SENATE
SÉNAT
CANADA

Privacy Issues Regarding Federal Political Parties under the *Canada Elections Act*

Interim report of the Standing Senate Committee on Legal and Constitutional Affairs

The Honourable David M. Arnot, *Chair*
The Honourable Denise Batters, *Deputy Chair*

MAY 2026

SENATE
SÉNAT
CANADA

For more information, please contact us by:
Email: LCJC@sen.parl.gc.ca
Mail: The Standing Senate Committee on Legal and Constitutional Affairs
Senate of Canada, Ottawa, Ontario, Canada, K1A 0A4
This report can be downloaded at: sencanada.ca
The Senate is on X: @SenateCA
Follow the committee using the hashtag #LCJC

Ce rapport est également offert en français.

Table of Contents

The Committee Membership

The Honourable
David M. Arnot
Chair

The Honourable
Denise Batters
Deputy Chair

The Honourable Senators

Bernadette Clement

Baltej S. Dhillon

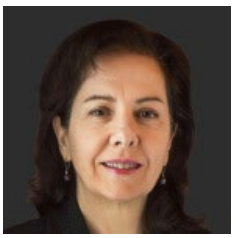
Yonah Martin

Julie Miville-Dechêne

Manuelle Oudar

Kim Pate

Paul Prosper (PJ)



Raymonde Saint-Germain

Paula Simons

Scott Tannas

Kristopher Wells

Ex officio members of the committee:

The Honourable Pierre Moreau (or Patti LaBoucane-Benson)
The Honourable Leo Housakos (or Yonah Martin)
The Honourable Lucie Moncion (or Joan Kingston)
The Honourable Flordeliz (Gigi) Osler (or Robert Black)
The Honourable Brian Francis (or Judy A. White)

Other senators who have participated in the study:

The Honourable Rodger Cuzner
The Honourable Pierre J. Dalphond
The Honourable Donna Dasko
The Honourable Colin Deacon
The Honourable Pat Duncan
The Honourable Farah Mohamed

Library of Parliament:

Michaela Keenan-Pelletier, Analyst
Dana Phillips, Analyst

Senate Committees Directorate:

Vincent Labrosse, Clerk
Natassia Ephrem, Administrative Assistant

Communications, Broadcasting and Publications Directorate:

Chelsea DeFazio, Communications Officer

Order of Reference

Extract from the *Journals of the Senate* of Thursday, October 2, 2025:

> The Honourable Senator Arnot moved, seconded by the Honourable Senator Coyle:
>
> That the Standing Senate Committee on Legal and Constitutional Affairs, in accordance with rule 12-7(9), be authorized to examine and report on such issues as may arise from time to time relating to legal and constitutional matters generally; and
>
> That the committee submit its final report to the Senate no later than October 10, 2027.
>
> The question being put on the motion, it was adopted.

Shaila Anwar

Clerk of the Senate

Introduction

On February 18, 2026, the Standing Senate Committee on Legal and Constitutional Affairs (the committee) presented a report[1] in which the majority of the committee expressed serious concerns about the regime governing the protection of personal information by federal political parties under the *Canada Elections Act*[2] (CEA). The report was prepared on an expedited basis following an accelerated study of the subject matter of Part 4 of Bill C-4, An Act respecting certain affordability measures for Canadians and another measure,[3] which introduced important changes to the privacy regime under the CEA. Despite the majority of the committee's concerns, Part 4 of Bill C-4 was ultimately adopted without amendment and received royal assent on March 12, 2026.

The evidence received by the committee suggests to the majority of the committee that the rules governing the protection of personal information by federal political parties are gravely inadequate, leaving Canadians vulnerable to the violation of their rights and to the erosion of democratic norms. The evidence also indicates that Canada is an outlier internationally in not having comprehensive data protection laws that apply to federal political parties. The committee heard that Canada's approach is more in line with the United States (U.S.) than with other liberal democracies around the world.

Given its ongoing concerns about this critical issue, the majority of the committee believes that a more detailed account of the evidence received during its study of Part 4 of Bill C-4 is warranted. On April 22, 2026, the committee adopted a motion to draft an interim report under its general order of reference based on this evidence.[4] This more comprehensive report aims to promote public awareness and to inform the review of future legislation, including the new amendments to the privacy regime governing federal political parties that have recently been introduced via Bill C-25, An Act to amend the Canada Elections Act and to enact An Act to change the names of certain electoral districts, 2026.[5]

---

[1] Standing Senate Committee on Legal and Constitutional Affairs (LCJC), *The subject matter of Part 4 of Bill C-4, An Act respecting certain affordability measures for Canadians and* another measure, Fourth Report, February 18, 2026.

[2] *Canada Elections Act*, S.C. 2000, c.9 (CEA).

[3] Bill C-4, An Act respecting certain affordability measures for Canadians and another measure, 1st session, 45th Parliament.

[4] LCJC, *Minutes of Proceedings*, 22 April 2026.

[5] Bill C-25, An Act to amend the Canada Elections Act and to enact An Act to change the names of certain electoral districts, 2026, 1st session, 45th Parliament (Bill C-25).

Legislative Context

Federal Privacy Laws

At the federal level, the protection of personal information is governed by the *Privacy Act*[6] in the public sector and the *Personal Information Protection and Electronic Documents Act*[7] (PIPEDA) in the private sector**.** Both regimes are subject to oversight and enforcement by the Office of the Privacy Commissioner of Canada. However, neither the *Privacy Act* nor *PIPEDA* apply to federal political parties. Instead, the obligations of federal political parties with respect to the protection of personal information are set out in the CEA, which is overseen and enforced by the Commissioner of Canada Elections.

