

— A Justice Centre Report —

— July 22, 2026

Privacy roadmap: Halting Canada's surveillance state

8 steps to restoring
privacy in Canada

Author: Nigel Hannaford



Justice Centre
for Constitutional Freedoms

We Defend
Freedom
in Canada

Abstract

The privacy rights of Canadians, long protected by common law and more recently under *Charter* section 8, are increasingly threatened by federal legislation that expands state access to personal information. Bills C-8, C-22, the *Customs Act*, and other laws have lowered disclosure thresholds, authorized information-sharing between government institutions and law enforcement, and normalized surveillance practices that undermine reasonable expectations of privacy. Bill C-34, now before Parliament, further threatens privacy rights. At the same time, weaknesses in Canada's foundational privacy laws – *PIPEDA* (and its proposed replacement, *PPCDA*) and the *Privacy Act* – leave Canadians vulnerable to unnecessary collection, retention, and disclosure of personal information. Robust legislative reforms are needed to restore meaningful privacy protections.

Copyright and reprinting

Copyright © 2026 Justice Centre for Constitutional Freedoms

Licensed under the Creative Commons [CC BY-NC-ND](#). This license enables reusers to copy and distribute the material in any medium or format in unadapted form only, for noncommercial purposes only, and only so long as attribution is given to the creator.



Acknowledgements

We thank the thousands of Canadians who continue to support the Justice Centre with their donations. Their generosity empowers the Justice Centre to defend freedom in Canada and to shape public policy that respects *Charter* rights and freedoms.

Updates to this report

This is Version 1.1 of this report, which may be updated periodically.

Authorship

This report was written by Nigel Hannaford, a veteran journalist and public policy analyst.

Contents

Introduction.....	5
Safeguarding privacy against state intrusion	5
Federal law undermines privacy protections	6
Bill C-8 – <i>An Act respecting cyber security</i>	6
Bill C-22 – <i>Lawful Access Act</i>	7
<i>The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)</i>	8
<i>The Customs Act</i>	9
Bill C-34 – <i>The Safe Social Media Act</i>	10
Restoring robust privacy protections	11
<i>The Personal Information Protection and Electronic Documents Act (PIPEDA)</i>	12
<i>The Protecting Privacy and Consumer Data Act (PPCDA)</i>	12
<i>The Privacy Act</i>	14
Conclusion	16
Bibliography	18



Executive Summary

Privacy is the foundation of freedom of thought, freedom of expression, personal autonomy, and human dignity. When citizens know (or have strong grounds to believe) that they may be monitored, they behave differently, speak differently, and think differently. Recent privacy-violating federal bills (e.g., C-8, C-22, C-34) demonstrate the urgent need to strengthen Canadian privacy laws. Failing to do so, Canadians risk losing one of the most important elements of a free and democratic society.

In 1984, the Supreme Court of Canada fundamentally reshaped privacy law in *Hunter v. Southam*. Rejecting a property-based approach to privacy, the Court held that section 8 of the *Canadian Charter of Rights and Freedoms* protects individuals wherever they have a reasonable expectation of privacy. Since then, the Court has applied that principle to new technologies, recognizing reasonable expectations of privacy in internet subscriber information, text messages, computers, cell phones, and other electronic communications.

Yet while courts have protected privacy rights, Parliament has increasingly undermined privacy by expanding state access to personal information, and by lowering the standards required to obtain sensitive data.

Having received Royal Assent in June, Bill C-8 is now law and authorizes sweeping government powers over telecommunications systems and permits enforcement officials to access records and systems in the name of national and cyber security. Bill C-22 proposes to lower the threshold for obtaining subscriber information from electronic service providers (definition in footnote¹) from “reasonable grounds to believe” to the weaker standard of “reasonable grounds to suspect” that a crime has or will occur. Bill C-22 also authorizes new warrantless demands for information and requires service providers to retain Canadians’ metadata for up to six months. Bill C-34 opens the door to requiring all Canadians to prove their ages and identities to access social media platforms, leading to increased collection of personal information by social media platforms, AI companies, and perhaps even government institutions.

Some existing older laws create similar risks. The federal anti-money-laundering regime (PCMLTFA²) requires extensive collection and sharing of personal financial information. Under the *Customs Act*, border officials exercise broad authority to search personal electronic devices.

These laws are presented as necessary for “security” or “safety.” Collectively, however, they authorize broader government access to Canadians’ digital lives, enabling government to monitor communications, financial transactions, and online activities. Canadians should

¹ Essentially all electronic and internet companies that provide any kind of services: E.g., phone services (Shaw, Telus), messaging apps (WhatsApp, Signal), emails, Google, Amazon, Apple Pay, Netflix, and others.

² Full name: *The Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

reject the false choice between privacy and security. Effective law enforcement does not require abandoning constitutional safeguards.³

Accordingly, Parliament should:

1. Amend the changes enacted under Bill C-8 to prohibit broad access to subscriber information;
2. Amend the *PCMLFTA* to narrow collection and reporting requirements of personal financial information to law enforcement;
3. Amend the *Customs Act* to exclude search of personal electronic devices at the border;
4. Reject Bill C-22;
5. Reject Bill C-34.

