review of the Privacy Act FIPA Submission

Table of Contents

Recognition	3
FIPA Narrative Privacy Submission Recommendations	4
1. Consideration of proportionality as a step of the necessity test for data collection	4
2. Create a legal obligation to apply the necessity and proportionality test to artificial intelligence (AI) and automated decision systems (ADS)	5
3. Data sharing between government bodies should be subject to the necessity test and should be governed by written agreements that are posted publicly	6
4. Create legal requirements for the elements of privacy impact assessments	8
5. Make breach notifications under the Privacy Act mandatory and based on the application of an “unlikely to result in risk” threshold	10
6. Engage in meaningful consultation with Indigenous peoples	11
7. Include predictions about individuals within the scope of “sensitive data”	13
8. Valid consent should be defined in the Privacy Act	14
9. Individuals must be allowed to withdraw consent from personal data sharing between government bodies	15
10. Re: AI decision making, governments should limit exposure of personal information to AI systems; individuals should be able to withdraw consent from AI decision-making and processing of their personal information	16
11. Transparency rights for public sector workers regarding employee monitoring should be enhanced	18
12. Application of the Privacy Act could extend to Parliamentary offices and offices of MPs	19
Appendix 1 FIPA Commentary on Policy Proposals	21
Theme 1: Enabling integrated services	21
Theme 2: Enhancing accountability and transparency	23

Theme 3: Advancing safeguards across the spectrum of data sensitivity	27
Theme 4: Modernizing the foundation for privacy and trust	31
Theme 5: Indigenous Peoples' access to, and protection of, their data	34
Theme 6: Updating the compliance framework	36
Appendix 2 Treasury Board Submission	38
Recommendations for the 2026 Review of the Privacy Act	38
Synopsis	38
Authorities Sought from the Treasury Board	38
Context	39
Design, Delivery and Implementation	41
Cost, Source of Funds and Strategic Considerations	41
Results	41
Risks	41
Appendix 3 Cited Sources	42
Legislation	42
Jurisprudence	42
Secondary Materials:	42

Recognition

FIPA extends its sincere gratitude to the groups and individuals who generously provided valuable feedback on early versions and drafts, helping us refine this document. Many have also made their own submissions. Of particular note we would like to draw attention to the B.C. Civil Liberties Association (BCCLA), First Nations Governance Information Council, Canadian Union of Public Employees, and Dr. Teresa Scassa, whose combined input and expertise consistently provides important insights that strengthen our arguments for progressive law reform.

About FIPA

The BC Freedom of Information and Privacy Association (FIPA) is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. While we are based in BC, our membership extends across Canada, and we regularly partner with organizations throughout the country.

Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform. We are one of very few public interest groups in Canada devoted solely to the advancement of freedom of information and privacy rights.

Institutional Funders

The BC Freedom of Information and Privacy Association thanks the Law Foundation of BC, the Province of British Columbia (Gaming Policy and Enforcement Branch), and all our contributors including donors, funders, and volunteers for their ongoing support of our advocacy, programs, projects, and activities.



FIPA Narrative Privacy Submission Recommendations

Bill C-36 proposes consequential legislative amendments with changes in resource allocation as well as oversight that impact the Privacy Act and could materially affect how participants respond to these policy questions while this consultation is still underway. Proceeding with an active consultation while advancing material amendments—without updating the consultation materials and providing a meaningful opportunity to comment on their implications—is deeply concerning. It creates a moving target, leaves participants uncertain whether their submissions should address the existing framework or the changes proposed in Bill C-36, and risks undermining public confidence in the integrity and purpose of the consultation.

1. Consideration of proportionality as a step of the necessity test for data collection

Proposal 10 of the Review of the *Privacy Act* recommends implementing a necessity test for data collection to prevent the over-collection of personal information.¹ This is an important safeguard but misses a key step in the proposed test: Proportionality.

Considerations for proportionality have been strongly advocated for many years. The House of Commons supported the Office of the Privacy Commissioner's (OPC's) recommendation that the necessity test for the collection of personal information resemble the factors of the *Oakes* test in the Supreme Court of Canada case *R v. Oakes*.² Each of these steps has been included in Proposal 10 with the exception of proportionality; the OPC has elucidated that “the loss of privacy is proportional to the importance of the objectives of the program or activity.”³ Upon hearing a range of testimony on whether or not proportionality should be included separately from the necessity consideration, the House of Commons Committee determined that proportionality was a vital consideration on its own as it informed the overall necessity of the collection of the data.⁴

An example from the private sector is illustrative of the difference: in 2022, the OPC investigated Tim Hortons' data collection through their mobile app for whether it

¹ Treasury Board of Canada Secretariat, “2026 Review of the Privacy Act: Policy Approaches” (2 April 2026) online: < <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/privacy-act-modernization-policy-approaches/2026-review-privacy-act-policy-approaches.html> > [TBS]

² Blaine Calkins, *Protecting the Privacy of Canadians: Review of the Privacy Act, Report of the Standing Committee on Access to Information, Privacy and Ethics*, (House of Commons, 2016). [House of Commons]

³ Daniel Therrien, “Letter to the Standing Committee on Access to Information, Privacy and Ethics” (22 March 2016) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/> at pt. 4

⁴ House of Commons *supra* note 2

complied with PIPEDA and found that Tim Hortons was collecting a continuous stream of users' location data.⁵ The OPC conducted separate necessity and proportionality assessments, demonstrating the unique significance of each step. This investigation exemplifies why proportionality must be considered separately from necessity.

On the necessity side, the OPC considered simply that Tim Hortons was not using this location data for its stipulated purposes.⁶

The OPC separately considered that the mass collection of users' locations at all times was not proportional to the potential benefits to Tim Hortons.⁷ In this vein, it is vital that the benefit, use and purpose of collecting the information not be considered in isolation but weighed against the impairment of privacy. To ensure that individuals' personal information is protected, the detriment to their privacy must be considered in comparison to the potential gain so as to give appropriate perspective. The higher the infringement of people's privacy, the stronger the justificatory benefit must be.

2. Create a legal obligation to apply the necessity and proportionality test to artificial intelligence (AI) and automated decision systems (ADS)

A true modernization of the *Privacy Act* requires strong safeguards against privacy being eroded by new and evolving technologies. Proposals 5 and 6 address artificial intelligence (AI) through the lens of transparency.⁸ That said, they do not recommend any limitations or regulations to serve as guardrails to protect individuals' privacy when AI is being used to process their personal information.

FIPA recommends that the justificatory test in Proposal 10 (referred to in the proposal as the "necessity test") be applied to the use of artificial intelligence and automated decision-making systems (ADS). In 2023, the OPC addressed privacy protection in the responsible use of AI.⁹ It recommended that organizations establish both the necessity and proportionality of AI's use and for its given purpose.¹⁰ The necessity test offered in Proposal 10 could be applied to decisions about AI use, with the addition of a proportionality step. The proportionality test would resemble that articulated by the OPC

⁵ Joint investigation into location tracking by the Tim Hortons App, 2022 CanLII 50894 (PCC), <<https://canlii.ca/t/jprwv>>, retrieved on 2026-07-09 [Tim Hortons Joint Investigation]

⁶ *Ibid* at paras. 40-45

⁷ *Ibid* at paras. 46-49

⁸ TBS *supra* note 1

⁹ Office of the Privacy Commissioner of Canada, "Principles for responsible, trustworthy and privacy-protective generative AI technologies" (7 December 2023) online: <https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/>

¹⁰ *Ibid* at Principle 3

whereby personal information is collected when “the loss of privacy is proportional to the importance of the objectives of the program or activity.”¹¹

This is highly relevant given systems like ADS may be influenced by biases derived from the models used to train them.¹² For example, Amazon was reportedly using a type of ADS system for hiring purposes which was proven to be discriminatory to women.¹³ UBC Professor Wendy H. Wong similarly uses the example of hiring tools, noting that such ADS systems are subject to inherent biases.¹³ Findings on facial recognition technologies (FRT) have shown as high as a 34% error rate for African American individuals, reporting an error rate of below 1% for White individuals.¹⁴ The addition of a proportionality step requires bodies to take into account the potential biases within their system of choice while they consider whether the benefit to using AI or ADS outweighs the potential harm to those affected.

The risks associated with AI are not insubstantial. When relying on third-party AI models for processing personal data, there is always a data leakage risk.¹⁵ Organizations like the Canadian Bar Association stress that inputting client information into an AI model could lead to a breach of lawyer-client confidentiality.¹⁶ Canadians’ personal information should not be subject to such risks without proper safeguards. A proportionality test demands a high level of due diligence; this is essential in the face of such severe threat to personal information. The necessity element should ensure that personal data is not being unnecessarily risked, and the proportionality element should ensure that all such risks are proportional to the expected societal benefit.

3. Data sharing between government bodies should be subject to the necessity test and should be governed by written agreements that are posted publicly

Modernizing the management of personal information cannot be done without ample checks and balances. Teresa Scassa notes that “there are... substantial risks with horizontal data sharing.”¹⁷ She points to surveillance and “problematic uses of data in AI systems” as possible detrimental outcomes from data sharing between governments

¹¹ Daniel Therrien *supra* note 3 at pt. 4

¹² Jiaheng Wei et al, “Memorization in Deep Learning: A survey” (2020) 18:9 Journal of Latex Class Files.

¹³ Wendy H. Wong, *We, the Data: Human Rights in the Digital Age* (The MIT Press, 2023).

¹⁴ Loso Judijanto, “Unmasking Racial Disparities: Epistemic Injustice and Bias in Facial Recognition Systems” (Indonesia: Scientia, 2025) 2:12, [https://doi.org/10.59324/stss.2025.2\(12\).01](https://doi.org/10.59324/stss.2025.2(12).01)

¹⁵ Natasha MacParland et al, “Artificial Intelligence in Canadian Insolvency Practice” (2025)

¹⁶ Natasha MacParland et al., *supra* note 15

¹⁷ Teresa Scassa, “Pragmatic Privacy: Reform of the Federal Privacy Act” (13 April 2026) online: <<https://teresascassa.substack.com/p/pragmatic-privacy-reform-of-the-federal>> at para. 8

without proper safeguards.¹⁸ Moreover, when smaller data sets are combined to create larger, integrated datasets, even if the data has already been de-identified, the risk of re-identification is substantially higher.¹⁹ The depth and breadth of the data increase the potential degree of harm in the event of a breach.²⁰

With that in mind, FIPA recommends that the justificatory test be applied not only to the collection of data as recommended in Proposal 10, but also to the disclosure of data between bodies. “Justificatory test” refers to the necessity test described in Proposal 10 with the additional element of proportionality. If consent from affected individuals is not required, there must be a mechanism in place to ensure that data is not being arbitrarily shared and used between institutions. This concept was supported by the House of Commons Committee in 2016.²¹ Ideally, this justificatory test would reflect FIPA’s 1st recommendation and include a consideration for proportionality.

In 2016, the House of Commons heard from a number of experts regarding the *Privacy Act*; many concurred that requiring written agreements governing data-sharing between governments was important for the protection of personal information.²² They officially recommended that all information sharing between government bodies be governed by written agreements and that these agreements be published.²³ This was supported by the Privacy and Access Law Section of the Canadian Bar Association for the following reasons: (i) to protect the fundamental rights of individuals and (ii) to hold government agencies to account.²⁴ FIPA agrees with this recommendation; in our view it should be applied to a modernized *Privacy Act*.

The contents of such written agreements can be broad, as made clear by former Privacy Commissioner Therrien in the House of Commons Committee report.²⁵ At minimum, and regardless of the sensitivity of the information, these agreements should:

- Specify the parties to the data-sharing;²⁶
- State the type of information shared, and how to determine its sensitivity;²⁷

¹⁸ *Ibid* at para. 8

¹⁹ Australian Institute of Statistics, “Understanding re-identification” (8 November 2021) online: <<https://www.abs.gov.au/statistics/understanding-statistics/data-confidentiality-guide/understanding-re-identification>> [Australian Bureau of Statistics]

²⁰ Australian Bureau of Statistics *supra* note 19

²¹ House of Commons *supra* note 2

²² House of Commons *supra* note 2

²³ *Ibid*

²⁴ *Ibid* at p. 11

²⁵ *Ibid*

²⁶ *Ibid*

²⁷ *Ibid*

- Specify the purposes of data sharing and clarify the limits of when disclosures of information can be made;²⁸
- Explain how the data will be retained and deleted (if applicable);²⁹ and
- Include a requirement that the agreements be submitted to the OPC for review.³⁰ The OPC should be empowered to advise on the agreement and veto in whole or in part if deemed necessary.