The CEA regime requires federal political parties to publish a privacy policy that describes certain aspects of how they handle personal information. However, there are no minimum requirements for the standards set out in the policy or for the actual handling of personal information.

Prior to the adoption of Bill C-4, there were certain provincial privacy laws that may have applied to federal political parties, most notably in British Columbia (B.C.). As explained below, these were ousted by Bill C-4.

Part 4 of Bill C-4

Part 4 of Bill C-4 replaced the provisions governing the protection of personal information by federal political parties under the CEA with a new regime. The new regime explicitly exempts federal political parties from the application of provincial or territorial privacy legislation, including any requirements to provide access to or to correct personal information under their control. The exemption, along with certain other parts of the new privacy regime, applies retroactively to May 31, 2000, the date on which the CEA first received royal assent.

The exemption provision in Part 4 of Bill C-4 has been widely understood as a response to the 2024 decision of the B.C. Supreme Court in *Liberal Party of Canada v. The Complainants,*[8] which affirmed that B.C.'s *Personal Information Protection Act*[9] *(*PIPA) applies to the collection, use and disclosure of personal information by

[6] *Privacy Act*, R.S.C. 1985, c. P-21.

[7] *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5.

[8] *Liberal Party of Canada v. The Complainants*, 2024 BCSC 814.

[9] *Personal Information Protection Act*, S.B.C. 2003, c. 63.

federal political parties in the province.[10] That decision was under appeal when Bill C-4 was introduced.

The new regime under Bill C-4 also makes certain other changes to the privacy obligations of federal political parties, including:

- requiring parties to designate a privacy officer, who must provide an annual statement to the Chief Electoral Officer confirming the party's compliance with its privacy policy;
- broadening the language of the provision that sets out what parties are allowed to do with personal information;
- expressly requiring parties to comply with their own privacy policies, and making non-compliance a violation of the CEA subject to administrative monetary penalties; and
- requiring the Chief Electoral Officer to hold an annual meeting relating to the protection of personal information by federal political parties.

Legislative History

Bill C-4 was introduced in the House of Commons on June 5, 2025 by the Minister of Finance and National Revenue. On December 11, 2025, the bill passed third reading in the House of Commons and received first reading in the Senate. Bill C-4 passed second reading in the Senate on February 5, 2026. On the same day, a motion[11] was adopted in the Senate referring the bill to the Standing Senate Committee on National Finance (NFFN) for study and authorizing the Standing Senate Committee on Legal and Constitutional Affairs to examine and report on the subject matter of Part 4 of the bill to inform NFFN's study. NFFN was required to submit its final report on Bill C-4 to the Senate by the end of Routine Proceedings on February 24, 2026.

---

[10] *Liberal Party of Canada v. The Complainants*, 2024 BCSC 814. The case stemmed from a 2019 request by three B.C. residents for access to their personal information held by three federal political parties, and for details about how their information was being used. Unsatisfied with the parties' response, the residents requested that the Office of the Information and Privacy Commissioner of British Columbia (OIPC) investigate the parties' data handling practices under B.C.'s *Personal Information Protection Act* (PIPA). The parties challenged the OIPC's jurisdiction, arguing that PIPA did not apply to them. The Commissioner conducted an inquiry on this issue and found that PIPA applied to federal political parties (*Conservative Party of Canada (Re)*, 2022 BCIPC 13 (CanLII)). On judicial review, the Supreme Court of B.C. upheld the Commissioner's decision, affirming that PIPA complements rather than conflicts with the CEA. For further commentary on the evolution of the case, see: Andrew Clement, Professor Emeritus, Faculty of Information, University of Toronto, Brief submitted to LCJC; J. Colin Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.

[11] Senate, *Journals*, 5 February 2026.

Of note, the Standing Senate Committee on Legal and Constitutional Affairs was authorized to study the subject matter of Part 4 of the bill, not the bill itself. Consequently, the committee presented a report that included observations and recommendations, but was unable to directly amend the bill.

The Committee's Study and Report

The committee studied Part 4 of Bill C-4 over the course of three meetings (totalling six hours) on February 12, 2026, and heard testimony from the Chief Electoral Officer of Canada, the Commissioner of Canada Elections, the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of British Columbia, the Privy Council Office, as well as from advocacy organizations and other experts. The committee also heard from counsel for the Liberal Party of Canada, the Conservative Party of Canada, and the New Democratic Party. In addition to the testimony heard, the committee received numerous written submissions from interested parties.

On February 18, 2026, the committee presented a report outlining its key observations and recommendations. While agreeing with the government's stated objective of establishing a uniform national privacy regime governing federal political parties, the majority of the committee expressed serious concerns about the adequacy of the regime advanced in Part 4 of Bill C-4. The committee also signaled its dissatisfaction with the inclusion of Part 4 in an affordability bill otherwise unrelated to privacy protections, and with the limited time provided for the committee's review. The majority of the committee ultimately recommended that Part 4 of Bill C-4 be either removed, severed from the rest of the bill to allow more time for review, or made subject to a sunset clause.

The Adoption of Bill C-4

During third reading of Bill C-4 in the Senate, a motion[12] to delete Part 4 of the bill was defeated; a second motion[13] to amend Part 4 to include specific minimum privacy safeguards was also defeated. A third motion[14] was moved to apply a sunset clause to the provisions of Part 4 establishing exclusive federal jurisdiction over the privacy policies of federal political parties. Under the proposed motion, these provisions would be repealed three years after the bill received royal assent, providing an opportunity for the federal government to introduce a more robust privacy regime. The motion to add a sunset clause was adopted, and the bill was amended accordingly. On February 26, 2026, Bill C-4 passed third reading in the

[12] Senate, *Debates*, 25 February 2026.