Most importantly, Canada's foundational privacy laws must be strengthened. Parliament should amend those as follows:

6. The *Personal Information Protection and Electronic Documents Act (PIPEDA)* – the law governing private-sector data practices – should require meaningful consent, strengthen data deletion requirements, and prohibit corporations from voluntarily disclosing Canadians' data to government institutions, except in genuine emergencies or with judicial authorization.
7. The recently introduced *Protecting Privacy and Consumer Data Act (PPCDA)* – which essentially replaces *PIPEDA* (see footnote 25, page 11) – includes important improvements, including recognizing privacy as a fundamental right. However, serious weaknesses remain. Most notably, *PPCDA* transfers oversight of how companies handle Canadians' data from the independent Privacy Commissioner, to a new cabinet-appointed commission and leaves many key privacy standards to future regulations. These weaknesses should be eliminated from the Bill.
8. The *Privacy Act* – the law regulating government data practices – also needs improvements. It should require stronger safeguards for information-sharing between government agencies, narrow government data collection to what is strictly necessary, strengthen deletion rules, require notification when personal information is disclosed, and mandate stronger Privacy Impact Assessments. Both, *PIPEDA* (or its proposed replacement, *PPCDA*) and the *Privacy Act*, should also include a clause that states where federal statutes conflict, the law providing greater protection for personal privacy will prevail.

Collectively, these reforms would help restore privacy protections under the *Charter* that allow Canadians to live freely, speak openly, and participate in democracy without fear of government surveillance.

³ Over the course of centuries, our common law developed a healthy balance that protected privacy and private property rights while also allowing police to obtain warrants from courts to enable law enforcement.

Introduction

This report explores how Canadian courts have protected privacy, examines new and previously existing legislation that threatens our privacy rights, and proposes necessary amendments. This report then analyses and recommends meaningful amendments to Canada's foundational privacy statutes – *PIPEDA*, the recently introduced *Protecting Privacy and Consumer Data Act (PPCDA)*, and the *Privacy Act*.

Safeguarding privacy against state intrusion

Section 8 of the *Canadian Charter of Rights and Freedoms* protects Canadians' "right to be secure against unreasonable search or seizure."⁴ This aligns with our common law heritage which, over time, established the property rights of citizens and their right to be free from state surveillance. Since 1982, Canadian courts have interpreted this section to include the protection of personal informational privacy.

In *Hunter v. Southam Inc* (1984)⁵, federal government investigators,⁶ authorized by the *Restrictive Trade Practices Commission*, had searched the Edmonton offices of Southam Newspapers, seizing documents related to an anti-competitive practices probe. Southam argued that the *Combines Investigation Act* authorized unreasonable search and seizure, and was therefore contrary to section 8 of the *Charter*. The Supreme Court agreed, holding that *Charter* section 8 protects against unjustified state intrusions upon a "reasonable expectation of privacy" wherever it exists – including in personal data, devices, and in communications. Further, the Court found that their reasonable expectation of privacy was not limited to personal information held at their own premises, thereby expanding privacy rights as existing beyond only private property rights.⁷

In *R v. Duarte* (1990), the Court held that, "Surreptitious [ie., secret] electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under s.8 of the *Charter*."⁸ Importantly, the Court added that, "The regulation of electronic surveillance is not directed at protecting a person from the risk that someone will repeat his words but from the much more insidious danger inherent in allowing the state, in its

⁴ Government of Canada. "The Canadian Charter of Rights and Freedoms." Justice Centre for Constitutional Freedoms. <https://www.jccf.ca/the-canadian-charter-of-rights-and-freedoms/>

⁵ *Hunter et al. v. Southam Inc.*, [1984] 2 SCR 145, 1984 CanLII 33 (SCC). <https://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html>. Retrieved on 2026-06-18.

⁶ The investigation was under the *Combines Investigation Act*.

⁷ Prior to this *Hunter v. Southam Inc.* decision, legal protections against searches were often rooted in property rights. Until then, privacy was considered better protected in a home or owned premises but protected to a lesser extent elsewhere. The Supreme Court of Canada rejected this narrow, location-based understanding of privacy rights.

⁸ *R. v. Duarte*, 1990 CanLII 150 (SCC), [1990] 1 SCR 30, <https://canlii.ca/t/1fszz>. Retrieved on 2026-06-18.

unfettered discretion, to record and transmit his words.”⁹ Most importantly, the Court cautioned that the state cannot circumvent constitutional privacy protections by relying on intermediaries to obtain information it could not lawfully access directly.¹⁰

In *R. v. Spencer* (2014), the Supreme Court ruled that police could not access subscriber information held by internet service providers (ISPs) without a warrant – even if the ISP provided it voluntarily upon request. That is, police requests for the voluntary disclosure of information it could not otherwise obtain without a warrant were found to violate the *Charter*’s protection against unreasonable search and seizure.¹¹

In *R. v. Marakah* (2017), the Court considered whether the sender of a text message retained a privacy right when the message was held on another person’s device. The Court decided that the sender of text messages retains a reasonable expectation of privacy in those messages, even after they are received and stored on a recipient’s device. Police therefore require a warrant to search recipients’ phones for senders’ texts. This marked a significant expansion of personal digital privacy rights.