The agreements are important both as a regulation mechanism and a way to increase transparency around when and how Canadians' information is shared between federal bodies. For sensitive data, FIPA recommends several additional requirements for written agreements:

- A consideration of potential risks to affected individuals if the data sharing is to occur;³¹
- Steps for mitigating risk in the case of breaches;³²
- Completion of a privacy impact assessment (PIA) prior to the sharing of data; and
- An assessment of safeguards in place to protect sensitive data.³³

Both the necessity test and the written agreements function to regulate data sharing between government bodies, to minimize risks related to overcollection and re-identification of data in integrated datasets and to increase transparency.

4. Create legal requirements for the elements of privacy impact assessments

To allow for flexibility, the contents of the personal impact assessments (PIA) recommended in Proposal 3 are left to be determined through policy³⁴. Teresa Scassa takes issue with this—without any legally enforceable requirements within the PIAs

²⁸ *Ibid*

²⁹ DPO Center, "What is a DPA and why do you need one?" (18 March 2024) online: <<https://www.dpo-centre.com/blog/what-is-a-dpa-and-why-do-you-need-one/>>

³⁰ *Ibid*

³¹ EU, *Regulation 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)*, [2016] OJ L 119/1. [GDPR] at art 6.

³² Information Commissioner's Office, "Data sharing agreements" (17 October 2022) online: <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-agreements/#include>>

³³ GDPR *supra* note 31 at art. 6

³⁴ TBS *supra* note 1

themselves, the significance of requiring them diminishes.³⁵ Scassa recommends instilling at least some legal requirements for what a PIA must contain.³⁶ FIPA strongly agrees.

The purpose of a PIA, as stated by former Privacy Commissioner Therrien, is to “[identify] and [mitigate] privacy risks.”³⁷ As such, this purpose should be engrained in legal language. Scassa makes reference to Alberta’s new public sector *Protection of Privacy Act*, and the listed legal requirements for PIAs within it, as an example of how this might look.³⁸ The *Act* requires that a PIA must: “identify and review risks associated with the public body’s collection, use and disclosure of personal information”; “develop mitigation strategies and safeguards respecting those risks”; “address how the public body will comply with its duties under this Act”; and “comply with the prescribed requirements.”³⁹ These recommendations provide a minimum for what should be contained within a PIA. That said, deference should be given to the sensitivity of the information being dealt with, and the level of mitigation and duties of public bodies should be proportional to the level of sensitivity.

In that vein, Quebec’s *Act respecting the protection of personal information in the private sector* requires that the sensitivity of the given information be considered during a privacy impact assessment⁴⁰ This is also true for the *Act respecting Access to documents held by public bodies and the Protection of personal information*.⁴¹ Due to the sensitive nature of the personal information dealt with by public bodies, FIPA recommends that a consideration for sensitivity be enshrined as a legal requirement for PIAs. The Quebec legislation greatly mirrors that seen in the structure of the EU’s General Data Protection Regulation (GDPR)⁴², which provides a good measure for leading privacy legislation globally. In terms of viewing sensitivity as a spectrum, FIPA would also encourage Treasury Board of Canada (TBS)⁴³ to consider additional

³⁵ Teresa Scassa, “Privacy Act Reform: Enhancing accountability and transparency” (20 April 2026) online: <<https://teresascassa.substack.com/p/privacy-act-reform-enhancing-accountability-963>>

³⁶ *Ibid*

³⁷ House of Commons *supra* note 2 at p. 39

³⁸ Scassa *supra* note 35

³⁹ *Personal Information Protection Act*, SA 2003, c P-6.5, <<https://canlii.ca/t/56kzz>> retrieved on 2026-06-26 at s. 25(1)

⁴⁰ *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, <<https://canlii.ca/t/56cq3>> retrieved on 2026-06-26 [Act respecting the protection of personal information in the private] at Division I.1 s. 3.3

⁴¹ *Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR c A-2.1, <<https://canlii.ca/t/56lg1>> retrieved on 2026-07-08 at ss. 63.5 & 70.1

⁴² Towards a Public Law of Privacy: Meeting the Big Data Challenge, (2015), 71 SCLR (2d) 541 - 561

⁴³ Office of the Privacy Commissioner, “Protecting the privacy rights of young people” (28 November 2023), online: <https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20231128/> [Protecting the privacy rights of young people] at Privacy by Design

measures to “address specific privacy risks to vulnerable groups,” particularly risks to young people who are members of other vulnerable groups. The OPC calls this “privacy-by-design,” and it encourages government bodies to account for the experiences of vulnerable groups of young people, for example 2SLGBTQIA+ youth, Indigenous youth or young people with disabilities.⁴⁴ These considerations are important to fully address potential risks when conducting a PIA.

5. Make breach notifications under the Privacy Act mandatory and based on the application of an “unlikely to result in risk” threshold

Proposal 8 suggests that the current federal breach notification policy be adopted into law.⁴⁵ FIPA agrees that the inclusion of a legal standard for breach notification is essential to a modernized *Privacy Act*. However, the threshold for breach notification used in the current policy—the “real risk of significant harm” (RROSH) threshold⁴⁶ — is too high. Significant harm is defined by a list of potential harms which include bodily harm, financial loss, identity theft, humiliation, and more⁴⁷ The issue with this threshold is that it encourages authorities to provide no notice in cases where the risk is uncertain. Said authorities may not be equipped to assess the kinds of harm that could be caused to a given individual by the exposure of certain information⁴⁸ This is particularly true for re-identification for de-identified or anonymized data, the risk of which is not always certain.⁴⁹

The high RROSH threshold neglects that people may be uniquely vulnerable to the outcomes of a breach that a person unfamiliar with their circumstances may not consider. Furthermore, the rise of artificial intelligence and surveillance capitalism may leave individuals vulnerable to manipulation in ways that go beyond the current framework of a RROSH evaluation. For example, voter information might be used to manipulate citizens, cause them reputational harm, make them vulnerable to foreign

⁴⁴ *Ibid*

⁴⁵ TBS *supra* note 1

⁴⁶ Government of Canada, *Privacy Act Material Breach Report Form*, (March 2024), online: <<https://www.canada.ca/content/dam/tbs-sct/documents/forms/350-64e-eng.pdf>> [Privacy Act Material Breach Form]

⁴⁷ Privacy Act Material Breach Report Form *supra* note 46

⁴⁸ BC Freedom of Information and Privacy Association, Submission to the Standing Committee on Procedure and House Affairs, May 2026, online: <<https://fipa.bc.ca/wp-content/uploads/2026/05/20260501-FIPA-Bil-C-25-PROC-Submission-FINAL-V2.pdf>> [FIPA Submission]

⁴⁹ Fasken, “De-identification of Personal Information Under the Proposed Consumer Privacy Protection Act” (1 March 2021) online: <<https://www.fasken.com/en/knowledge/2021/03/1-de-identification-of-personal-information-under-the-proposed-consumer-privacy-protection-act>>

interference, and more.⁵⁰ Thus, the importance of transparency regarding breaches of personal information is substantial and ever-increasing.

In its place, FIPA suggests adopting a threshold akin to that used by the GDPR, which provides greater transparency. Outlined in Article 33, organizations must notify the relevant authority (in the Canadian case, this would be the OPC) of any breach of personal information unless it is “unlikely to result in harm.”⁵¹ This is lower than the RROSH threshold because it removes the requirement that the risk be “significant.” Furthermore, the individual should be notified of the breach “when the personal data breach is likely to result in a high risk.”⁵² This evaluation should be made by the OPC.

FIPA also recommends that breach notices provided to individuals include: the information that was subject to the breach, the perpetrator of the breach (if known), the time that the breach occurred, what steps were taken to mitigate risk, and how an individual might proceed to protect themselves from any further harm.⁵³

6. Engage in meaningful consultation with Indigenous peoples

FIPA encourages TBS to consult with rights holding collectives to ensure the government is meeting its obligations under UNDRIP, the constitution (specifically s. 35 of the *Constitution Act, 1982*), and the laws of First Nations. A rights holding collective is a term which can address First Nations, band councils, families, communities and any other group with the collective right to assert governance. FIPA is not an Indigenous organization and is not intending to speak on behalf of Indigenous Peoples, but we take this as an opportunity to highlight the importance of meaningful consultation. FIPA encourages TBS to consider the rights protected by UNDRIP, including “the right to self-determination, the right to be recognized as distinct peoples, the right to be consulted and provide free, prior and informed consent on legislation before adoption, and the right to participate in decision-making matters which would affect their rights.”⁵⁴

FIPA supports the submission made by the First Nations Information Governance Council (FNIGC) and would like to amplify the message that Indigenous peoples’ collective rights, as defined in UNDRIP, are not reflected in the current privacy

⁵⁰ FIPA Submission *supra* note 48

⁵¹ GDPR *supra* note 31 at art. 33.

⁵² GDPR *supra* note 31 art. 34

⁵³ FIPA Submission *supra* note 48

⁵⁴ Office of the Privacy Commissioner, “Issue Sheets on the examination of the federal government’s constitutional, treaty, political and legal responsibilities to First Nations, Inuit and Métis peoples and any other subject concerning Indigenous Peoples” (27 February 2024) online: < https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/appa_20240227/is_20240227/ > at Background

legislation. Specifically, this would involve meeting the obligation defined under UNDRIP as: ⁵⁵Recognizing and reaffirming that indigenous individuals are entitled without discrimination to all human rights recognized in international law, and that indigenous peoples possess collective rights which are indispensable for their existence, well-being and integral development as peoples.”⁵⁶ Meaningful consultation requires the proper acknowledgement of these collective rights and asserting them requires the government to be in conversation with rights holding collectives (given that collective rights will be asserted differently across these rights holding collectives).

Differing assertions of privacy rights by rights holding collectives is closely correlated with the “grandmother perspective,” a framework through which data governance is viewed. It centers the idea that “we need to know because we care.”⁵⁶ Meaningful consultation incorporates these perspectives, as opposed to organizing data governance systems from a purely Western view. In alignment with the grandmother perspective is the idea of creating a process for data management that is rooted in “respectful relationship.”⁵⁷ Within the scope of “respectful relationship” is the meaningful involvement of marginalized communities in the “collection, storage, use and distribution of disaggregated data.”⁵⁸

We encourage TBS to consider the FNIGC’s principles of OCAP® (Ownership, Control, Access, Possession) and their relationship to Indigenous data sovereignty, which has a direct impact on self-determination.⁵⁹ FIPA urges TBS to recall that only the rights holding collective can determine how principles of data governance and data sovereignty are implemented. OCAP® cannot be universally applied but must instead be applied in discussion with depending on how they define and implement the principles.

FIPA emphasizes that none of the above should be misconstrued to limit the expression of self-governance rights, data sovereignty rights, or any other rights. FIPA implores TBS to recall the statement of the Joint Advisory Committee on Fiscal Relations that bringing Canadian law into alignment with Indigenous data sovereignty and the

⁵⁵ United Nations Declaration on the Rights of Indigenous Peoples Act, SC 2021, c 14, <<https://canlii.ca/t/56fdv>> retrieved on 2026-07-07 at Annex.

⁵⁶ British Columbia’s Office of the Human Rights Commissioner, “Disaggregated demographic data collection in British Columbia: The grandmother perspective” (September 2020) online: < https://bchumanrights.ca/wp-content/uploads/BCOHRC_Sept2020_Disaggregated-Data-Report-FINAL.pdf page 8.> at p. 8

⁵⁷ *Ibid* at p. 9

⁵⁸ *Ibid* at p. 9

⁵⁹ First Nations Information Governance Center, “The First Nations Principles of OCAP®” online: < <https://fnigc.ca/ocap-training/>>

principles of OCAP® will require changes to legislation.⁶⁰ Indigenous perspectives are foundational to the proper, equitable, and just implementation of these principles in privacy law.

7. Include predictions about individuals within the scope of “sensitive data”

In her evaluations of the TBS Proposals for the Review of the *Privacy Act*, Scassa notes that predictions about individuals as missing from the definition of “sensitive data.”⁶¹ The sensitivity of predictions about individuals can be explained through Harvard professor Shoshana Zuboff’s concept of surveillance capitalism.⁶² This concept speaks to the level of control an organization has over individuals when given access to large-scale personal data and predictive models.⁶³ For Zuboff, surveillance capitalism is synonymous with “an overthrow of people’s sovereignty” for the sake of being controlled through behavioural modification and predictions made possible through the large-scale collection of personal data.⁶⁴ In other words, the large-scale collection of data generates predictions about behaviour which can then be used to manipulate, intervene in, and condition behaviour.⁶⁵ The desire for more accurate and invasive predictions incentivizes expanding mass private surveillance.