[13] Senate, *Debates*, 26 February 2026.

[14] Senate, *Debates*, 26 February 2026.

Senate. It was then sent back to the House of Commons for consideration of the Senate amendments.

On March 12, 2026, the House of Commons rejected the Senate amendments, concurring that:

> Parliament should be the body that decides the rules that govern communication by federal parties with Canadians, the amendment constitutes a substantive reversal of the principle of the proposed amendments to the Canada Elections Act in Part 4 of Bill C-4, the government intends to bring forward additional privacy provisions in legislative changes to the Canada Elections Act within this parliamentary session, and furthermore, there is a long tradition of the Senate deferring to the House of Commons on amendments to the Canada Elections Act, particularly those which have unanimous support of all recognized parties in the House and which govern the operations of candidates representing political parties seeking election to the House of Commons.[15]

The Senate did not insist on its amendments, and Part 4 received royal assent without amendment, along with the rest of Bill C-4, on March 12, 2026.

What the Committee Heard

Jurisdiction and Uniformity

During the committee's study, witnesses from the Privy Council Office described Part 4 of Bill C-4 as a narrowly targeted effort to clarify the federal government's exclusive jurisdiction over the privacy obligations of federal political parties. They underscored the importance of ensuring that federal political parties are subject to a uniform national privacy regime under the CEA, rather than a patchwork of provincial and territorial laws—a point echoed by counsel for the parties.[16]

Counsel for the parties stressed that federal political parties are run largely by volunteers, who could be deterred by complex regulatory requirements.[17] "Asking volunteers to comply with as many as 14 conflicting and overlapping provincial and

---

[15] House of Commons, *Debates*, 12 March 2026 (Hon. Maninder Sidhu (Brampton East)).

[16] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Cathy Hawara, Assistant Secretary to the Cabinet, Machinery of Government and Democratic Institutions, Privy Council Office; Rachel Pereira, Director, Electoral and Senatorial Policy Unit, Democratic Institutions, Privy Council Office); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada; Michael Wilson, Outside Counsel, Goodmans LLP, Conservative Fund Canada; Carmela Allevato, Senior Counsel, Allevato Quail and Associates, New Democratic Party of Canada).

[17] Ibid.

federal laws is not realistic,"[18] Alexis Levine, counsel for the Federal Liberal Agency of Canada, told the committee. Mr. Levine and Michael Wilson, counsel for the Conservative Fund Canada, emphasized that all voters should have the same rights, regardless of where they live.[19]

However, other witnesses pointed out that the CEA regime is not uniform from the perspective of electors or for enforcement purposes, since each party establishes their own policy with respect to the collection, use, and retention of Canadians' personal information.[20] "There is nothing 'national or uniform' about these provisions," asserted Colin J. Bennett, Professor Emeritus, Department of Political Science, University of Victoria, in a brief to the committee.[21]

Caroline Simard, the Commissioner of Canada Elections, explained that "every party has its own unique policy, which would require my office to essentially develop expertise in 15 distinct policies. This lack of uniformity increases complexity and can undermine the consistency of our investigations."[22] She added that the policies are often drafted in vague language and frequently changed, creating further enforcement challenges.[23]

In addition to the concern about a patchwork of laws, counsel for the parties argued that regulating how federal political parties communicate with voters is, in Mr. Wilson's words, "tantamount to regulating federal elections themselves," which "must plainly be a federal responsibility."[24] On the other hand, the committee heard that the protection of personal information is an area of shared jurisdiction between the federal and provincial governments.[25] Several witnesses viewed Part 4 of Bill C-4 as undermining provincial privacy rights and running counter to the principle of

---

[18] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada).

[19] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada; Michael Wilson, Outside Counsel, Goodmans LLP, Conservative Fund Canada).

[20] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada; Caroline Simard, Commissioner of Canada Elections, Office of the Commissioner of Canada Elections).

[21] Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.

[22] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Caroline Simard, Commissioner of Canada Elections, Office of the Commissioner of Canada Elections).

[23] Ibid.

[24] *Proceedings : Evidence of 12 February 2026, Meeting 2* (Michael Wilson, Outside Counsel, Goodmans LLP, Conservative Fund Canada).

[25] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Michael Harvey, Commissioner, Office of the Information and Privacy Commissioner for British Columbia).

cooperative federalism, which favours "collaboration and coordination between federal and provincial governments."[26]

Stakeholders were especially concerned about the move to oust provincial privacy laws without establishing equivalent federal protections. As expressed by Tamir Israel of the Canadian Civil Liberties Association, "a comprehensive set of regulations at the federal level would be preferable," but "these [provincial] rights are being removed, moving forward, as well as retroactively, while nothing meaningful is being put in place at the federal level."[27]

Retroactivity

Several participants voiced concerns about the retroactive application of certain provisions in Part 4 of Bill C-4, including the provision exempting federal political parties from provincial and territorial privacy laws. According to Rachel Pereira of the Privy Council Office, "these provisions do not mean provincial laws no longer apply. These provisions are intended to clarify that the requirements for political parties have been and continue to be exclusively governed by the Canada Elections Act."[28] In practice, however, some witnesses indicated that Part 4 of Bill C-4 would retroactively remove privacy protections applicable to federal political parties in Quebec and B.C., such as the right of access to personal information held by political parties.[29]

Privacy experts condemned the bill's retroactive reach as immunizing federal political parties from accountability for past privacy violations.[30] In a brief to the

---

[26] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Bill Hearn, Principal, HearnLaw, External General Counsel to Centre for Digital Rights, Centre for Digital Rights). See also: LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance; Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Michael Harvey, Commissioner, Office of the Information and Privacy Commissioner for British Columbia).