Despite such clear and consistent direction from the Supreme Court of Canada, the federal government is increasingly seeking to authorize government bodies and enforcement agencies to collect, use, and share Canadians’ personal information in ways that are inconsistent with these established *Charter* section 8 principles.

Federal law undermines privacy protections

Bill C-8 – *An Act respecting cyber security*

Bill C-8, *An Act respecting cybersecurity*, became law on June 15, 2026 (full title in footnote).¹² It amended the *Telecommunications Act* (TA) and enacted the *Critical Cyber Systems Protection Act* (CCSPA).

The TA amendments grant the federal government sweeping powers to require telecommunications service providers (e.g., Rogers, Telus, Bell, Videotron) “to do a

⁹ Ibid.

¹⁰ Ibid.

¹¹ In this case, the [police request to link a given IP address to subscriber information was in effect a request to link a specific person to specific online activities](#). This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized in other circumstances as engaging significant privacy interests.

¹² Parliament of Canada. House of Commons. “Bill C-8: An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts.” 45th Parliament, 1st Session, 2025. <https://www.parl.ca/LegisInfo/en/bill/45-1/c-8>.

specified thing” to secure their systems against threats. This can include withdrawing services to a “specified person” and providing “any information” necessary to do so.

The CCSPA authorizes officials to enter premises, examine cyber systems, and remove records without needing to obtain a warrant from a court. Police can act based only on having “reasonable grounds to suspect” that a crime has occurred – as opposed to the higher standard of “reasonable grounds to believe” that a crime has occurred. These new powers violate the principles articulated by the Supreme Court in *Hunter v. Southam*: searches should generally be authorized in advance by an independent judicial officer.

While acknowledging that Bill C-8 has just become law, the Justice Centre urges Parliament to amend the TA and the CCSPA to:

1. Explicitly exclude subscriber data from the broadly defined government powers to order a telecommunications service provider “to do a specified thing,” including providing subscriber information to the government.
2. Restore “reasonable grounds to believe” as the standard for police to obtain warrants to enter premises and remove records without judicial pre-authorization.

Bill C-22 – Lawful Access Act

Bill C-22,¹³ the *Lawful Access Act*, passed third reading in the House of Commons on June 18, 2026, despite widespread opposition from privacy experts, tech companies, and civil liberties organizations. This Bill will expand law enforcement access to electronic data held by internet and electronic service providers.

Bill C-22 will amend the *Criminal Code* to effectively expand police access to information held by internet service providers in several ways.¹⁴ Clause 5 of Part 1 of the *Lawful Access Act* will lower the legal threshold for police to obtain warrants to demand subscriber information if they have “reasonable grounds to suspect” that a crime has been or will be committed – a lower standard than “reasonable grounds to believe.”

Part 2 enacts the *Supporting Authorized Access to Information Act*, new legislation that empowers the government to order electronic service providers to:

- develop and implement operational and technical capabilities for extracting and organizing Canadians’ data;
- install and maintain devices enabling the government to access Canadians’ data; and
- retain Canadians’ metadata for up to six months.

¹³ Parliament of Canada. House of Commons. “Bill C-22: An Act Respecting Lawful Access (Lawful Access Act, 2026).” 45th Parliament, 1st Session, 2026. <https://www.parl.ca/legisinfo/en/bill/45-1/c-22>.

¹⁴ Parliament of Canada. House of Commons. “Bill C-22: An Act Respecting Lawful Access (Lawful Access Act, 2026).” 45th Parliament, 1st Session. As passed by the House of Commons, June 18, 2026. <https://www.parl.ca/documentviewer/en/45-1/bill/C-22/third-reading>.

While metadata, or “data about data,” does not reveal the contents of communication, it does reveal the context of communication: with whom a person communicated, for how long, when, from where, and more. With this information, police can construct and infer much about a person’s life and identity, including their contacts, affiliations, behaviours, habits, and beliefs, even if police have no authority to read our texts and emails. Of particular concern, neither Bill C-22 nor the *Criminal Code* provide a clear definition of “metadata,” leaving the scope of what governments may order companies to retain subject to future interpretation and susceptible to abuse.

Furthermore, clauses 14 and 15 of Part 2 prohibit electronic service providers from disclosing government orders to the public or to affected customers, unless the government authorizes them to do so.