Zuboff’s work makes clear that predictive behavioural models have a high potential for harm against individuals. To emphasize this point, Scassa provides the example of predictions about a person’s likelihood to re-offend in a criminal context.⁶⁶ If an individual is deemed likely to re-offend, it is highly possible that this will affect their treatment in a given federal program, including federal law enforcement, potentially resulting in a harmful or unjust outcome.⁶⁷

⁶⁰ Joint Advisory Committee on Fiscal Relations, “Honouring our Ancestors by Trailblazing a Path to the Future Interim Report of the Joint Advisory Committee on Fiscal Relations - for Engagement Purposes” (2019) at page vii

⁶¹ Teresa Scassa, “Privacy Act reform must get key definitions right” (4 May 2026) online: <<https://teresascassa.substack.com/p/privacy-act-reform-must-get-key-definitions>> [Privacy Act reform]

⁶² Shoshana Zuboff, “Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization” (2022) 3: 1–79 *Organization Theory*.
<https://doi.org/10.1177/26317877221129290>

⁶³ *Ibid*

⁶⁴ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019) pt. VI

⁶⁵ John Laidler, “High tech is watching you” (4 March 2019) online: <<https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>>

⁶⁶ Privacy Act reform *supra* note 61

⁶⁷ Privacy Act reform *supra* note 54

In her book, *We, the Data: Human Rights in the Digital Age*, political scientist and scholar Wendy H. Wong discusses “data generated from data.”⁶⁸ That is, predictions drawn from personal data. She specifically references predictions around whether an individual will receive welfare, go to jail, and the like.⁶⁹ These predictions have the capacity to shape the lives of the affected individuals, leaving a huge amount of power in the hands of those in possession of the information. Given the potential power of this “data generated from data”⁷⁰ and the resulting possibility that it could cause harm if misused, it is essential that it be treated as sensitive.

8. Valid consent should be defined in the Privacy Act

As explained by Justice Canada, there are nuances to consent within the *Privacy Act*.⁷¹ For example, individuals may not be well positioned to understand what it is they are consenting to.⁷² It is also possible that requiring they consent to complex data management process may over-burden them.⁷³ These are valid concerns. That said, FIPA proposes that the clear standard of valid consent which exists in the private sector be adopted into the public sector legislation. Including this standard in the *Privacy Act* supports several of the recommendations FIPA has made about withdrawal of consent from ADS or data sharing. This may manifest as a statutory definition but may also appear in the *Act* as a freestanding section which sets a clear standard for valid consent. Advancing technology demands mechanisms through which individuals are provided more agency over their own information. Enshrining a definition of consent allows for this. The GDPR is clear that the right to withdraw consent is essential to a modern privacy regime.⁷⁴ This will be further in the following recommendation. Without a definition for valid consent, enforcement is not possible.

The consent principles in Personal Information Protection and Electronic Documents Act (*PIPEDA*), listed in both Schedule 1 Principle 3⁷⁵ and under section 6.1 (Valid Consent)⁷⁶ empower individuals to take legal action when their consent is violated. For

⁶⁸ Wong *supra* note 13

⁶⁹ Wong *supra* note 13

⁷⁰ *Ibid*

⁷¹ Government of Canada, “Privacy principles and modernized rules for a digital age” (1 September 2021) online: <https://justice.canada.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_1.html?>

⁷² *Ibid*

⁷³ *Ibid*

⁷⁴ GDPR, “What is GDPR, the EU’s new data protection law?” online: <<https://gdpr.eu/what-is-gdpr/>> [What is GDPR]

⁷⁵ *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, <<https://canlii.ca/t/56gxt>> retrieved on 2026-07-09 at 4.3 Principle 3 [PIPEDA]

⁷⁶ *Ibid* at s. 6.1

example, in *Canada (Privacy Commissioner) v. Facebook Inc.*⁷⁷, the Privacy Commissioner was found to be empowered by the consent provisions of PIPEDA to protect Facebook users whose data had been disclosed to third parties without their consent. This is a fundamental protection that should be enforced in the public sector as well as the private sector.

FIPA recommends the implementation of a clear statutory standard of valid consent akin to that included in PIPEDA:

“for the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.”⁷⁸

Section 7 in PIPEDA clarifies under what circumstances information may be used, disclosed or collected without obtaining consent from the affected individual.⁷⁹ This dimension will be essential to a standard of valid consent in the *Privacy Act*. Moreover, FIPA recommends that the Treasury Board include within the explicit standard of consent a requirement that an organization consider the reasonable expectation of the individual in relation to what they are consenting to. These recommendations are in line with the existing PIPEDA principles of consent.⁸⁰

9. Individuals must be allowed to withdraw consent from personal data sharing between government bodies

This recommendation goes hand in hand with Recommendation 7 as the principle of valid consent requires that individuals have the opportunity to withdraw consent if desired. The purpose of Proposal 1 is to eliminate bureaucratic redundancies and create an information management system that is efficient and in line with what citizens expect in a modern age.⁸¹ That said, consent cannot be entirely discarded in this pursuit. Voluntary, informed and ongoing consent sit at the core of privacy protection. Individuals must be given a mechanism through which to exercise this foundational privacy right.

⁷⁷ *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2024 FCA 140 (CanLII), <<https://canlii.ca/t/k6pn1>>, retrieved on 2026-06-26

⁷⁸ PIPEDA supra note 76 at s. 6.1

⁷⁹ *Ibid* at s. 7

⁸⁰ *Ibid* at Principle 4.3.5

⁸¹ TBS supra note 1

The GDPR represents leading legislation on privacy globally. Its regulations around consent are strict and create a necessarily high bar. The GDPR stipulates that consent must be “freely given, specific, informed and unambiguous.”⁸² Furthermore, individuals have the ability to withdraw consent at any time—which must be honored.⁸³ In line with the principle of valid consent and the example set by the GDPR, Canadian public bodies should provide the opportunity to citizens to withdraw consent from data sharing between federal bodies.

10. Re: AI decision making, governments should limit exposure of personal information to AI systems; individuals should be able to withdraw consent from AI decision-making and processing of their personal information

The Public Service Alliance of Canada (PSAC) recently shared results from a poll, indicating that “56 per cent of people across the country don’t trust AI technologies to handle their sensitive data.”⁸⁴ As with data sharing between government bodies, individuals should be given an opportunity to withdraw consent from their personal information being input to a third-party ADS or AI system. FIPA recognizes that there may be certain circumstances—for example, an emergency—where consent may need to be assumed in order for timely processing. That said, the possibility to withdraw consent should still exist.

Proposal 6 provides that individuals will receive a privacy notice before processing or as soon as possible after it begins, that their information is being processed through an ADS to make a decision about them.⁸⁵ While Proposal 5 provides that an individual may have the opportunity to ask for a human review if they believe the decision rendered by AI is incorrect⁸⁶, there are several issues with this approach.

It is unclear in the proposal whether the ability to request human review will be a requirement enshrined in law and under what circumstances an individual might request this before AI processing begins. If individuals are only able to request a re-evaluation of their information following a decision made by ADS rather than contest prior to the decision, it is possible any subsequent review may be unfairly influenced by the AI decision. This is referred to as automation bias—a tendency to over-rely on automated, computer-generated decisions rather than deferring to human input which may, in some

⁸² What is GDPR *supra* note 74 at Consent

⁸³ *Ibid*

⁸⁴ Public Service Alliance of Canada, “PSAC pushes back on federal AI strategy” (12 June 2026) online: <<https://psacunion.ca/psac-pushes-back-federal-ai-strategy>> at para. 4

⁸⁵ TBS *supra* note 1

⁸⁶ TBS *supra* note 1

circumstances, be more accurate.⁸⁷ FIPA's concern is that even with the ability to request human review following the rendering of a decision based on personal information, inaccurate decisions may still be made due to the prevalence of automation bias and the known biases that can be perpetuated by ADS systems.

Individuals concerned about data leakage through third-party AI systems, or profiling based on biases, should have a right to contest their information being used by AI or ADS before it is entered into the system. If notice that an individual's information will be processed through AI comes after processing has begun, there is no recourse of the individual to avoid the processing altogether. It is well documented that unconscious or unintentional biases in either the data or the algorithm used for AI can be reflected in the decisions it makes.⁸⁸ Called algorithmic bias, this can lead to discriminatory decisions based on biases within AI systems around race, gender, religion, disability, sexual orientation, and more.⁸⁹ For example, 2SLGBTQIA+ representation in data used to train AI can be lacking.⁹⁰ This can lead to AI output which reproduces stereotypes and "misrepresent[s] diverse experiences."⁹¹ These misrepresentations can then impact results generated from ADS and lead to unfair and discriminatory outcomes.

It is also important to consider an angle of over-collection and potential dangers this poses to members of a given community. These can include the "predicting of LGBTQ+ identities based upon sensitive data,"⁹² which has the potential to lead to targeted manipulation, cyberbullying⁹³ or hate speech in the hands of bad actors.⁹⁴ These harms are often exacerbated for 2SLGBTQIA+ youth.⁹⁵ FIPA encourages the consideration of potential harms to vulnerable groups, namely the potential for data leakage, over-collection, and algorithmic bias.

These issues are heightened by the opacity of automated decision making. When a decision is made through ADS, its reasoning may not be accessible.⁹⁶ While the

⁸⁷ Kate Goddard, Abdul Roudsari & Jeremy C Wyatt, "Automation bias: a systematic review of frequency, effect mediators, and mitigators" (2011) 19:1 Journal of the American Medical Informatics Association 121. 10.1136/amiajnl-2011-000089

⁸⁸ Practical Guidance Lawyer Team, "Artificial Intelligence Risk Management" (16 December 2025) online: <<https://plus.lexis.com/api/permalink/a81934bf-8aeb-49f5-8385-7d0b82db9e18/?context=1537339>>

⁸⁹ Anna Su, "Gender Equality, AI and the Future of Human Rights" (2025) University of Toronto Law Journal.

⁹⁰ GLAAD, "Understanding LGBTQ Impacts Across AI" online: <<https://glaad.org/2026-ai-report-build-for-everyone/lgbtq-impacts/>> [GLAAD]

⁹¹ *Ibid* at para. 2

⁹² Let's Talk about Bias: LGBTQ+ People and AI" (28 June 2022) online: <<https://www.correlation-one.com/blog/lgbtq-people-ai-algorithmic-bias-harm>> at algorithmic harm

⁹³ *Ibid*

⁹⁴ Institut national de la recherche scientifique, "David Myles: The Paradox of Digital Platforms for LGBTQ+ Communities LGBTQ" (10 June 2025) online: <<https://inrs.ca/en/news/david-myles-the-paradox-of-digital-platforms-for-lgbtq-communities-lgbtq/>>

⁹⁵ *Ibid*

⁹⁶ Bradley Henderson, *Maintaining Legitimacy: Artificial Intelligence, Automated Decision Making, and Reasonableness Review under Canadian Administrative Law*, (2025) 58:2 UBC L Rev 415 – 474

personal data inputted can be reported, how the ADS came to a certain decision is unlikely to be transparent. As put by the Bradley Henderson in the UBC Law Review, “If affected individuals cannot understand an [ADS] tool’s reasoning, how are those individuals [...] expected to assess whether the decision maker exercised its public power in a fair, proper, and otherwise lawful manner?”⁹⁷ It is also important to note an existing distrust of government decision making which is further eroded by the integration of AI into such decisions.⁹⁸ If government bodies are to proceed with the integration of ADS in their daily tasks, individuals should be given the opportunity to object on the basis that the potential harms are uncertain and severe.

A major issue with machine learning is how difficult it is to be certain that data has been removed from the model. Generative AI models trained on data scraped from the internet, such as those powering many chatbot-style interfaces like ChatGPT and Claude have been known to memorize personal data, making it nearly impossible to be certain if a person’s information has been truly deleted from the model.⁹⁹ Furthermore, it is becoming increasingly easy for bad actors to re-identify de-identified or anonymized data.¹⁰⁰ As noted in Recommendation 1.¹⁰¹ With this in mind, FIPA recommends that synthetic data be used whenever possible to minimize the risk of identifiable personal information being scraped by AI systems and misused. Furthermore, individuals should be given the opportunity to withdraw their consent from their information being inputted into AI or ADS before it happens.