[27] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association). See also: LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Michael Harvey, Commissioner, Office of the Information and Privacy Commissioner for British Columbia).

[28] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Rachel Pereira, Director, Electoral and Senatorial Policy Unit, Democratic Institutions, Privy Council Office).

[29] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Bill Hearn, Principal, HearnLaw, External General Counsel to Centre for Digital Rights, Centre for Digital Rights) (regarding Quebec); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia) (regarding B.C.).

[30] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Matthew Alexander Hatfield, Executive Director, OpenMedia; Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association); Andrew Clement, Professor Emeritus, Faculty of

committee, the BC Freedom of Information and Privacy Association (FIPA) noted that the retroactive application also forecloses the possibility of making access requests regarding personal information collected prior to the passage of the bill.[31] The Digital ID and Authentication Council of Canada described the retroactive aspect of Part 4 of Bill C-4 as "an extraordinary measure" that "undermines the rule of law and public confidence in democratic institutions."[32]

Procedural Concerns

Concerns were also voiced about the legislative process through which the amendments in Part 4 of Bill C-4 were presented and studied. Many were troubled by the inclusion of these amendments within an omnibus bill focused on urgent cost of living issues. As stated by Jim Balsillie, Founder of the Centre for Digital Rights:

> *Measures that compromise democratic integrity should not be held hostage to much-needed relief measures aimed at affordability. Challenges this serious deserve separate study through stand-alone legislation and full public scrutiny.*[33]

The lack of debate on Part 4 of Bill C-4 in the House of Commons, and the fast-tracking of its study in the Senate, were also sharply criticized.[34] Some experts suggested that a more active Senate role with respect to Part 4 was warranted, given the "vested interest" of federal political party members in the privacy laws that govern them.[35] According to Jason Woywada, Executive Director of the BC

Information, University of Toronto, Brief submitted to LCJC; Digital ID and Authentication Council of Canada, Brief submitted to LCJC, 12 February 2026.

[31] BC Freedom of Information and Privacy Association, Brief submitted to LCJC.

[32] Digital ID and Authentication Council of Canada, Brief submitted to LCJC, 12 February 2026.

[33] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jim Balsillie, Founder, Centre for Digital Rights). See also: Alberta Enterprise Group, Brief submitted to LCJC, 12 February 2026; Michael Geist, Canada Research Chair in Internet and E-commerce Law and Full Professor, Faculty of Law, Brief submitted to LCJC, February 2026.

[34] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association); Michael Geist, Canada Research Chair in Internet and E-commerce Law and Full Professor, Faculty of Law, Brief submitted to LCJC, February 2026.

[35] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association). See also: LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Matthew Alexander Hatfield, Executive Director, OpenMedia); Andrew Clement, Professor Emeritus, Faculty of Information, University of Toronto, Brief submitted to LCJC.

Freedom of Information and Privacy Association, this "is precisely the sort of scenario where sober second thought is essential."[36]

The Need for Robust Privacy Protections

A repeated refrain throughout the committee's study was the lack of minimum privacy standards or meaningful oversight governing federal political parties. "Political data sits at the core of democratic participation, yet Canadian political parties have placed themselves outside the privacy rules they impose on others,"[37] Mr. Balsillie told the committee. According to Mr. Woywada, federal political parties are subject to less restrictions and oversight than Canadian spy agencies.[38]

Advocacy organizations and policy experts cautioned that, at a time when data-driven technologies used to influence voters are becoming increasingly sophisticated, this lack of protections creates significant risks to Canada's democracy, digital sovereignty, and national security. In Mr. Woywada's words:

> *Bill C-4, Part 4, represents a significant departure from established Canadian democratic and privacy norms that places the personal information of Canadians at increased risk. It does not simply modernize electoral rules. It removes guardrails protecting the personal information of Canadians at a time when global experience tells us those guardrails are increasingly important.*[39]

The Power of Data

The committee received compelling evidence about how profoundly data now shapes the economic and political landscape.

Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance at McMaster University, described how federal political parties use the services of many different data companies, including foreign companies.[40] She explained how these companies use the data they collect to create more data through statistical inferences, AI techniques and cross-linking to other datasets,

---

[36] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association).

[37] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jim Balsillie, Founder, Centre for Digital Rights).

[38] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association).

[39] Ibid.

[40] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance).

allowing them to draw inferences about people's political views, behaviours and economic circumstances "that would be relevant in a trade context, in a political context or in a context relating to sovereignty."[41]

Professor Bannerman underlined the potential consequences of data breaches and misuses in this context, which she described as "no longer a question of 'if,' but 'when'."[42] She warned about "the wall between political parties and government breaking down," such that "[d]ata could be used against civil servants at the border or passed to other governments."[43]

Mr. Woywada informed the committee that foreign interference "often relies on lawfully obtained domestic personal information accessed through intermediary domestic actors that can include Canadian political parties."[44] He asserted: "That is why privacy and fair information safeguards are also national security safeguards."[45]

Mr. Balsillie warned:

> *[T]he absence of governance for the contemporary surveillance economy has allowed personal data generated by our experiences, choices and even our thoughts to be captured, processed and traded as an economic input for profit and power. ... This has caused a new era of human commodification that violates fundamental human rights in new ways*.[46]

The Threat to Democracy

The evidence received by the committee underscored the threat that the unchecked data practices of federal political parties pose to democratic norms, in particular. Several privacy experts described how federal political parties, aided by technology companies, leverage personal information to develop detailed voter profiles and deliver increasingly targeted political messages. "We are talking about voter discouragement and misinforming voters, as well as providing very different

---

[41] Ibid.