Bill C-22 will force companies to store more data than ever before in preparation for government or law enforcement access, generating significant security risks as a result. The government will be authorized to issue orders to electronic service providers in secret. And, because this legislation can apply to any electronic service provider (including phone, social media, and other online services) in Canada, it will effectively frustrate Canadians’ ability to choose to do business with companies that do not store sensitive data at all (such as Signal) or for short periods of time only.¹⁵

Accordingly, the Senate should defeat Bill C-22 in its entirety.

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)

The *PCMLTFA* is Canada's primary federal legislation for combatting money laundering and terrorist financing.¹⁶ Through the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC),¹⁷ this legislation serves important public safety goals while also creating significant privacy risks. The *PCMLTFA* requires private financial entities to collect, store, and share detailed financial data with FINTRAC for transactions of \$10,000 or more. This information can then be disclosed by FINTRAC to law enforcement, Canadian Security Intelligence Service, Canada Revenue Agency, and other government entities.

The *PCMLTFA* requires reporting of these financial transactions regardless of whether there are reasonable grounds to suspect money laundering, terrorist financing, child exploitation, or other criminal activities. As a result, millions of transactions conducted by law-abiding Canadians are reported to FINTRAC each year.

¹⁵ Foreign-based electronic service providers (ESPs) have already indicated their intention to withdraw from Canada, if this regulation is enforced. For example, [Signal](#).

¹⁶ The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA, S.C. 2000, c. 17)

¹⁷ Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) was [established in 2000](#).

Testifying before the House of Commons' Standing Committee on Finance in 2018, Privacy Commissioner Daniel Therrien highlighted the fact that the financial transactions of law-abiding Canadians were being disproportionately reported to and stored by FINTRAC. He testified, "According to their latest annual report, FINTRAC reported that out of 24.7 million records received during the last fiscal year there were only 2,015 actionable disclosures, which represents less than 1 in 10,000."¹⁸

During the 2024-2025 reporting period, 2.9 million cash transactions, 61 million electronic funds transfers, and 633,882 suspicious transactions were reported to FINTRAC. During that same period, FINTRAC generated a mere "6,236 financial intelligence disclosure packages in support of investigations of money laundering, terrorist financing, sanctions evasion and threats to the security of Canada."¹⁹

Seven years after Privacy Commissioner Therrien's testimony to the House of Commons, the ratio of FINTRAC disclosures to reports received still remains approximately one disclosure for every 10,000 reports submitted.

Accordingly, Parliament should amend the *PCMLTFA* to:

1. Require judicial authorization before FINTRAC may disclose personal financial information to law enforcement, the Canada Revenue Agency, CSIS, or any other government agency.
2. Grant the Office of the Privacy Commissioner binding enforcement powers over FINTRAC.
3. Require FINTRAC to permanently delete personal information that does not result in an intelligence disclosure or is otherwise unnecessary for an ongoing investigation.
4. Replace the current expansive mandatory reporting (based solely on transaction thresholds) with a different requirement to report only transactions for which there are reasonable grounds to suspect money laundering, terrorist financing, or other criminal activities.

The Customs Act

¹⁸ Office of the Privacy Commissioner of Canada. "Appearance before the House of Commons' Standing Committee on Finance for its statutory review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)." February 28, 2018. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180228/.

¹⁹ Government of Canada. "FINTRAC Annual Report 2024–25." Financial Transactions and Reports Analysis Centre of Canada. <https://fintrac-canafe.canada.ca/publications/ar/2025/ar2025-eng.pdf>

Unlike suitcases or other physical goods, modern smartphones contain years of personal communications, photographs, financial records, location histories, internet browsing activity, health information, relationship details, and access to cloud-based accounts. They provide an extraordinarily detailed picture of an individual's private life, relationships, beliefs, and activities. The privacy interests engaged by a search of a personal electronic device are therefore fundamentally different from those engaged by a search of ordinary imported goods.

Section 99 of the *Customs Act* authorizes border services officers to examine goods entering Canada, including personal electronic devices. Although Parliament has imposed a statutory threshold for searches of personal digital devices, that threshold remains below the standard ordinarily required for criminal investigations. While policing cross-border traffic is a legitimate interest for governments, the current provision goes too far. Phones contain highly personal information, going to the biographical core of their users.

As previously noted, the Supreme Court has found that data privacy is protected wherever it is held, including on electronic devices (*Hunter v. Southam* and *R. v. Marakah*). In *R. v. Canfield* (2020), the Alberta Court of Appeal held that suspicionless border searches of personal electronic devices violated section 8 of the *Charter* because digital devices attract an exceptionally high expectation of privacy.

These rulings confirm that the traditional "border exception" does not justify unrestricted access to the personal information contained on electronic devices.

Accordingly, Parliament should amend the *Customs Act* as follows:

1. Require judicial authorization or another constitutionally adequate, independent authorization before border officials may examine the digital contents of personal electronic devices.
2. For cross-border transportation of goods, narrow the definition of "goods" to exclude personal electronic devices.