11. Transparency rights for public sector workers regarding employee monitoring should be enhanced

Defined as the “computerized collection, storage, analysis and reporting of information about employees’ productive activities,”¹⁰² employee monitoring is a phenomenon of increasing concern.¹⁰³ New technology is capable of collecting new types of data, causing a rise in employee monitoring.¹⁰⁴ A sound and just approach to legal regulation of this practice requires that the employer’s legitimate business interests be balanced

⁹⁷ *Ibid* at p. 416

⁹⁸ *Ibid*

⁹⁹ Stanford University, “Privacy in an AI Era: How Do We Protect Our Personal Information?” (18 March 2024) online: <<https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>>

¹⁰⁰ Rishabh Poddar, “Why Data Anonymization Isn’t Enough in the Age of AI” (24 April 2024) online: <<https://www.opaque.co/resources/articles/why-data-anonymization-isnt-enough-in-the-age-of-ai>>

¹⁰¹ Australian Bureau of Statistics *supra* note 19

¹⁰² Johnathan Yerby, “Legal and ethical issues of employee monitoring” (2013) 1:2 Online Journal of Applied Knowledge Management 44 at p. 44

¹⁰³ Office of the Privacy Commissioner, “Protecting Employee Privacy in the Modern Workplace” 4-5 October 2023) online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_02/> [OPC 2023]

¹⁰⁴ Mohammed (Joe) Masoodi et al, Monitoring Remote Work in Canada: Support or Surveillance?, (Future Skills Center, 2023).

with their employees' individual rights. That said, there are several transparency concerns linked to employee monitoring.

One concern noted by PSAC is so-called “enhanced tracking,” where surveillance is bolstered by AI tools to monitor worker performance and to discipline them.¹⁰⁵ As this data is used by algorithmic models to make predictions about future output and productivity as an employee, there is a higher chance that the collection of this data can impact employee’s careers. Examples of the data collected goes beyond typical human observation, for example, monitoring of fatigue levels, abilities to stay calm under pressure, predictions about whether they are likely to succeed or about whether they may search for a different job.¹⁰⁶ The OPC has described it as having a “chilling effect” on employee’s sense of autonomy and creativity.¹⁰⁷ FIPA agrees with this conclusion. Taking into account examples from the above recommendations concerning the potential for predictive models to perpetuate harmful biases, and the effects monitoring can have on employees, certain safeguards should be put in place to minimize these prospective harms.

To ensure employee privacy rights are protected, the OPC recommends three principles to provide guidance on employee monitoring: employee monitoring should be “reasonable, proportionate and minimally intrusive.”¹⁰⁸ Codification of these principles would balance permitting a reasonable level of data collection about workers with respect to workers’ rights. At minimum, these principles should be enshrined in law to ensure sufficient protection for workers whose information is held by federal bodies. The OPC is also concerned about over-collection of data, or monitoring that is excessive¹⁰⁹ and FIPA shares these concerns. If enshrined in law, the three aforementioned principles would address these concerns.

12. Application of the Privacy Act could extend to Parliamentary offices and offices of MPs

In a submission to Senate Standing Committee on Legal and Constitutional Affairs on Bill C-4, Professor at McMaster University and Canada Research Chair in Communication Policy and Governance Sara Bannerman stated that the *Privacy Act*

¹⁰⁵ OPC 2023 *supra* note 103

¹⁰⁶ OPC 2023 *supra* note 103

¹⁰⁷ OPC 2023 *supra* note 103 at Context

¹⁰⁸ Office of the Privacy Commissioner, “Privacy in the Workplace” (29 May 2025) online: <https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17/?wbdisable=true> [Privacy in the Workplace]

¹⁰⁹ *Ibid*

and *PIPEDA* are governed by ten fair information principles.¹¹⁰ These include requirements to establish safeguards against privacy breaches, “obtain consent for the collection, use and disclosure of personal information,” “identify the purpose for which personal information is collected,” and more.¹¹¹ These rights are vital to maintaining the safety of individuals’ personal information.

Members of Parliament are not regulated by either the *Privacy Act* or *PIPEDA*—this is a problem. MPs regularly deal with voter data, which is generally considered highly sensitive because of the severe potential harms of misusing such personal information. Profiling voters, the identification of vulnerable groups, and voter intimidation are just a few examples.¹¹² Bill C-4, now the *Making Life More Affordable for Canadians Act*, and Bill C-25, now the *Strong and Free Elections Act*, work effectively to exempt federal political parties from both the *Privacy Act* and *PIPEDA* and thus the ten information principles. MPs are governed purely by internal privacy policies, which can lead to problems of enforcement and regulation. This is far below the standard Canadians expect.¹¹³

The dangers of unregulated access to sensitive voter information were demonstrated by this year’s Alberta data breach, wherein the highly sensitive voter data possessed by a provincial political party was disclosed to a third party. The number of people who have accessed the information is still unknown, and investigations estimate it could range as high as the thousands.¹¹⁴ This breach, and the public’s reaction to it, demonstrates a clear need for external data governance within the offices of Parliament that, at minimum, make them answerable to the ten fair information principles. Beyond that, the *Privacy Act* should be implemented by Parliament to the greatest extent possible.

¹¹⁰ Sara Bannerman, “Submission to the Senate Standing Committee on Legal and Constitutional Affairs on Bill C-4, an Act Respecting Certain Affordability Measures for Canadians and Another Measure” (11 December 2025) online: < https://sencanada.ca/Content/Sen/Committee/451/LCJC/briefs/LCJC_SM-C-4_Brief_SaraBannerman_e.pdf>

¹¹¹ The Honourable David M. Arnot & The Honourable Denise Batters, Privacy Issues Regarding Federal Political Parties under the Canada Elections, Interim report of the Standing Senate Committee on Legal and Constitutional Affairs, (Ottawa, Ontario: Senate Canada, 2026) at p. 25

¹¹² FIPA Submission *supra* note 48

¹¹³ *Ibid*

¹¹⁴ Jack Farrell and Lisa Johnson, “Scope of access to leaked Alberta voter list may be incomplete: Elections Alberta,” The Canadian Press (13 May 2026), online: <https://www.thecanadianpressnews.ca/prairies_bc/alberta/scope-of-access-to-leaked-alberta-voter-list-may-be-incomplete-elections-alberta/article_7a819434-87ce-5d63-abf0-f82e50814478.html>

Appendix 1 FIPA Commentary on Policy Proposals

This portion of FIPA's submission is formatted to reflect the online questions for the Treasury board review found online on [2026 Review of the Privacy Act: Policy Approaches](#).

Theme 1: Enabling integrated services

Proposal 1: Enable responsible sharing and reuse of personal data across government programs

FIPA would like to highlight the potential dangers of data sharing without the consent of the affected individuals. Consent is a foundational pillar of an individual's privacy rights—should it be sidestepped as suggested by Proposal 1, it is vital that several additional safeguards be implemented to increase the security of individuals' personal information. FIPA recommends employing the necessity test recommended in Proposal 10 to data sharing between government programs. When smaller data sets are combined to create larger, integrated datasets, the risk of re-identification is substantially higher, even if the data has been de-identified or anonymized.¹¹⁵ The depth and expansiveness of the data increase the potential degree of harm in the event of a breach. The idea of utilizing a necessity test for cross-program data sharing was supported by the House of Commons Committee in 2016.¹¹⁶

Moreover, in 2016, the House of Commons heard from a number of experts regarding the *Privacy Act*; many concurred that requiring written agreements governing data-sharing between governments was important for the protection of personal information.¹¹⁷ They officially recommended that all information sharing between government bodies be governed by written agreements and that these agreements be published.¹¹⁸ This was supported by the Privacy and Access Law Section of the Canadian Bar Association for the following reasons: (i) to protect the fundamental rights of individuals and (ii) to hold government agencies to account.¹¹⁹ FIPA agrees with this recommendation; in our view it should be applied to a modernized *Privacy Act*.

The agreements are important both as a regulation mechanism and a way to increase transparency around when and how Canadian's information is shared between federal

¹¹⁵ Australian Institute of Statistics, "Understanding re-identification" (8 November 2021) online: <<https://www.abs.gov.au/statistics/understanding-statistics/data-confidentiality-guide/understanding-re-identification>> [Australian Bureau of Statistics]

¹¹⁶ Blaine Calkins, *Protecting the Privacy of Canadians: Review of the Privacy Act, Report of the Standing Committee on Access to Information, Privacy and Ethics*, (House of Commons, 2016). [House of Commons]

¹¹⁷ House of Commons *supra* note 116

¹¹⁸ *Ibid*

¹¹⁹ *Ibid* at p. 11

bodies. Both the necessity test and the requirement of written agreements function to regulate data sharing between government bodies, minimize risks related to overcollection and re-identification of data in integrated datasets, and increase transparency.

The purpose of Proposal 1 is to eliminate bureaucratic redundancies and create an information management system that is efficient and in line with what citizens expect in a modern age.¹²⁰ That said, consent cannot be entirely discarded in this pursuit. Voluntary, informed and ongoing consent sit at the core of privacy protection. Individuals must be given a mechanism through which to exercise this foundational privacy right.

The GDPR represents leading legislation on privacy globally. Its regulations around consent are strict and create a necessarily high bar. The GDPR stipulates that consent must be “freely given, specific, informed and unambiguous.”¹²¹ Furthermore, individuals have the ability to withdraw consent at any time—which must be honored.¹²² In line with the principle of valid consent and the example set by the GDPR, Canadian public bodies should provide the opportunity to citizens to withdraw consent from data sharing between federal bodies.

Proposal 2: Establish designated official sources of government digital data

FIPA would like to take this opportunity to point to the Canadian Union of Public Employees’ (CUPE) submission which asks about the safeguards that will be put in place to protect a source of personal data that is centralized to the degree described in Proposal 2. CUPE is particularly concerned with information specific to workers—for example, data related to their hiring or termination. FIPA would like to amplify CUPE’s concern for how this data will be protected if it is stored within a designated official source.

Moreover, as pointed out by FIPA in response to Proposal 1, large, integrated datasets raise the risk of harm for those whose personal data they contain, particularly with respect to re-identification of de-identified or anonymized data.¹²³ Taking these risks into account with the added consideration of CUPE’s concern for worker’s personal data

¹²⁰ Treasury Board of Canada Secretariat, “2026 Review of the Privacy Act: Policy Approaches” (2 April 2026) online: <<https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/privacy-act-modernization-policy-approaches/2026-review-privacy-act-policy-approaches.html>> [TBS]

¹²¹ GDPR, “What is GDPR, the EU’s new data protection law?” online: <<https://gdpr.eu/what-is-gdpr/>> at Consent [What is GDPR]

¹²² *Ibid*

¹²³ Australian Bureau of Statistics *supra* note 115

in particular, FIPA urges TBS to consider substantial safeguards before implementing a data management system with this degree of integration.

Theme 2: Enhancing accountability and transparency

Proposal 3: Create a legal requirement to conduct a privacy impact assessment when a program or activity uses personal data to make a decision about someone

To allow for flexibility, the contents of the personal impact assessments (PIA) recommended in Proposal 3 are left to be determined through policy¹²⁴. Teresa Scassa takes issue with this—without any legally enforceable requirements within the PIAs themselves, the significance of requiring them diminishes.¹²⁵ Scassa recommends instilling at least some legal requirements for what a PIA must contain.¹²⁶ FIPA strongly agrees.

The purpose of a PIA, as stated by former Privacy Commissioner Therrien, is to “[identify] and [mitigate] privacy risks.”¹²⁷ As such, this purpose should be engrained in legal language. Scassa makes reference to Alberta’s new public sector *Protection of Privacy Act*, and the listed legal requirements for PIAs within it, as an example of how this might look.¹²⁸ The *Act* requires that a PIA must: “identify and review risks associated with the public body’s collection, use and disclosure of personal information”; “develop mitigation strategies and safeguards respecting those risks”; “address how the public body will comply with its duties under this Act”; and “comply with the prescribed requirements.”¹²⁹ These recommendations provide a minimum for what should be contained within a PIA. That said, deference should be given to the sensitivity of the information being dealt with, and the level of mitigation and duties of public bodies should be proportional to the level of sensitivity.