[42] Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance, Brief submitted to LCJC, 11 December 2025.

[43] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance).

[44] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association).

[45] Ibid.

[46] Ibid.

messages to different types of voters,"[47] indicated Matthew Alexander Hatfield, Executive Director of OpenMedia.

Professor Bannerman spoke of "a transformation of how electoral campaigning is being done that does go heart of questions about how our democracy works."[48] As she explained in her brief:

> *Rather than appealing to collective political values or visions of what Canadians may want in the future or as a society — critically important at this troubling moment in history — datafied campaigning addresses individual citizens who are alone on their phones, computers and other devices.*[49]

Professor Bannerman added that, as campaigns increasingly target narrow bands of persuadable voters, many people risk being excluded from the political process.[50]

In another brief to the committee, the Centre for Digital Rights tied the fragmentation of political messaging to the fragmentation of party platforms themselves, and pointed to a range of other harms that can result from the weak privacy regulation of federal political parties. These include the misuse of voter data for commercial ends, voter cynicism and disengagement, and inequality between parties (since "data-driven elections tend to favour better-resourced parties").[51]

According to the Centre for Digital Rights and the BC Freedom of Information and Privacy Association, the inadequate regime established under Part 4 of Bill C-4 violates "quasi-constitutional" privacy protections as well as the democratic rights enshrined in section 3 of the *Canadian Charter of Rights and Freedoms*[52] (the Charter).[53] Section 3 of the Charter guarantees citizens' rights to vote in federal and

---

[47] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Matthew Alexander Hatfield, Executive Director, OpenMedia).

[48] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance).

[49] Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance, Brief submitted to LCJC, 11 December 2025.

[50] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance).

[51] Centre for Digital Rights, Brief submitted to LCJC, 9 December 2025.

[52] The *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982 (UK),* 1982, c 11.

[53] Centre for Digital Rights, Brief submitted to LCJC, 9 December 2025; BC Freedom of Information and Privacy Association, Brief submitted to LCJC.

provincial elections, and has been interpreted as ensuring meaningful participation in the electoral process.[54]

Cambridge Analytica

Many witnesses pointed to the activities of British company Cambridge Analytica as the most striking example of the threat that data-driven campaigning poses to democracy. As Mr. Israel explained, Cambridge Analytica used a Facebook quiz to harvest massive amounts of sensitive personal information without consent. The data was then used to create detailed psychometric profiles in order to micro-target voters, most notably during the 2016 election of Donald Trump in the U.S.[55]

The committee heard from Elizabeth Denham, former Information Commissioner of the United Kingdom (U.K.) and former Information and Privacy Commissioner of B.C., whose U.K. office undertook an 18-month long investigation into Cambridge Analytica, Facebook, and several other organizations in 2017.

> *What we found was that there was a disturbing disregard for voters' personal privacy by players across the whole political campaigning ecosystem, in which personal data is collected, shared and used to target and influence voters, often without transparency and without consent.*[56]

In a brief to the committee, Andrew Clement, Professor Emeritus in the Faculty of Information at the University of Toronto, highlighted Cambridge Analytica's connections to Canada. He noted that the company's primary whistleblower was from Victoria, B.C. and had previously worked as a data consultant for the federal Liberal party. Furthermore, the company's election software was developed by a Victoria-based company—Aggregate IQ—that has been reprimanded for violating Canadian privacy laws in the context of the U.K.'s Brexit campaign.[57]

---

[54] Centre for Digital Rights, Brief submitted to LCJC, 9 December 2025, citing *Frank v. Canada (Attorney General)*, 2019 SCC 1, at para 26.

[55] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association). See also Andrew Clement, Professor Emeritus, Faculty of Information, University of Toronto, Brief submitted to LCJC; Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The Guardian,* 17 March 2018.

[56] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

[57] Andrew Clement, Professor Emeritus, Faculty of Information, University of Toronto, Brief submitted to LCJC.

Ms. Denham reminded the committee that the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) conducted a lengthy study on the Cambridge Analytica-Facebook data breach, and ultimately recommended that the private sector privacy regime set out in PIPEDA be applied to federal political parties.[58]

The Rapid Evolution of Data-Based Technologies

Nearly a decade after the investigation into Cambridge Analytica, several witnesses raised alarms over how rapidly the technologies and methods that underlie data-driven campaigning are evolving, amplifying the risks to democracy. Mr. Israel told the committee:

> *Political parties are subjecting people to intrusive scrutiny, and the ability to leverage this data-rich ecosystem to manipulate the electorate in real time is growing daily. Data-driven political campaigning is also not limited to elections, but instead is becoming integral to how political parties interact with the public all year round.*[59]

Mr. Hatfield stressed the power of artificial intelligence (AI) to transform political playbooks. "An AI agent can take in a thousand points of data and influence your specific vote, which is going to escalate the abuse quite a bit," he remarked. "What will be possible for parties to do in a few years will make canvassing voters on their doorsteps or through their phones look like a pointy stick next to an atom bomb."[60]

The International Landscape

The committee learned that Canada's privacy regime for federal political parties is more in step with the U.S. than with other liberal democracies.