Bill C-34 – The Safe Social Media Act

Introduced on June 10, 2026, with the stated goal of protecting children from harm, Bill C-34, the *Safe Social Media Act*,²⁰ will vastly expand the federal government's power over social media platforms and AI companies.

Clause 27(1) will force regulated social media platforms to prevent Canadians under age 16 from accessing social media through age-verification and age-estimation measures. If Bill C-34 passes in its current form, all Canadians will have to verify their age and identity before accessing social media. This opens the door for the federal government to

²⁰ Parliament of Canada. House of Commons. "C-34 - Safe Social Media Act." First Session, Forty-fifth Parliament. First Reading. <https://www.parl.ca/documentviewer/en/45-1/bill/C-34/first-reading>

implement a national digital ID platform that functions as an age-verification gateway to regulated platforms. Or the federal government would require online platforms themselves to analyze users' biometric data (e.g., facial recognition technology) to verify users' ages. Regardless of the means used by the government to try to keep minors off social media platforms, Bill C-34 will see Canadians surrender massive amounts of metadata (or identifying data) to access the platforms they use every day for work, leisure, discovery, and expression.

Social media platforms are not the only target of Bill C-34. Clauses 48 to 58 will effectively regulate what Canadians can say to AI chatbots and what AI chatbots can “say” to Canadians. Faced with vague obligations and fines up to \$10 million or three percent of gross global revenue for non-compliance,²¹ AI companies will be forced to monitor all Canadians' private AI conversations, and will likely report more of those conversations to police.

Finally, Part 2 of Bill C-34 will establish a Digital Safety Commission of three to five full-time members, to be appointed by the federal cabinet, with broad powers to regulate online content. Bill C-34 does not define clearly what powers it gives to the Digital Safety Commission or to the federal cabinet. According to privacy expert and law professor Michael Geist, the federal cabinet and Digital Safety Commission will have the power to determine 50 major questions not addressed in Bill C-34, for example, which social media platforms and AI companies will be affected, and what methods the government will use to keep minors off social media.²² The answers to these questions will have far-reaching implications for Canadians' enjoyment of privacy.

Accordingly, Parliament should reject Bill C-34 in its entirety.²³

Restoring robust privacy protections

Privacy protection in Canada rests primarily on the *Privacy Act* (for government institutions) and *PIPEDA* (for private-sector organizations). Both laws contain significant weaknesses. Strengthening them is essential to restore privacy as the default state in Canada.

²¹ Clause 88 of the Bill

²² Geist, Michael. “The Law to Be Named Later: Bill C-34 Punts 50 Key Decisions to Cabinet and a Digital Safety Commission That Does Not Yet Exist.” Blog. June 11, 2026. <https://www.michaelgeist.ca/2026/06/the-law-to-be-named-later-bill-c-34-punts-50-key-decisions-to-cabinet-and-a-digital-safety-commission-that-does-not-yet-exist/>.

²³ As for the regulation of AI systems, we acknowledge that AI can make mistakes and even cause harm to some users. Parliament could address this in part by requiring AI systems to repeatedly remind users that they are machines, not humans, and to state repeatedly that they are not qualified to give legal, financial, medical, or relationship advice.

The Personal Information Protection and Electronic Documents Act (PIPEDA)

The *Personal Information Protection and Electronic Documents Act (PIPEDA)* governs how **private-sector organizations** collect, use, and disclose Canadians' personal information. It is founded on fair information principles, including accountability, consent, limiting collection, safeguarding personal information, openness, and individual access.

PIPEDA defines "valid consent" as consent that is "only valid if it is reasonable to expect that an individual...would understand the nature, purpose, and consequences of the collection, use, or disclosure of their personal information." However, *PIPEDA* falls short of ensuring meaningful consent in practice. It relies heavily on opt-out mechanisms, allowing organizations to presume consent unless individuals object. Organizations may also satisfy their legal obligations through lengthy, complex privacy policies that few users read or understand, undermining informed decision-making.

PIPEDA also provides insufficient safeguards against the long-term retention of personal information. Clause 4.5.3 of Schedule 1 merely recommends, rather than requires, that organizations destroy or anonymize personal information once it is no longer needed for the purpose for which it was collected.²⁴

Finally, although *PIPEDA* generally requires consent or statutory authority before personal information may be disclosed, broad statutory exceptions can substantially weaken those protections. For example, organizations' compliance with reporting obligations under legislation such as the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* can result in extensive disclosures of personal information to government authorities without the knowledge or consent of the individuals concerned.

The Protecting Privacy and Consumer Data Act (PPCDA)

On June 15, 2026, the federal government introduced Bill C-36, the *Protecting Privacy and Consumer Data Act (PPCDA)*. This Act would **essentially replace PIPEDA** (see footnote²⁵).

²⁴ Government of Canada. "Personal Information Protection and Electronic Documents Act." Act current to 2026-05-26. <https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-7.html#h-417659>.