In that vein, Quebec’s *Act respecting the protection of personal information in the private sector* requires that the sensitivity of the given information be considered during

¹²⁴ TBS *supra* note 120

¹²⁵ Teresa Scassa, “Privacy Act Reform: Enhancing accountability and transparency” (20 April 2026) online: <<https://teresascassa.substack.com/p/privacy-act-reform-enhancing-accountability-963>> [Scassa]

¹²⁶ *Ibid*

¹²⁷ House of Commons *supra* note 116 at p. 39

¹²⁸ Scassa *supra* note 125

¹²⁹ *Personal Information Protection Act*, SA 2003, c P-6.5, <<https://canlii.ca/t/56kzz>> retrieved on 2026-06-26 at s. 25(1)

a privacy impact assessment¹³⁰ This is also true for the *Act respecting Access to documents held by public bodies and the Protection of personal information*.¹³¹ Due to the sensitive nature of the personal information dealt with by public bodies, FIPA recommends that a consideration for sensitivity be enshrined as a legal requirement for PIAs. The Quebec legislation greatly mirrors that seen in the structure of the EU's General Data Protection Regulation (GDPR)¹³², which provides a good measure for leading privacy legislation globally.

In terms of viewing sensitivity as a spectrum, FIPA would also encourage Treasury Board of Canada (TBS)¹³³ to consider additional measures to “address specific privacy risks to vulnerable groups,” particularly risks to young people who are members of other vulnerable groups. The OPC calls this “privacy-by-design,” and it encourages government bodies to account for the experiences of vulnerable groups of young people, for example 2SLGBTQIA+ youth, Indigenous youth or young people with disabilities.¹³⁴ These considerations are important to fully address potential risks when conducting a PIA.

Proposal 4: Create a central registry of personal data holdings and publish key information on personal data management practices

No additional commentary.

Proposal 5: Establish transparency requirements for the use of artificial intelligence and automated decision systems that support the right to the correction of personal data

Transparency requirements are important for the use of AI and ADS, as is the ability to assert the fundamental right of correction. That said, Proposal 5 does not go far enough to protect individual rights when their personal data is used by AI. While this proposal provides that an individual may have the opportunity to ask for human review if they believe the decision rendered by AI is incorrect, there are several issues with this approach.

¹³⁰ *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, <<https://canlii.ca/t/56cq3>> retrieved on 2026-06-26 [Act respecting the protection of personal information in the private] at Division I.1 s. 3.3

¹³¹ *Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR c A-2.1, <<https://canlii.ca/t/56lg1>> retrieved on 2026-07-08 at ss. 63.5 & 70.1

¹³² Towards a Public Law of Privacy: Meeting the Big Data Challenge, (2015), 71 SCLR (2d) 541 - 561

¹³³ Office of the Privacy Commissioner, “Protecting the privacy rights of young people” (28 November 2023), online: <https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20231128/> [Protecting the privacy rights of young people] at Privacy by Design

¹³⁴ *Ibid*

It is unclear in the proposal whether the ability to request human review will be a requirement enshrined in law and under what circumstances an individual might request this before AI processing begins. If individuals are only able to request a re-evaluation of their information following a decision made by ADS rather than contest prior to the decision, it is possible any subsequent review may be unfairly influenced by the AI decision. This is referred to as automation bias—a tendency to over-rely on automated, computer-generated decisions rather than deferring to human input which may, in some circumstances, be more accurate.¹³⁵ FIPA's concern is that even with the ability to request human review following the rendering of a decision based on personal information, inaccurate decisions may still be made due to the prevalence of automation bias and the known biases that can be perpetuated by ADS systems.

Individuals concerned about data leakage through third-party AI systems, or profiling based on biases, should have a right to contest their information being used by AI or ADS before it is entered into the system. If notice that an individual's information will be processed through AI comes after processing has begun, there is no recourse of the individual to avoid the processing altogether. It is well documented that unconscious or unintentional biases in either the data or the algorithm used for AI can be reflected in the decisions it makes.¹³⁶ Called algorithmic bias, this can lead to discriminatory decisions based on biases within AI systems around race, gender, religion, disability, sexual orientation, and more.¹³⁷ For example, 2SLGBTQIA+ representation in data used to train AI can be lacking.¹³⁸ This can lead to AI output which reproduces stereotypes and “misrepresent[s] diverse experiences.”¹³⁹ These misrepresentations can then impact results generated from ADS and lead to unfair and discriminatory outcomes.

These issues are heightened by the opacity of automated decision making. When a decision is made through ADS, its reasoning may not be accessible.¹⁴⁰ While the personal data inputted can be reported, how the ADS came to a certain decision is unlikely to be transparent. As put by the Bradley Henderson in the UBC Law Review, “If affected individuals cannot understand an [ADS] tool's reasoning, how are those individuals [...] expected to assess whether the decision maker exercised its public power in a fair, proper, and otherwise lawful manner?”¹⁴¹ It is also important to note an existing distrust of government decision making which is further eroded by the

¹³⁵ Kate Goddard, Abdul Roudsari & Jeremy C Wyatt, “Automation bias: a systematic review of frequency, effect mediators, and mitigators” (2011) 19:1 Journal of the American Medical Informatics Association 121. 10.1136/amiajnl-2011-000089

¹³⁶ Practical Guidance Lawyer Team, “Artificial Intelligence Risk Management” (16 December 2025) online: <<https://plus.lexis.com/api/permalink/a81934bf-8aeb-49f5-8385-7d0b82db9e18/?context=1537339>>

¹³⁷ Anna Su, “Gender Equality, AI and the Future of Human Rights” (2025) University of Toronto Law Journal.

¹³⁸ GLAAD, “Understanding LGBTQ Impacts Across AI” online: <<https://glaad.org/2026-ai-report-build-for-everyone/lgbtq-impacts/>> [GLAAD]

¹³⁹ *Ibid* at para. 2

¹⁴⁰ Bradley Henderson, *Maintaining Legitimacy: Artificial Intelligence, Automated Decision Making, and Reasonableness Review under Canadian Administrative Law*, (2025) 58:2 UBC L Rev 415 – 474

¹⁴¹ *Ibid* at p. 416

integration of AI into such decisions.¹⁴² If government bodies are to proceed with the integration of ADS in their daily tasks, individuals should be given the opportunity to object on the basis that the potential harms are uncertain and severe.

A major issue with machine learning is how difficult it is to be certain that data has been removed from the model. Generative AI models trained on data scraped from the internet, such as those powering many chatbot-style interfaces like ChatGPT and Claude have been known to memorize personal data, making it nearly impossible to be certain if a person's information has been truly deleted from the model.¹⁴³ Furthermore, it is becoming increasingly easy for bad actors to re-identify de-identified or anonymized data.¹⁴⁴

A true modernization of the *Privacy Act* requires strong safeguards against new and evolving technology. FIPA recommends that the necessity test in Proposal 10 be applied to the use of artificial intelligence and automated decision-making systems. In 2023, the Office of the Privacy Commissioner of Canada addressed privacy protection in the responsible use of artificial intelligence.¹⁴⁵ It recommended that organizations using AI establish both the necessity and proportionality of its use for the given purpose.¹⁴⁶ The necessity test (as described in Proposal 10) could be applied to decisions about AI use, with the addition of a proportionality step.

With all this in mind and to minimize the risk of identifiable personal information being scraped from AI systems and misused, FIPA recommends that synthetic data be used whenever possible. Furthermore, individuals should be given the opportunity to withdraw consent from their information being inputted into AI or ADS before it happens. Lastly, Canadians' personal information should not be subject to such risks without proper safeguards—a necessity and proportionality test demands a level of due diligence that is essential in the face of this high a threat to personal information.

Proposal 6: Strengthen privacy notice requirements, including when automated decision systems are used

Privacy notices are important but do not go far enough to empower the individual in the management of their personal information. Proposal 6 provides that individuals will

¹⁴² *Ibid*

¹⁴³ Stanford University, “Privacy in an AI Era: How Do We Protect Our Personal Information?” (18 March 2024) online: <<https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>>

¹⁴⁴ Rishabh Poddar, “Why Data Anonymization Isn’t Enough in the Age of AI” (24 April 2024) online: <<https://www.opaque.co/resources/articles/why-data-anonymization-isnt-enough-in-the-age-of-ai>>

¹⁴⁵ Office of the Privacy Commissioner of Canada, “Principles for responsible, trustworthy and privacy-protective generative AI technologies” (7 December 2023) online: <https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_a_i/#fn4>

¹⁴⁶ *Ibid*

receive a privacy notice before, or as soon as possible, that their information is being processed through an ADS to make a decision about them. FIPA recommends going a step further and allowing individuals to withdraw consent from ADS being used to process their personal information.

The Public Service Alliance of Canada (PSAC) recently shared results from a poll, indicating that “56 per cent of people across the country don’t trust AI technologies to handle their sensitive data.”¹⁴⁷ As with data sharing between government bodies, individuals should be given an opportunity to withdraw consent from their personal information being input to a third-party ADS or AI system. FIPA’s response to Proposal 5 highlights the numerous dangers associated with the input of personal information into AI or ADS. With these risks in mind, FIPA recommends that individuals have the opportunity to withdraw consent from AI or ADS processing of their information before it begins.

Theme 3: Advancing safeguards across the spectrum of data sensitivity

Proposal 7: Recognize a spectrum of data sensitivity and identifiability in law

FIPA supports this proposal and furthermore recommends that predictions about people be included within the scope of sensitive data. In her evaluations of the TBS Proposals for the Review of the *Privacy Act*, Scassa notes that predictions about individuals as missing from the definition of “sensitive data.”¹⁴⁸ The sensitivity of predictions about individuals can be explained through Harvard professor Shoshana Zuboff’s concept of surveillance capitalism.¹⁴⁹ This concept speaks to the level of control an organization has over individuals when given access to large-scale personal data and predictive models.¹⁵⁰ For Zuboff, surveillance capitalism is synonymous with “an overthrow of people’s sovereignty” for the sake of being controlled through behavioural modification

¹⁴⁷ Public Service Alliance of Canada, “PSAC pushes back on federal AI strategy” (12 June 2026) online: <<https://psacunion.ca/psac-pushes-back-federal-ai-strategy>> at para. 4

¹⁴⁸ Teresa Scassa, “Privacy Act reform must get key definitions right” (4 May 2026) online: <<https://teresascassa.substack.com/p/privacy-act-reform-must-get-key-definitions>> [Privacy Act reform]

¹⁴⁹ Shoshana Zuboff, “Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization” (2022) 3: 1–79 *Organization Theory*.
<https://doi.org/10.1177/26317877221129290>

¹⁵⁰ *Ibid*

and predictions made possible through the large-scale collection of personal data.¹⁵¹ In other words, the large-scale collection of data generates predictions about behaviour which can then be used to manipulate, intervene in, and condition behaviour.¹⁵² The desire for more accurate and invasive predictions incentivizes expanding mass private surveillance.

Zuboff's work makes clear that predictive behavioural models have a high potential for harm against individuals. To emphasize this point, Scassa provides the example of predictions about a person's likelihood to re-offend in a criminal context.¹⁵³ If an individual is deemed likely to re-offend, it is highly possible that this will affect their treatment in a given federal program, including federal law enforcement, potentially resulting in a harmful or unjust outcome.¹⁵⁴

In her book, *We, the Data: Human Rights in the Digital Age*, political scientist and scholar Wendy H. Wong discusses "data generated from data."¹⁵⁵ That is, predictions drawn from personal data. She specifically references predictions around whether an individual will receive welfare, go to jail, and the like.¹⁵⁶ These predictions have the capacity to shape the lives of the affected individuals, leaving a huge amount of power in the hands of those in possession of the information. Given the potential power of this "data generated from data"¹⁵⁷ and the resulting possibility that it could cause harm if misused, it is essential that it be treated as sensitive.

Proposal 8: Create a legal requirement for the management, notification and reporting of privacy breaches

Proposal 8 suggests that the current federal breach notification policy be adopted into law.¹⁵⁸ FIPA agrees that the inclusion of a legal standard for breach notification is essential to a modernized *Privacy Act*. However, the threshold for breach notification used in the current policy—the "real risk of significant harm" (RROSH) threshold¹⁵⁹ — is too high. Significant harm is defined by a list of potential harms which include bodily

¹⁵¹Soshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019) pt. VI

¹⁵²John Laidler, "High tech is watching you" (4 March 2019) online: <<https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>>

¹⁵³ Privacy Act reform *supra* note 61

¹⁵⁴ Privacy Act reform *supra* note 54

¹⁵⁵ Wendy H. Wong, *We, the Data: Human Rights in the Digital Age* (The MIT Press, 2023).