Evidence presented to the committee indicated that data-driven campaign tactics are becoming increasingly prominent in the U.S., and that the technology companies

---

[58] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia). House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, Seventeeth report, 11 December 2018, Recommendation 1.

[59] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association).

[60] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Matthew Alexander Hatfield, Executive Director, OpenMedia).

developing and supporting these methods are primarily American.[61] According to Mr. Israel, a study from 2020 found that one political party in the U.S. had gathered more than 3,000 data points on every voter. Furthermore, online ads have targeted Black Americans "with the express intention of deterring them from voting."[62]

Professor Bannerman advised the committee that Canadian federal political parties rely on American firms, and that Canada's permissive approach to the privacy regulation of federal political parties is pushing our election dynamics in the same direction as the U.S.[63] Bill Hearn, counsel for the Centre for Digital Rights, similarly affirmed: "Canada, federally, is an outlier here in the G7. We are more in line with the United States on this at the moment."[64]

Ms. Denham informed the committee that the U.K. and the European Union (E.U.) have "comprehensive data protection laws that extend across that whole political ecosystem, including political parties," and that New Zealand, South Korea, South Africa, Brazil and many other jurisdictions also include political parties in their privacy laws. [65]

"In Europe, under the General Data Protection Regulation, or GDPR, political opinions and political affiliation are classified as data of the highest sensitivity and subject to heightened protection,"[66] noted Mr. Balsillie. Quebec and British Columbia were also identified as examples of jurisdictions where privacy protections apply to political parties.[67] Mr. Woywada described Quebec, in particular, as "leading the charge" in its efforts to develop strong, modern privacy legislation.[68]

Indeed, the committee heard that, except for the U.S., most liberal democracies have comprehensive privacy laws that apply to political parties. In contrast,

---

[61] Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance, Brief submitted to LCJC, 11 December 2025.

[62] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association).

[63] Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance, Brief submitted to LCJC, 11 December 2025.

[64] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Bill Hearn, Principal, HearnLaw, External General Counsel to Centre for Digital Rights, Centre for Digital Rights).

[65] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

[66] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jim Balsillie, Founder, Centre for Digital Rights).

[67] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Bill Hearn, Principal, HearnLaw, External General Counsel to Centre for Digital Rights, Centre for Digital Rights); Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.

[68] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association).

Professor Bennett described the federal regime under the CEA as amounting to "little more than 'self-regulation' –entirely at odds with the contemporary international consensus on how to protect personal information in the modern digital age."[69]

What Canadians Want

The evidence presented to the committee suggests that the Canadian public is broadly in favour of holding federal political parties to a higher standard when it comes to privacy.

Stéphane Perrault, the Chief Electoral Officer, told the committee that when he undertook public consultations on this issue in 2021, "surveys showed that Canadians do want some rules around the use of personal information by political parties; that is something that came out very clearly."[70]

Professor Bannerman's research found that "Canadians are very concerned and very uncomfortable with data collection when asked, but they are also not necessarily aware of all those potential uses and the political consequences of those uses."[71] For this reason, she emphasized the importance of transparency, in addition to stronger protections.

According to Mr. Hatfield:

> *When you ask Canadians what the law should be here, we're of one mind: Privacy laws should be applied to political parties, just like everyone else. When OpenMedia and B.C. FIPA polled on this some years back, 72% of Canadians said so across partisan lines. You don't see that level of agreement on much else in politics.*[72]

The Special Context of Political Parties

Counsel for the parties offered a different perspective on the data practices of federal political parties. They noted that parties collect personal information primarily through volunteers, and characterized the data obtained as a tool to

---

[69] Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.

[70] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada).

[71] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance).

[72] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Matthew Alexander Hatfield, Executive Director, OpenMedia).

facilitate political communication. “When regulating communication by federal political parties with Canadian voters, we need balance to allow for democratic dialogue. Political parties need to be free to communicate with, and keep track of, the feedback they are receiving from, voters,” contended Mr. Levine. “That political dialogue is the best tool we have to combat foreign interference, misinformation and disinformation,”[73] he argued.

There was general agreement that parties do need access to some personal information, such as the data provided to parties by Elections Canada under the CEA,[74] to facilitate interactions with the public.[75] However, almost every expert who appeared before the committee or submitted a brief stressed that meaningful privacy protections and oversight remain critical. As the Digital ID and Authentication Council of Canada stated in its brief:

> *These considerations warrant a thoughtful approach that may differ in certain respects from the regimes governing commercial or government activities. However, uniqueness of context is not a justification for the absence of substantive privacy protections.*[76]

“[T]here are more surgical ways to balance democratic engagement with personal privacy,” remarked Ms. Denham.[77] She pointed to the U.K. General Data Protection Regulation,[78] which establishes broad privacy protections with some specially tailored exceptions for political parties. “There are some legitimate interests for political parties to collect data, but it doesn’t take away the rights of U.K. citizens,”[79] she explained.

---

[73] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada).

[74] Under the CEA, Elections Canada’s Chief Electoral Officer must provide lists of electors to registered or eligible parties at various points in the election cycle. The list includes each elector’s surname, given names, civic address and mailing address. See sections 45, 93, 104.2, 107, 109 and 110 of the CEA.

[75] See for example: LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association; Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

[76] Digital ID and Authentication Council of Canada, Brief submitted to LCJC, 12 February 2026.