²⁵ The summary of Bill C-36 states: "This enactment **enacts the Protecting Privacy and Consumer Data Act [PPCDA]** to govern the protection of personal information of individuals while taking into account the need of organizations to collect, use or disclose personal information in the course of commercial activities. Consequently, it **repeals Part 1 of the Personal Information Protection and Electronic Documents Act [(PIPEDA) – Part 1 is the privacy part of PIPEDA]** and **changes the short title of that Act to the Electronic Documents Act**. Finally, it also makes amendments to other Acts." Emphasis added. In other words, the *PPCDA* would replace the privacy part of *PIPEDA*, and rename the rest. So *PIPEDA* itself will no longer exist if Bill C-36 is passed in its current form.

Clause 5 of Part 1 states:

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

The *PPCDA* includes several improvements²⁶ over the 25-year-old *PIPEDA*:

- recognizing privacy as a fundamental right (Part 1, clause 5);
- recognizing that children’s information is sensitive and that children enjoy a heightened expectation of privacy (Part 1, clause 2(1))
- expanding the definition of “personal information” to include information that is inferred about an individual (Part 1, clause 2(1));
- requiring regulated companies to dispose of an individual’s personal information at their request (Part 1, clause 54);

The *PPCDA*, however, leaves several concerns unaddressed. Most notably, it transfers private-sector privacy oversight from the independent Office of the Privacy Commissioner to a new government-appointed Digital Safety and Data Protection Commission.²⁷ This removes the Privacy Commissioner from independent oversight over a federal government that has repeatedly demonstrated a poor track record of upholding Canadians’ right to privacy. This further leaves many significant privacy standards to be defined by a future, cabinet-controlled Commission.

Accordingly, Parliament should:

1. Strengthen retention and deletion requirements. While clauses 52, 53, and 54 of the *PPCDA* improve upon *PIPEDA*’s Schedule 1 by introducing clearer rules regarding the retention and disposal of Canadians’ personal information, clause 54(2) specifies that an organization may refuse an individual’s request to dispose of their personal information if “the disposal of the information would have an undue adverse effect on the organization that outweighs any potential adverse effect on the individual resulting from the retention of the information.”²⁸ This exception

²⁶ Geist, Michael. “One Step Forward, Two Steps Back: Bill C-36 Modernizes Canada’s Privacy Law, Then Delays It to 2030.” Blog. June 18, 2026. <https://www.michaelgeist.ca/2026/06/billc36/>

²⁷ Ibid.

²⁸ Parliament of Canada. House of Commons. “Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts.” 45th Parliament, 1st session. First reading, June 15, 2026. <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading>.

establishes a subjective guideline that undermines Canadians' meaningful control over their personal information.

2. Restrict warrantless disclosures to the government and require notification of disclosures. The *PPCDA* leaves many of *PIPEDA*'s disclosure exceptions (including sections 7(3)(c.1) and 7(3)(d)) largely intact, particularly for law enforcement and national security requests. These should be amended to prohibit voluntary disclosures to government entities based on mere requests or suspicion. Except in genuine emergencies, disclosures to government authorities should require judicial authorization. Organizations should also be required to notify individuals when their personal information has been disclosed (subject to narrow, clearly defined exceptions).
3. Adopt the Privacy Commissioner's "meaningful consent" standard.²⁹ The *PPCDA* largely retains a "valid consent" model for the collection of personal information. Parliament should go further by adopting the Privacy Commissioner's recommendation that the standard for collecting Canadians' information be "meaningful consent," thereby requiring organizations to clearly highlight in plain language what personal information is collected, how it will be used, with whom it will be shared, and what risks the user may be exposed to as a result. Individuals should be given accessible, user-friendly options to control the amount of information shared, and the right to meaningfully opt out of data collection.

The Justice Centre will continue to monitor this legislation over the coming months.

The *Privacy Act*

The *Privacy Act* governs the collection, use, retention, and disclosure of personal information by **federal government authorities**, while granting individuals rights of access and correction of personal information. However, significant weaknesses undermine its effectiveness.

While Bill C-36 proposes significant reforms to the rules governing how private-sector organizations collect and use Canadians' personal information, the federal government has proposed no comparable reforms to the *Privacy Act*.³⁰

Notably, s. 8(2)(e)³¹ permits government institutions to voluntarily disclose personal information to investigative bodies upon written request, for investigation purposes. This

²⁹ Office of the Privacy Commissioner. "Guidelines for obtaining meaningful consent." Date modified: 2025-08-11. https://www.priv.gc.ca/en/privacy-topics/business-privacy/collecting-personal-information/consent/gL_omc_201805/.

³⁰ Government of Canada. "Privacy Act." (R.S.C., 1985, c. P-21). Current to May 26, 2026. <https://laws-lois.justice.gc.ca/eng/acts/p-21/>

³¹ The Privacy Act version is slightly narrower, emphasizing information "recorded in any form."

creates a lower protection threshold than what exists for private-sector data under *PIPEDA*'s consent-based model (and Schedule 1 principles).