¹⁵⁶ Wong *supra* note 155

¹⁵⁷ *Ibid*

¹⁵⁸ TBS *supra* note 120

¹⁵⁹ Government of Canada, *Privacy Act Material Breach Report Form*, (March 2024), online: <<https://www.canada.ca/content/dam/tbs-sct/documents/forms/350-64e-eng.pdf>> [Privacy Act Material Breach Form]

harm, financial loss, identity theft, humiliation, and more¹⁶⁰ The issue with this threshold is that it encourages authorities to provide no notice in cases where the risk is uncertain. Said authorities may not be equipped to assess the kinds of harm that could be caused to a given individual by the exposure of certain information¹⁶¹ This is particularly true for re-identification for de-identified or anonymized data, the risk of which is not always certain.¹⁶²

The high RROSH threshold neglects that people may be uniquely vulnerable to the outcomes of a breach that a person unfamiliar with their circumstances may not consider. Furthermore, the rise of artificial intelligence and surveillance capitalism may leave individuals vulnerable to manipulation in ways that go beyond the current framework of a RROSH evaluation. For example, voter information might be used to manipulate citizens, cause them reputational harm, make them vulnerable to foreign interference, and more.¹⁶³ Thus, the importance of transparency regarding breaches of personal information is substantial and ever-increasing.

In its place, FIPA suggests adopting a threshold akin to that used by the GDPR, which provides greater transparency. Outlined in Article 33, organizations must notify the relevant authority (in the Canadian case, this would be the OPC) of any breach of personal information unless it is “unlikely to result in harm.”¹⁶⁴ This is lower than the RROSH threshold because it removes the requirement that the risk be “significant.” Furthermore, the individual should be notified of the breach “when the personal data breach is likely to result in a high risk.”¹⁶⁵ This evaluation should be made by the OPC.

FIPA also recommends that breach notices provided to individuals include: the information that was subject to the breach, the perpetrator of the breach (if known), the time that the breach occurred, what steps were taken to mitigate risk, and how an individual might proceed to protect themselves from any further harm.¹⁶⁶

¹⁶⁰ *Ibid*

¹⁶¹ BC Freedom of Information and Privacy Association, Submission to the Standing Committee on Procedure and House Affairs, May 2026, online: < <https://fipa.bc.ca/wp-content/uploads/2026/05/20260501-FIPA-Bil-C-25-PROC-Submission-FINAL-V2.pdf> > [FIPA Submission]

¹⁶² Fasken, “De-identification of Personal Information Under the Proposed Consumer Privacy Protection Act” (1 March 2021) online: <<https://www.fasken.com/en/knowledge/2021/03/1-de-identification-of-personal-information-under-the-proposed-consumer-privacy-protection-act>>

¹⁶³ FIPA Submission *supra* note 161

¹⁶⁴ EU, *Regulation 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)*, [2016] OJ L 119/1. [GDPR] at art. 33.

¹⁶⁵ GDPR *supra* note 164 art. 34

¹⁶⁶ FIPA Submission *supra* note 161

Proposal 9: Reinforce existing safeguard requirements by making them a legal requirement

While FIPA agrees that elevating existing safeguards to legal requirements is beneficial, it shares a concern put forth in CUPE's submission. That concern is about federal employee's personal information stored outside of Canada. FIPA would like to both amplify this concern and extend it more generally to personal information of Canadian citizens en masse, that is held outside of Canada. Importantly, the flow of data between countries creates uncertainty as to which data protection laws apply.¹⁶⁷ This uncertainty creates a situation in which citizens' personal data may be disclosed to foreign governments.¹⁶⁸ More clarity is needed on the precise safeguards that will be implemented to protect information stored or processed outside of Canada.

Proposal 10: Add necessity test to the threshold for limiting collection

FIPA agrees with this proposal but suggests adding proportionality as a step in the necessity test. Proportionality has been strongly advocated for many years. The House of Commons supported the OPC's recommendation that the necessity test for the collection of personal information resemble the factors of the Oakes test in the Supreme Court of Canada case *R v. Oakes*.¹⁶⁹ Each of these steps have been included in Proposal 10 except for proportionality, (the OPC describes proportionality as personal information being collected when "the loss of privacy is proportional to the importance of the objectives of the program or activity"¹⁷⁰). The House of Commons Committee, upon hearing a range of testimony on whether or not proportionality should be included separately from the necessity consideration, determined that proportionality was a vital consideration on its own as it informed the overall necessity of the collection of the data.¹⁷¹

It is vital that the benefit, use, and purpose of the information not be considered in isolation. To ensure that individuals' personal information is protected and provide appropriate perspective, the detriment to their privacy must be considered in comparison to the potential gain. The higher the infringement of peoples' privacy, the stronger the justification must be.

¹⁶⁷ Government of Canada. "Government of Canada White Paper: Data Sovereignty and Public Cloud" (23 April 2026) online: < <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html?>>

¹⁶⁸ *Ibid*

¹⁶⁹ *R. v. Oakes*, [1986] 1 S.C.R. 103

¹⁷⁰ House of Commons *supra* note 116 at pt. 4

¹⁷¹ House of Commons *supra* note 116

Proposal 11: Create a new requirement to dispose of personal data that is not necessary

FIPA agrees with this proposed amendment. Data deletion is important in the context of the collection of personal information as it prioritizes the security of the individual's information. This is particularly important given certain points brought to light by FIPA under different proposals. For example, de-identified and anonymized data can be re-identified with increasing ease.¹⁷² Benjamin J. Keele discusses the importance of data deletion and emphasizes that, when implemented, the risk of misuse of personal information is minimized, and the security of the information is thus enhanced.¹⁷³

Theme 4: Modernizing the foundation for privacy and trust

Proposal 12: Amend the *Act* to recognize privacy as a fundamental right, underscore the importance of enabling service, and advance reconciliation with Indigenous Peoples

FIPA supports the treatment of privacy as a “core democratic value,”¹⁷⁴ and encourages its transformation into a fundamental right. FIPA endorses amending the preamble of the *Act* to reflect both the individual's right to privacy and the advancement of reconciliation with Indigenous Peoples.

Proposal 13: Incorporate principles into the *Privacy Act* to strengthen privacy practices and align with private sector privacy legislation and other international standards

FIPA agrees that incorporating principles into the *Privacy Act* will serve to strengthen its interpretation in favour of enhancing individuals' privacy protection. In line with the recommendations it has made above, FIPA would like to specifically encourage the adoption several principles suggested by TBS, namely proportionality, necessity, privacy-by-design, effectiveness, and minimal intrusiveness.

In addition to the principles already included within this proposal, FIPA proposes several other principles for consideration. Articulated by Justice Canada, reasonableness has been described as a principle going hand in hand with proportionality because it encourages the consideration of privacy risks to individuals before information is

¹⁷² Australian Bureau of Statistics *supra* note 115

¹⁷³ Benjamin J. Keele, “Privacy by Deletion: The Need for a Global Data Deletion Principle” (2009) 16:1 *Indiana Journal of Global Legal Studies* 363

¹⁷⁴ TBS *supra* at note 120

shared, used, disclosed or retained.¹⁷⁵ Data security was another principle proposed by Justice Canada that FIPA would like to call attention to here.¹⁷⁶ A data security principle encourages bodies “to take appropriate care” which involves maintaining up-to-date security protocols and adjusting these principles according to the sensitivity of the information.¹⁷⁷ FIPA encourages TBS to consider both of these principles alongside those already articulated.

Proposal 14: Add key definitions in the *Privacy Act*

FIPA agrees with the proposed definitions but poses another for consideration: consent. As explained by Justice Canada, there are nuances to consent within the *Privacy Act*.¹⁷⁸ For example, individuals may not be well positioned to understand what it is they are consenting to.¹⁷⁹ It is also possible that requiring they consent to complex data management process may over-burden them.¹⁸⁰ These are valid concerns. That said, FIPA proposes that the clear standard of valid consent which exists in the private sector be adopted into the public sector legislation. Including this standard in the *Privacy Act* supports several of the recommendations FIPA has made about withdrawal of consent from ADS or data sharing. This may manifest as a statutory definition but may also appear in the *Act* as a freestanding section which sets a clear standard for valid consent. Advancing technology demands mechanisms through which individuals are provided more agency over their own information. Enshrining a definition of consent allows for this. The GDPR is clear that the right to withdraw consent is essential to a modern privacy regime.¹⁸¹ This will be further in the following recommendation. Without a definition for valid consent, enforcement is not possible.

The consent principles in Personal Information Protection and Electronic Documents Act (*PIPEDA*), listed in both Schedule 1 Principle 3¹⁸² and under section 6.1 (Valid Consent)¹⁸³ empower individuals to take legal action when their consent is violated. For example, in *Canada (Privacy Commissioner) v. Facebook Inc.*¹⁸⁴, the Privacy

¹⁷⁵ Government of Canada, “Privacy principles and modernized rules for a digital age” (1 September 2021) online: https://justice.canada.ca/eng/csjs-jc/pa-lprp/dp-dd/modern_1.html? [Privacy principles and modernized rules]

¹⁷⁶ *Ibid*

¹⁷⁷ *Ibid*

¹⁷⁸ Privacy principles and modernized rule *supra* note 175

¹⁷⁹ *Ibid*

¹⁸⁰ *Ibid*

¹⁸¹ What is GDPR *supra* note 121

¹⁸² *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, <<https://canlii.ca/t/56gxt>> retrieved on 2026-07-09 at 4.3 Principle 3 [PIPEDA]

¹⁸³ *Ibid* at s. 6.1

¹⁸⁴ *Canada (Privacy Commissioner) v. Facebook, Inc.*, 2024 FCA 140 (CanLII), <<https://canlii.ca/t/k6pn1>>, retrieved on 2026-06-26

Commissioner was found to be empowered by the consent provisions of PIPEDA to protect Facebook users whose data had been disclosed to third parties without their consent. This is a fundamental protection that should be enforced in the public sector as well as the private sector.

FIPA recommends the implementation of a clear statutory standard of valid consent akin to that included in PIPEDA:

“for the purposes of clause 4.3 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.”¹⁸⁵

Section 7 in PIPEDA clarifies under what circumstances information may be used, disclosed or collected without obtaining consent from the affected individual.¹⁸⁶ This dimension will be essential to a standard of valid consent in the *Privacy Act*. Moreover, FIPA recommends that the Treasury Board include within the explicit standard of consent a requirement that an organization consider the reasonable expectation of the individual in relation to what they are consenting to. These recommendations are in line with the existing PIPEDA principles of consent.¹⁸⁷

Proposal 15: Harmonize the request regime by incorporating requests for personal data into the *Access to Information Act*

A concern brought to light by Teresa Scassa that FIPA would like to highlight here concerns the right of correction: how will the right of correction be impacted if access to information gathered under the *Privacy Act* is regulated by the Information Commissioner of Canada (ICC) under the *Access to Information Act* (ATIA)?¹⁸⁸ This is particularly relevant given the proposals around AI, ADS and data-sharing. Existing in these regimes are rights of correction, rights to human review and more. These rights inherently require access to be properly executed. There is a potential for conflict and unnecessary complication if access to information gathered under the *Privacy Act* is regulated separately from rights of correction and rights to request human review, which would remain regulated under the *Privacy Act*. Scassa recommends that, rather than

¹⁸⁵ PIPEDA *supra* note 182 at s. 6.1

¹⁸⁶ *Ibid* at s. 7

¹⁸⁷ *Ibid* at Principle 4.3.5

¹⁸⁸ Teresa Scassa, “Access and Correction in Proposed Privacy Act Reforms” (28 May 2026) online: <<https://teresascassa.substack.com/p/access-and-correction-in-proposed>>

shifting access powers to the ICC, the Privacy Commissioner's enforcement powers and ability to manage complaints be bolstered.¹⁸⁹ FIPA agrees.