[77] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

[78] United Kingdom, *Regulation (EU) 2016/679 of the European Parliament and of the Council*.

[79] Ibid.

Many participants were skeptical that basic privacy protections would interfere with democratic dialogue. On the contrary, the committee was told that democracy is "alive and well" in jurisdictions where comprehensive privacy laws apply to political parties.[80] As Mr. Israel pointed out, provincial parties in B.C. are already campaigning under such a regime. "These are not rules that are impossible to navigate and to do political campaigning around,"[81] he insisted.

The Types of Protections Needed

There was widespread agreement amongst those who appeared before the committee or made written submissions that federal political parties should be subject to baseline privacy requirements similar to those that govern other sectors of society. "Privacy is a fundamental right,"[82] asserted Philippe Dufresne, the Privacy Commissioner of Canada. "Privacy rules for political parties should parallel requirements that are already set out for public and private sector organizations under federal law — while being adapted to the unique role that political parties play in the democratic process."[83]

The most common proposal was to include federal political parties within the PIPEDA regime, as recommended by ETHI in 2018.[84] "That would be an easy way to leverage the existing infrastructure in the federal Office of the Privacy Commissioner and apply it to political parties on a moving-forward basis,"[85] explained Mr. Israel. Ms. Denham suggested that more specific rules should also be set out in a code of practice, as has been done in the U.K.[86]

---

[80] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia); Centre for Digital Rights, Supplementary Brief submitted to LCJC, 21 February 2026.

[81] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association).

[82] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

[83] Ibid. See also: Michael Geist, Canada Research Chair in Internet and E-commerce Law and Full Professor, Faculty of Law, Brief submitted to LCJC, February 2026.

[84] See for example: LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Bill Hearn, Principal, HearnLaw, External General Counsel to Centre for Digital Rights, Centre for Digital Rights); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association; Matthew Alexander Hatfield, Executive Director, OpenMedia; Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

[85] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Tamir Israel, Director, Privacy, Surveillance and Technologies Program, Canadian Civil Liberties Association.

[86] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

The Fair Information Principles

Regardless of the legislative vehicle, many witnesses were clear that federal political parties should be governed by the ten fair information principles set out in Schedule 1 of PIPEDA.[87] These include, among other things, requirements to:

- identify the purposes for which personal information is collected;
- obtain consent for the collection, use and disclosure of personal information;
- limit the collection, use, disclosure and retention of personal information to what is necessary for identified purposes;
- establish data security safeguards to protect against privacy breaches; and
- provide a mechanism for individuals to access and correct their personal information.

The committee was informed that both the *Privacy Act* and *PIPEDA* are grounded in the fair information principles.[88] As Mr. Perrault noted, his office has previously recommended that these principles be applied to federal political parties with oversight by the Privacy Commissioner of Canada.[89] Mr. Dufresne added that the Office of the Privacy Commissioner and the Chief Electoral Officer have jointly published privacy guidelines[90] for political parties that cover the fair information principles. He suggested that these could be incorporated into legislation.[91]

Consent

Witnesses indicated that the appropriate application of the fair information principles may vary depending on the context—particularly the principle of consent. For example, Mr. Dufresne indicated that implied consent can be appropriate when a party's actions are "within the reasonable expectations of individuals" but not when dealing with more sensitive information.[92] According to Professor Bannerman's research, Canadians expect that certain sensitive information, such as ethnicity, sexual orientation, and gender identity "should never be collected and

---

[87] *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5, Schedule 1.

[88] Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance, Brief submitted to LCJC, 11 December 2025.

[89] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada).

[90] Office of the Privacy Commissioner of Canada, *Guidance for federal political parties on protecting personal information*, 2019.

[91] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

[92] Ibid.

retained, or should be done only with individuals' explicit consent."[93] On the other hand, the Centre for Digital Rights suggested that federal political parties could be granted a limited exception to the consent requirement "*for reasons of public interest* provided that appropriate safeguards are established."[94]

Rights of Access and Correction

Counsel for the parties testified that the privacy policies of federal political parties provide for a right of correction; they do not explicitly include a right of access,[95] though Mr. Levine and Carmela Allevato, counsel for the New Democratic Party of Canada, noted that their parties have provided access in the past when requested to do so. [96]

Several witnesses underscored the importance of a formal right of access. [97] As Mr. Perrault explained, it is difficult to correct inaccurate information without knowing what information the party has in its possession.

Mr. Levine expressed some reservation that a right of access could be abused for tactical reasons. He gave the example of one campaign flooding another with access requests to tie up campaign resources. However, the Centre for Digital Rights questioned the practical significance of this concern, and suggested that the law could include tailored exceptions to address potentially abusive or time-consuming requests.[98]

Breach Notification Requirements

Privacy experts were of the view that federal political parties should be required to report privacy breaches to affected individuals as well as to an independent

---

[93] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance).

[94] Centre for Digital Rights, Supplementary Brief submitted to LCJC, 21 February 2026. Emphasis in the original.

[95] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada; Michael Wilson, Outside Counsel, Goodmans LLP, Conservative Fund Canada; Carmela Allevato, Senior Counsel, Allevato Quail and Associates, New Democratic Party of Canada).

[96] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Michael Wilson, Outside Counsel, Goodmans LLP, Conservative Fund Canada; Carmela Allevato, Senior Counsel, Allevato Quail and Associates, New Democratic Party of Canada).

[97] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance; Jason Woywada, Executive Director, BC Freedom of Information and Privacy Association); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada).