Data held by government institutions under the *Privacy Act* can thus more easily flow to investigators than comparable data held by a *private company* under *PIPEDA*. This creates a legal pathway for personal information collected for administrative purposes to be repurposed for law enforcement investigations – a concern frequently raised by privacy advocates and the Privacy Commissioner.³² Court-ordered disclosures under section 8(2)(c) already provide a proper mechanism, rendering the broad exception in section 8(2)(e) unnecessary and dangerous.

As with *PIPEDA*, retention and deletion rules under section 6 are inadequate. While personal information must be retained long enough to allow access requests, there are no meaningful statutory limits on how long unnecessary personal information may continue to be retained. Notification-of-disclosure obligations under section 8(5) are weak and discretionary.

Accordingly, Parliament should:

1. Strengthen privacy protections broadly. Parliament should enact a clear supremacy clause applicable to both *PIPEDA* (or the new *PPCDA*), the *Privacy Act*, and any other federal privacy legislation: “Where a provision of this *Act* conflicts with another federal enactment authorizing the disclosure, collection, retention, or access to personal information, the provision offering the greater protection for personal privacy shall prevail.” This principle would resolve conflicts in favour of privacy, prevent function creep, and reaffirm that privacy is not a secondary consideration but a foundational right essential to dignity, autonomy, and democratic freedom.
2. Repeal section 8(2)(e) to eliminate low-threshold voluntary disclosures, and require stronger safeguards, such as judicial warrants or court orders, for disclosures to investigative bodies.
3. Narrow the scope of data that can be collected by government institutions. Section 4 currently permits government institutions to collect personal information whenever that information “relates directly” to a government program or activity. This standard is too broad and should be replaced with a necessity requirement, allowing collection only where information is demonstrably necessary for a clearly defined statutory purpose.
4. Strengthen retention limits and deletion requirements. Amend sections 6(1) and 6(3) to require mandatory deletion deadlines, automatic deletion of information no

<https://laws-lois.justice.gc.ca/eng/acts/p-21/section-8.html>

³² Office of the Privacy Commissioner of Canada, Submission on Privacy Act Modernization (March 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103/

longer needed, and periodic independent review of retention practices by the Office of the Privacy Commissioner.

5. Mandate notification of disclosure to affected Canadians. Section 8(2)(m) authorizes the disclosure of personal information for any purpose where, in the opinion of the head of a government institution, “the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure” or where the “disclosure would clearly benefit the individual to whom the information relates.”³³ In such cases, the government institution is obligated to notify the Privacy Commissioner of the disclosure, but the Privacy Commissioner is not obligated to notify affected individuals of the disclosure. Section 8(5) should be amended to require government institutions themselves to notify affected Canadians whenever their personal information is disclosed.
6. Mandate stronger Privacy Impact Assessments. The *Privacy Act* should require Privacy Impact Assessments for high-risk programs involving extensive data collection, data sharing, or surveillance. Assessments should be publicly available whenever possible and subject to independent review.

Conclusion

The Supreme Court’s commitment to privacy, through its interpretations of section 8 of the *Charter*, is a bulwark against state intrusion into Canadians’ private lives.

Yet, successive recent federal statutes (e.g., C-8, C-22, C-34) and existing older laws (e.g., *PCMLTFA* and *Customs Act*) have undercut these protections through lowered thresholds, expanded sharing powers, mandatory data retention, and weakened oversight. These measures risk normalizing surveillance by proxy, and they risk undermining reasonable privacy expectations in both personal data and digital communications.

Canada needs proactive, restorative amendments to its privacy laws. Strengthening *PIPEDA* (or its proposed replacement, *PPCDA*) through mandatory data minimization, new enhanced powers for the Privacy Commissioner, and explicit rights-based language, accompanied by targeted reforms to the *Privacy Act*, will re-establish meaningful safeguards.

This report’s proposed reforms aim to restore privacy as the default rule rather than the exception. Stronger consent, tighter limits on collection/retention, meaningful deletion rights, restrictions on voluntary disclosures, and independent oversight would ensure

³³ Government of Canada. “Privacy Act.” R.S.C., 1985, c. P-21. <https://laws-lois.justice.gc.ca/eng/acts/p-21/FullText.html>.

personal information is collected only when necessary, and handled with appropriate safeguards.

Privacy is a precondition for freedom of thought, freedom of expression, personal autonomy, and human dignity. Protecting privacy is therefore essential not only to safeguarding personal information, but to preserving freedom itself.

Bibliography

Carpay, John. "Privacy Is the Shield of a Free People: How Bill C-22 Undermines Canadians' Right to Privacy." Brief to the Standing Committee on Public Safety and National Security. Justice Centre for Constitutional Freedoms, May 12, 2026. <https://www.jccf.ca/wp-content/uploads/2026/05/2026-05-12-Brief-to-SECU-about-C-22-.pdf>.

Department of Justice Canada. "General principles for the interpretation and application of the Charter." Last modified July 14, 2025. <https://www.justice.gc.ca/eng/cs/sjc/rfc-dlc/ccrf-ccd/check/principles-principes.html>. Accessed June 15, 2026.