Theme 5: Indigenous Peoples' access to, and protection of, their data

FIPA encourages TBS to consult with rights holding collectives to ensure the government is meeting its obligations under UNDRIP, the constitution (specifically s. 35 of the *Constitution Act, 1982*), and the laws of First Nations. A rights holding collective is a term which can address First Nations, band councils, families, communities and any other group with the collective right to assert governance. FIPA is not an Indigenous organization and is not intending to speak on behalf of Indigenous Peoples, but we take this as an opportunity to highlight the importance of meaningful consultation. FIPA encourages TBS to consider the rights protected by UNDRIP, including "the right to self-determination, the right to be recognized as distinct peoples, the right to be consulted and provide free, prior and informed consent on legislation before adoption, and the right to participate in decision-making matters which would affect their rights."¹⁹⁰

FIPA supports the submission made by the First Nations Information Governance Council (FNIGC) and would like to amplify the message that Indigenous peoples' collective rights, as defined in UNDRIP, are not reflected in the current privacy legislation. Specifically, this would involve meeting the obligation defined under UNDRIP as: ¹⁹¹Recognizing and reaffirming that indigenous individuals are entitled without discrimination to all human rights recognized in international law, and that indigenous peoples possess collective rights which are indispensable for their existence, well-being and integral development as peoples."² Meaningful consultation requires the proper acknowledgement of these collective rights and asserting them requires the government to be in conversation with rights holding collectives (given that collective rights will be asserted differently across these rights holding collectives).

Differing assertions of privacy rights by rights holding collectives is closely correlated with the "grandmother perspective," a framework through which data governance is

¹⁸⁹ *Ibid*

¹⁹⁰ Office of the Privacy Commissioner, "Issue Sheets on the examination of the federal government's constitutional, treaty, political and legal responsibilities to First Nations, Inuit and Métis peoples and any other subject concerning Indigenous Peoples" (27 February 2024) online: <https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/appa_20240227/is_20240227/> at Background

¹⁹¹ United Nations Declaration on the Rights of Indigenous Peoples Act, SC 2021, c 14, <<https://canlii.ca/t/56fdv>> retrieved on 2026-07-07 at Annex.

viewed. It centers the idea that “we need to know because we care.”¹⁹² Meaningful consultation incorporates these perspectives, as opposed to organizing data governance systems from a purely Western view. In alignment with the grandmother perspective is the idea of creating a process for data management that is rooted in “respectful relationship.”¹⁹³ Within the scope of “respectful relationship” is the meaningful involvement of marginalized communities in the “collection, storage, use and distribution of disaggregated data.”¹⁹⁴

We encourage TBS to consider the FNIGC’s principles of OCAP® (Ownership, Control, Access, Possession) and their relationship to Indigenous data sovereignty, which has a direct impact on self-determination.¹⁹⁵ FIPA urges TBS to recall that only the rights holding collective can determine how principles of data governance and data sovereignty are implemented. OCAP® cannot be universally applied but must instead be applied in discussion with depending on how they define and implement the principles.

FIPA emphasizes that none of the above should be misconstrued to limit the expression of self-governance rights, data sovereignty rights, or any other rights. FIPA implores TBS to recall the statement of the Joint Advisory Committee on Fiscal Relations that bringing Canadian law into alignment with Indigenous data sovereignty and the principles of OCAP® will require changes to legislation.¹⁹⁶ Indigenous perspectives are foundational to the proper, equitable, and just implementation of these principles in privacy law.

Proposal 16: Broadening terms used to refer to “aboriginal government,” “Indian band,” and lists of individual Indigenous governments

FIPA would like to support the submission made by the First Nations Information Governance Center (FNIGC) and echo their point that, rather than set terms proposed in Proposal 16, “rights holding collective” better encompasses the range of groups which may express self-governing rights. For example, the language of

¹⁹² British Columbia’s Office of the Human Rights Commissioner, “Disaggregated demographic data collection in British Columbia: The grandmother perspective” (September 2020) online: < https://bchumanrights.ca/wp-content/uploads/BCOHRC_Sept2020_Disaggregated-Data-Report-FINAL.pdf page 8.> at p. 8

¹⁹³ *Ibid* at p. 9

¹⁹⁴ *Ibid* at p. 9

¹⁹⁵ First Nations Information Governance Center, “The First Nations Principles of OCAP®” online: < <https://fnigc.ca/ocap-training/>>

¹⁹⁶ Joint Advisory Committee on Fiscal Relations, Honouring our Ancestors by Trailblazing a Path to the Future Interim Report of the Joint Advisory Committee on Fiscal Relations - for Engagement Purposes” (2019) at page vii

“rights holding collective” addresses the fact that the principles of OCAP® are applied differently within different communities or groups and cannot always be aptly categorized under “First Nations governments, bands, or aboriginal government.” There is no umbrella system of First Nations data governance, and the language in the *Privacy Act* should reflect that.

Proposal 17: Define Indigenous personal data as subject to distinct governance considerations

No additional commentary.

Proposal 18: Create a mechanism to enable Indigenous governments to access Indigenous personal data of their citizens who have opted to share it in key programs

No additional commentary.

Theme 6: Updating the compliance framework

Proposal 19: Grant the Commissioner binding order-making powers for corrective action plan enforcement and provide them with the discretion to discontinue or decline complaints

As noted in the 2016 House of Commons Review, the Information Commissioner was granted binding order-making powers.¹⁹⁷ That the Privacy Commissioner’s powers match those of the Information Commissioner’s in this capacity was supported by numerous authorities, including the House of Commons Committee itself.¹⁹⁸ Increasing the Privacy Commissioner’s enforcement powers serves to encourage compliance. Thus, FIPA is supportive of this proposal.

Proposal 20: Authorize the Commissioner to collaborate and share information with other jurisdictions

FIPA would like to echo its concerns from the above proposals about issues of information sharing without the consent of the affected individuals. As emphasized in leading privacy legislation like the GDPR, consent is a pillar of modern privacy.¹⁹⁹ Moreover, the data sharing proposed here lacks detailed safeguards. FIPA expresses concern for the lack of limitations suggested under this proposal. Such limits should be considered alongside the missing consent requirements. Lastly, FIPA emphasizes a

¹⁹⁷ House of Commons *supra* note 116

¹⁹⁸ *Ibid*

¹⁹⁹ What is GDPR *supra* note 121

point made by the Canadian Union of Public Employee (CUPE) that highlights the risk to employees when they do not have access to information about where their data is being stored. CUPE illuminates that this may lead to employees' information being used in unforeseeable ways. FIPA urges TBS to consider this in depth, and to detail specific safeguards that will be put in place if/when this data sharing takes place.

Proposal 21: Offences for attempts to re-identify data, except under specific, limited circumstances

This proposal enhances protections around individuals' personal data and strengthens enforcement mechanisms which will serve to deter bad actors from abusing said data. FIPA is supportive of these added safeguards.

Proposal 22: Expand judicial remedies and clarify Federal Court authority

This proposal reflects recommendations made in the 2016 House of Commons Review of the *Privacy Act* and was supported by numerous participants, including the CBA.²⁰⁰ FIPA supports this proposal and encourages its adoption.

Proposal 23: Introduce requirement for five-year review of the *Privacy Act*

This proposal aligns with prior OPC recommendations for amendments to the *Privacy Act*²⁰¹ and would support a modernization of the *Act* that is ongoing and consistent with fast-evolving technology.

²⁰⁰ House of Commons *supra* note 121

²⁰¹ Privacy Commissioner of Canada, *Privacy Act Reform Recommendations*, online: <https://www.priv.gc.ca/media/1316/parl_090511_02_e.pdf?>

Appendix 2 Treasury Board Submission

Organization: BC Freedom of Information and Privacy Association

Recommendations for the 2026 Review of the Privacy Act

Synopsis

The focus of this submission is the identification of gaps in privacy protection that are vital to address as technology advances. A modernized *Privacy Act* considers the ways in which technology can be ingrained in the privacy regime while carefully ensuring it is done transparently and with adequate safeguards to protect people and their personal information. This submission emphasizes the protection of personal information and sensitive data in the face of artificial intelligence (AI) technologies, automated decision-making systems (ADS), data sharing between government bodies without consent of the affected individuals, and the expanding definition of ‘sensitive data’ in the evolving age of information. Consent is vital to upholding individual rights and is a consistent through-line in this submission.

Authorities Sought from the Treasury Board

FIPA recommends the following for the consideration of the Treasury Board in the Review of the *Privacy Act*:

- 1) Consideration of proportionality as a step of the necessity test for data collection.
- 2) Create a legal obligation to apply the necessity and proportionality test to AI and ADS.
- 3) Data sharing between government bodies should be subject to the necessity test and should be governed by written agreements that are posted publicly.
- 4) Create legal requirements for the elements of Personal Impact Assessments (PIA).
- 5) Make breach notifications under the *Privacy Act* mandatory and based on the application of an “unlikely to result in risk” threshold.
- 6) Engage in meaningful consultation with Indigenous Peoples.
- 7) Include predictions about individuals within the scope of ‘sensitive data.’
- 8) Valid consent should be defined in the *Privacy Act*.
- 9) Individuals must be allowed to withdraw consent from personal data sharing between government bodies.
- 10) Re: AI decision-making, governments should limit exposure of personal information to AI systems; individuals should be given the opportunity to withdraw consent from AI decision-making and processing of their personal information.

- 11) Transparency rights for public sector workers regarding employee monitoring. should be enhanced
- 12) Application of the *Privacy Act* could extend to Parliamentary offices and the offices of MPs.

Context

This submission is focused largely on important safeguards for individual privacy and data as technology progresses, and what this may look like in a modernized *Privacy Act*. It references suggestions from the 2016 House of Commons Committee for review of the *Privacy Act*²⁰² which were not taken up in the 28 proposals put forth by the Treasury Board (TBS), as well as research and suggestions from experts in the field.

Strengthen consent requirements

Several definitions have been recommended in Proposal 14 for inclusion in the *Privacy Act*. However, this list is lacking an important term: Valid consent. As a fundamental pillar of privacy rights, it is critical that consent be defined within the *Privacy Act*. Furthermore, consent requirements should be enforced in various areas of the *Act*.

Proposals 5 & 6 suggest the use of AI and ADS for the processing and management of personal data. There are numerous privacy concerns related to third-party AI systems, concerns which vast numbers of Canadians share. It is critical that Canadians have the opportunity to withdraw consent from the input of their information into a third-party AI or ADS. Furthermore, in reference to data-sharing between government bodies, it is critical that the possibility to withdraw consent apply as well.

The scope and application of the necessity test should be expanded

The necessity test in Proposal 10 contains several important elements, but neglects proportionality. For clarity, the necessity test refers to the test as a whole, but necessity is also an individual element of the whole test. Proportionality is a consideration that has been recommended widely, specifically by the House of Commons in their 2016 Review of the *Privacy Act*,²⁰³ and by other experts in the field. It entails a consideration of whether “the loss of privacy is proportional to the importance of the objectives of the program or activity.”²⁰⁴ This is a critical consideration because it focuses specifically on the loss of individual privacy in

²⁰² House of Commons *supra* note 2

²⁰³ *Ibid*

²⁰⁴ Daniel Therrien *supra* note 3

relation to the purpose of the activity—rather than the importance of the purpose alone.

In terms of application, the necessity test, with the inclusion of proportionality as a step, should be applied beyond the collection of data. Additionally, it should be applied both to the use of artificial intelligence (AI) or automated decision-making systems (ADS) and to the sharing of data between government bodies without the consent of the individual's affected, as suggested in Proposal 1.

Enhancement of legal requirements and transparency within safeguard mechanisms

Several proposals have recommended elevating to law certain policy requirements that strengthen privacy security for personal data. These include legally requiring privacy impact assessments and breach notification and strengthening the legal regime around sensitive data. FIPA applauds and encourages these endeavors and recommends adjustments that strengthen the protection provided by each change.

Included in such recommended adjustments is enshrining requirements for the contents of privacy impact assessments within the law itself (thus ensuring they move beyond a bureaucratic checkbox and into a substantial safeguard to effectively protect personal information). Delineating explicit requirements within a PIA sets a standard for the level of due diligence required and ensures important considerations—such as developing mitigation strategies for perceived risks—are not neglected. In this vein, FIPA also recommends that data sharing between government bodies be governed by written agreements. Recognizing that not all data is sensitive, FIPA recommends a minimum floor of legal requirements as well as an expansive list of best practices that should be considered and applied in proportion to the sensitivity of the data for each of the above suggestions. Furthermore, FIPA suggests a lower threshold for breach notification—an important recommendation which highlights the retrospective nature of the current harm mitigation mechanisms. Lastly, FIPA suggests an expansion of the definition of sensitive data to ensure it evolves with rapidly changing technological capabilities.