Geist, Michael. "One Step Forward, Two Steps Back: Bill C-36 Modernizes Canada's Privacy Law, Then Delays It to 2030." Blog. June 18, 2026. <https://www.michaelgeist.ca/2026/06/billc36/>.

Geist, Michael. "The Law to Be Named Later: Bill C-34 Punts 50 Key Decisions to Cabinet and a Digital Safety Commission That Does Not Yet Exist." Blog. June 11, 2026. <https://www.michaelgeist.ca/2026/06/the-law-to-be-named-later-bill-c-34-punts-50-key-decisions-to-cabinet-and-a-digital-safety-commission-that-does-not-yet-exist/>.

Government of Canada. "The Canadian Charter of Rights and Freedoms." Justice Centre for Constitutional Freedoms. <https://www.jccf.ca/the-canadian-charter-of-rights-and-freedoms/>.

Government of Canada. "Customs Act." R.S.C. 1985, c. 1 (2nd Supp.), s. 99. Current to March 2, 2026. <https://laws-lois.justice.gc.ca/eng/acts/C-52.6/section-99.html>.

Government of Canada. "FINTRAC Annual Report 2024–25." Financial Transactions and Reports Analysis Centre of Canada. <https://fintrac-canafe.canada.ca/publications/ar/2025/ar2025-eng.pdf>.

Government of Canada. "Personal Information Protection and Electronic Documents Act." Act current to 2026-05-26. <https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-7.html#h-417659>.

Government of Canada. "Privacy Act." (R.S.C., 1985, c. P-21). Current to May 26, 2026. <https://laws-lois.justice.gc.ca/eng/acts/p-21/>.

Government of Canada. National Security and Intelligence Review Agency (NSIRA). "About NSIRA - The Trusted Eyes and Ears of Canadians." <https://nsira-ossnr.gc.ca/en/about-nsira/>.

Harrison Faulkner. "'Big Step Towards Police State' — Lawyers Sound Alarm Against Liberal Bill C-2." YouTube video, July 3, 2025. <https://www.youtube.com/watch?v=Zzi7Wpx2iow>.

Hunter et al. v. Southam Inc., [1984] 2 SCR 145, 1984 CanLII 33 (SCC). <https://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html>. Retrieved on 2026-06-18.

Ibid.

Office of the Privacy Commissioner of Canada. "Appearance before the House of Commons' Standing Committee on Finance for its statutory review of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)." February 28, 2018. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180228/.

Office of the Privacy Commissioner of Canada. "Public Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime: Submission of the Office of the Privacy Commissioner of Canada to Finance Canada." August 10, 2023. https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_fc_230810/.

Office of the Privacy Commissioner of Canada, Submission on Privacy Act Modernization (March 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103/.

Office of the Privy Council. "Guidelines for obtaining meaningful consent." Date modified: 2025-08-11. https://www.priv.gc.ca/en/privacy-topics/business-privacy/collecting-personal-information/consent/gl_omc_201805/.

Parliament of Canada. House of Commons. "Bill C-22: An Act Respecting Lawful Access (Lawful Access Act, 2026)." 45th Parliament, 1st Session, 2026. <https://www.parl.ca/legisinfo/en/bill/45-1/c-22>.

Parliament of Canada. House of Commons. "Bill C-22: An Act Respecting Lawful Access (Lawful Access Act, 2026)." 45th Parliament, 1st Session. As passed by the House of Commons, June 18, 2026. <https://www.parl.ca/documentviewer/en/45-1/bill/C-22/third-reading>.

Parliament of Canada. House of Commons. "Bill C-8: An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts." 45th Parliament, 1st Session, 2025. <https://www.parl.ca/LegisInfo/en/bill/45-1/c-8>.

Parliament of Canada. House of Commons. "C-34 - Safe Social Media Act." First Session, Forty-fifth Parliament. First Reading. <https://www.parl.ca/documentviewer/en/45-1/bill/C-34/first-reading>.

Parliament of Canada. House of Commons. "Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act." 45th Parliament, 1st session. First reading, June 15, 2026. <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading>.

R. v. Duarte, 1990 CanLII 150 (SCC), [1990] 1 SCR 30, <https://canlii.ca/t/1fszz>, retrieved on 2026-06-18 <https://www.canlii.org/en/ca/scc/doc/1990/1990canlii150/1990canlii150.html>

Shinfield, Jacqueline D., Vladimir Shatiryan, and Ora Morison. "Strong Borders Act: A Landmark Shift in Canada's AML Penalties." Blake, Cassels & Graydon LLP. Lexology. June 4, 2025. <https://www.lexology.com/library/detail.aspx?g=327738bc-b505-4aa2-8f5f-45047d400ba9>.



Justice Centre

for Constitutional Freedoms

253-7620 Elbow Drive SW, Calgary, Alberta, T2V 1K2

www.jccf.ca