Expand the scope of the *Privacy Act* to cover gaps in the field

The *Privacy Act* has yet to reach certain areas of Canadian society. FIPA would like to take this opportunity to highlight these gaps and recommend that legislation be implemented to address them.

The first is employee monitoring, an area of increasing concern with the development of AI. There is a growing conflict between a worker's right to privacy in

the performance of job functions and an employer's right to oversee their employees' work and effectively run their business. FIPA recommends implementing a legal standard which enhances transparency around what is and is not permitted, specifically in reference to monitoring. Second is the lack of any statutory regulation of political parties' privacy management and the extension of this lack of regulation into Parliament and caucus. Currently in Canada neither political parties nor members of Parliament are subject to any privacy legislation. Rather, they abide by internal privacy policies which lack enforcement or meaningful remedy. The dangers of this lack of regulation for voter privacy were exemplified by the recent voter-list breach in Alberta, which was highlighted in the recent Senate report and identified in national polling. This issue deserves attention in any discussions about federal privacy law in Canada.

Design, Delivery and Implementation

FIPA currently does not have a plan for how the elements of this proposal will be implemented but asks that they be considered alongside the proposals for modernizing the *Privacy Act*.

Cost, Source of Funds and Strategic Considerations

As an organization external to the government, FIPA does not have the information required to estimate the implementation costs for these proposals.

Results

There are several ways the results of these recommendations may be tracked and accounted for. The first is a significant increase in public trust. It is well documented that the public trust in relation to the use of AI and ADS by government bodies is low. As such, improvement would be demonstrated by an increase in public trust in the government's discretion and transparency in using these systems.

The other ways in which government bodies might note the successful implementation of these recommendations is through a noted reduction in the over-collection of data, and a decrease of individual complaints related to lack of transparency around data sharing, AI/ADS and other related recommendations.

Risks

FIPA does not currently estimate any risks associated with the implementation of the proposals in this submission.

Appendix 3 Cited Sources

Legislation

- Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR c A-2.1, <<https://canlii.ca/t/56lg1>> retrieved on 2026-07-08
- Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, <<https://canlii.ca/t/56cq3>> retrieved on 2026-06-26
- EU, *Regulation 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)*, [2016] OJ L 119/1.
- Personal Information Protection Act*, SA 2003, c P-6.5, <<https://canlii.ca/t/56kzz>> retrieved on 2026-06-26
- Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, <<https://canlii.ca/t/56gxt>> retrieved on 2026-06-26
- United Nations Declaration on the Rights of Indigenous Peoples Act*, SC 2021, c 14, <<https://canlii.ca/t/56fdv>> retrieved on 2026-07-07 at annex.

Jurisprudence

- Canada (Privacy Commissioner) v. Facebook, Inc.*, 2024 FCA 140 (CanLII), <<https://canlii.ca/t/k6pn1>>, retrieved on 2026-06-26
- R. v. Oakes*, [1986] 1 S.C.R. 103

Secondary Materials:

Electronic Sources

- Australian Institute of Statistics, “Understanding re-identification” (8 November 2021) online: <<https://www.abs.gov.au/statistics/understanding-statistics/data-confidentiality-guide/understanding-re-identification>>
- British Columbia’s Office of the Human Rights Commissioner, “Disaggregated demographic data collection in British Columbia: The grandmother perspective” (September 2020) online: <https://bchumanrights.ca/wp-content/uploads/BCOHRC_Sept2020_Disaggregated-Data-Report-FINAL.pdf>
- Daniel Therrien, “Letter to the Standing Committee on Access to Information, Privacy and Ethics” (22 March 2016) online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/>
- DPO Center, “What is a DPA and why do you need one?” (18 March 2024) online: <<https://www.dpo-centre.com/blog/what-is-a-dpa-and-why-do-you-need-one/>>

Fasken, “De-identification of Personal Information Under the Proposed Consumer Privacy Protection Act” (1 March 2021) online:
<https://www.fasken.com/en/knowledge/2021/03/1-de-identification-of-personal-information-under-the-proposed-consumer-privacy-protection-act>

First Nations Information Governance Center, “The First Nations Principles of OCAP®” online: <https://fnigc.ca/ocap-training/>

GDPR, “What is GDPR, the EU’s new data protection law?” online:
<https://gdpr.eu/what-is-gdpr/>

GLAAD, “Understanding LGBTQ Impacts Across AI” online: <https://glaad.org/2026-ai-report-build-for-everyone/lgbtq-impacts/>

Government of Canada, *Privacy Act Material Breach Report Form*, (March 2024), online: <https://www.canada.ca/content/dam/tbs-sct/documents/forms/350-64e-eng.pdf>

Government of Canada, “Privacy principles and modernized rules for a digital age” (1 September 2021) online: https://justice.canada.ca/eng/csj-sjc/pa-lprp/dp-dd/modern_1.html?>

Imran Ahmad & Katherine Barbacki, “Cybersecurity Fundamentals” (2026) Norton Rose Fulbright.

Information Commissioner’s Office, “Data sharing agreements” (17 October 2022) online: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-agreements/#include>

Institut national de la recherche scientifique, “David Myles: The Paradox of Digital Platforms for LGBTQ+ Communities LGBTQ” (10 June 2025) online:
<https://inrs.ca/en/news/david-myles-the-paradox-of-digital-platforms-for-lgbtq-communities-lgbtq/>

Jack Farrell and Lisa Johnson, “Scope of access to leaked Alberta voter list may be incomplete: Elections Alberta,” *The Canadian Press* (13 May 2026), online:
https://www.thecanadianpressnews.ca/prairies_bc/alberta/scope-of-access-to-leaked-alberta-voter-list-may-be-incomplete-elections-alberta/article_7a819434-87ce-5d63-abf0-f82e50814478.html

John Laidler, “High tech is watching you” (4 March 2019) online:
<https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/>

Joint investigation into location tracking by the Tim Hortons App, 2022 CanLII 50894 (PCC), <https://canlii.ca/t/jprwv>, retrieved on 2026-07-09

“Let’s Talk about Bias: LGBTQ+ People and AI” (28 June 2022) online:
<https://www.correlation-one.com/blog/lgbtq-people-ai-algorithmic-bias-harm>

Loso Judijanto, “Unmasking Racial Disparities: Epistemic Injustice and Bias in Facial Recognition Systems” (*Indonesia: Scientia*, 2025) 2:12,
[https://doi.org/10.59324/stss.2025.2\(12\).01](https://doi.org/10.59324/stss.2025.2(12).01)

Office of the Privacy Commissioner of Canada, “Principles for responsible, trustworthy and privacy-protective generative AI technologies” (7 December 2023) online:
https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_a_i/#fn4

Office of the Privacy Commissioner, “Protecting the privacy rights of young people” (28 November 2023), online: <https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20231128/>

Office of the Privacy Commissioner, “Issue Sheets on the examination of the federal government’s constitutional, treaty, political and legal responsibilities to First Nations, Inuit and Métis peoples and any other subject concerning Indigenous Peoples” (27 February 2024) online: <https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/appa_20240227/is_20240227/?wbdisable=true>

Office of the Privacy Commissioner, “Privacy in the Workplace” (29 May 2025) online: <https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17/?wbdisable=true>

Office of the Privacy Commissioner, “Protecting Employee Privacy in the Modern Workplace” 4-5 October 2023) online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_02/>

Privacy Commissioner of Canada, *Privacy Act Reform Recommendations*, online: <https://www.priv.gc.ca/media/1316/parl_090511_02_e.pdf?>

Practical Guidance Lawyer Team, “Artificial Intelligence Risk Management” (16 December 2025) online: <<https://plus.lexis.com/api/permalink/a81934bf-8aeb-49f5-8385-7d0b82db9e18/?context=1537339>>

Public Service Alliance of Canada, “PSAC pushes back on federal AI strategy” (12 June 2026) online: <<https://psacunion.ca/psac-pushes-back-federal-ai-strategy>>

Rishabh Poddar, “Why Data Anonymization Isn’t Enough in the Age of AI” (24 April 2024) online: <<https://www.opaque.co/resources/articles/why-data-anonymization-isnt-enough-in-the-age-of-ai>>

Stanford University, “Privacy in an AI Era: How Do We Protect Our Personal Information?” (18 March 2024) online: <<https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information>>

Teresa Scassa, “Access and Correction in Proposed Privacy Act Reforms” (28 May 2026) online: <<https://teresascassa.substack.com/p/access-and-correction-in-proposed>>

Teresa Scassa, “Privacy Act Reform: Enhancing accountability and transparency” (20 April 2026) online: <<https://teresascassa.substack.com/p/privacy-act-reform-enhancing-accountability-963>>

Teresa Scassa, “Pragmatic Privacy: Reform of the Federal Privacy Act” (13 April 2026) online: <<https://teresascassa.substack.com/p/pragmatic-privacy-reform-of-the-federal>>

Teresa Scassa, “Privacy Act reform must get key definitions right” (4 May 2026) online: <<https://teresascassa.substack.com/p/privacy-act-reform-must-get-key-definitions>>

The Guardian, “Amazon ditched AI recruiting tool that favored men for technical jobs” (11 October 2018) online: <<https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine>>

Treasury Board of Canada Secretariat, “2026 Review of the Privacy Act: Policy Approaches” (2 April 2026) online: < <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/privacy-act-modernization-policy-approaches/2026-review-privacy-act-policy-approaches.html>>

Towards a Public Law of Privacy: Meeting the Big Data Challenge, (2015), 71 SCLR (2d) 541 - 561

Submissions

BC Freedom of Information and Privacy Association, *Submission to the Standing Committee on Procedure and House Affairs*, May 2026, online: < <https://fipa.bc.ca/wp-content/uploads/2026/05/20260501-FIPA-Bil-C-25-PROC-Submission-FINAL-V2.pdf>>

Articles, Books and Publications

Anna Su, “Gender Equality, AI and the Future of Human Rights” (2025) University of Toronto Law Journal.

Bradley Henderson, Maintaining Legitimacy: Artificial Intelligence, Automated Decision Making, and Reasonableness Review under Canadian Administrative Law, (2025) 58:2 UBC L Rev 415 – 474

Jiaheng Wei et al, “Memorization in Deep Learning: A survey” (2020) 18:9 Journal of Latex Class Files.

Johnathan Yerby, “Legal and ethical issues of employee monitoring” (2013) 1:2 Online Journal of Applied Knowledge Management 44.

Kate Goddard, Abdul Roudsari & Jeremy C Wyatt, “Automation bias: a systematic review of frequency, effect mediators, and mitigators” (2011) 19:1 Journal of the American Medical Informatics Association 121. doi: 10.1136/amiajnl-2011-000089

Natasha MacParland et al, “Artificial Intelligence in Canadian Insolvency Practice” (2025).

Shoshana Zuboff, “Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization” (2022) 3: 1–79 Organization Theory. <https://doi.org/10.1177/26317877221129290>.

Soshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

Wendy H. Wong, *We, the Data: Human Rights in the Digital Age* (The MIT Press, 2023).

Reports

Blaine Calkins, *Protecting the Privacy of Canadians: Review of the Privacy Act, Report of the Standing Committee on Access to Information, Privacy and Ethics*, (House of Commons, 2016).

Mohammed (Joe) Masoodi et al, *Monitoring Remote Work in Canada: Support or Surveillance?*, (Future Skills Center, 2023).

Sara Bannerman, "Submission to the Senate Standing Committee on Legal and Constitutional Affairs on Bill C-4, an Act Respecting Certain Affordability Measures for Canadians and Another Measure" (11 December 2025) online: <https://sencanada.ca/Content/Sen/Committee/451/LCJC/briefs/LCJC_SM-C-4_Brief_SaraBannerman_e.pdf>

PIPEDA Findings No 2022-001, [2022] CPCSF No 1, [2022] SCCPVPC no 1 [PIPEDA Findings]

Privacy Commissioner of Canada, *Privacy Act Reform Recommendations*, online: <https://www.priv.gc.ca/media/1316/parl_090511_02_e.pdf>

The Honourable David M. Arnot & The Honourable Denise Batters, *Privacy Issues Regarding Federal Political Parties under the Canada Elections*, Interim report of the Standing Senate Committee on Legal and Constitutional Affairs, (Ottawa, Ontario: Senate Canada, 2026).

Joint Advisory Committee on Fiscal Relations, "Honouring our Ancestors by Trailblazing a Path to the Future Interim Report of the Joint Advisory Committee on Fiscal Relations - for Engagement Purposes" (2019) at page vii.