[98] Ibid.

oversight body. This was one of Mr. Dufresne's key recommendations.[99] Mr. Levine cautioned that breaches may be used to force disclosure in the context of foreign interference.[100] On the other hand, Mr. Perrault described such breach notification requirements as "fairly routine."[101]

"We have already witnessed a number of data breaches from political parties.[27] They are only likely to continue,"[102] stated Professor Bennett in his brief. Like Mr. Dufresne, he advised that the obligation to notify an affected individual should be triggered when there is a "real risk of significant harm" to that person.[103]

The Digital ID and Authentication Council of Canada called for breaches to be reported "within a defined and reasonable timeframe."[104] Mr. Dufresne advised that "political parties should report [a data breach] as early as possible when they are aware of it."[105]

Other Key Protections

Policy experts identified several other privacy protection measures that should be included in the regime governing federal political parties. Professor Michael Geist, Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, advocated for restoring the restrictions on the sale or "non-consensual transfer" of personal information that were included in former Bill C-65, An Act to amend the Canada Elections Act[106].[107] This bill, which also incorporated some of the fair information principles, died on the Order Paper in the House of Commons when Parliament was dissolved due to the 2025 general election. Mr. Levine and Ms. Denham both characterized Bill C-65 as a useful "starting point."[108]

---

[99] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

[100] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada).

[101] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada).

[102] Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.

[103] Ibid.

[104] Digital ID and Authentication Council of Canada, Brief submitted to LCJC, 12 February 2026.

[105] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

[106] Bill C-65, An Act to amend the Canada Elections Act, 1st Session, 44th Parliament.

[107] Michael Geist, Canada Research Chair in Internet and E-commerce Law and Full Professor, Faculty of Law, Brief submitted to LCJC, February 2026.

[108] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada; Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

Mr. Perrault reiterated a recommendation his office made in 2022 that political parties identify themselves in their communications with voters. He explained:

> *Canadians receive messages, but they don't know the source of the messages and when they receive a survey through a text message, they don't know that the information is being collected by a party and it can be used for political or electoral purposes. To me, the lack of transparency in communications only makes the lack of protection worse.*[109]

Michael Harvey, the Information and Privacy Commissioner for British Columbia, advocated for "a codification of individual data subjects' rights."[110] In addition to rights of notice, access, and correction, he listed the "right to be forgotten" as a common element of established privacy regimes.[111]

Oversight and Enforcement

The call for strong, independent oversight and enforcement of federal political parties' privacy obligations surfaced repeatedly throughout the testimony and written submissions. Ms. Denham described Canada as an international outlier in this respect as well.[112]

Mr. Levine pointed out that the Commissioner of Canada Elections is an independent agency with the power to enforce the CEA.[113] Witnesses from the Privy Council Office highlighted that under Part 4 of Bill C-4, the CEA would require federal political parties to comply with their own privacy policies or face sanctions from the Commissioner.[114]

---

[109] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada).

[110] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Michael Harvey, Commissioner, Office of the Information and Privacy Commissioner for British Columbia).

[111] Ibid.

[112] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia).

[113] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP, Federal Liberal Agency of Canada).

[114] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 1* (Rachel Pereira, Director, Electoral and Senatorial Policy Unit, Democratic Institutions, Privy Council Office; Cathy Hawara, Assistant Secretary to the Cabinet, Machinery of Government and Democratic Institutions, Privy Council Office).

However, Ms. Simard testified that her office would need additional powers to effectively enforce Part 4 of Bill C-4.

> *[T]he Canada Elections Act does not provide for investigative powers adapted to administrative investigations. In fact, without prior judicial authorizations, we do not have the power to compel testimony and the obligation to preserve or disclose documents or other evidence. Without these tools, the ability to access evidence would be difficult.* [115]

Given these limitations, Ms. Simard worried that "there would be a public perception that we can achieve more than what we can do in reality."[116]

Mr. Perrault and others indicated that the Privacy Commissioner of Canada would be better placed to oversee the privacy obligations of federal political parties.[117] The committee was advised that this is how it works in other jurisdictions, including the U.K.[118] "With all due respect to Elections Canada, and the Commissioner of Canada Elections, they do not possess the resources or the expertise to monitor the complex technical environment of modern digital campaigning," argued Professor Bennett. "The OPC [Office of the Privacy Commissioner], and its provincial and territorial counterparts do have that expertise and can give appropriate guidance about best practices."[119]

Both Ms. Simard and Mr. Dufresne agreed that effective oversight and implementation would require collaboration between the Privacy Commissioner of Canada, the Chief Electoral Officer, and the Commissioner of Canada Elections.[120] "Enabling inter-agency collaboration would strengthen the work of regulators, and would allow us to address complex issues that cut across sectors and

---

[115] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Caroline Simard, Commissioner of Canada Elections *Office of the Commissioner of Canada Elections*).
[116] Ibid.
[117] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada); Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC; Digital ID and Authentication Council of Canada, Brief submitted to LCJC, 12 February 2026.
[118] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia); LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Stéphane Perrault, Chief Electoral Officer, Elections Canada).
[119] Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.
[120] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Caroline Simard, Commissioner of Canada Elections *Office of the Commissioner of Canada Elections*; Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

jurisdictions,"[121] asserted Mr. Dufresne. Professor Bennett noted that such an approach would follow the model in B.C., where oversight of political parties is exercised jointly between the Office of the Information and Privacy Commissioner and Elections BC.[122]

At the same time, witnesses cautioned that the identity of the regulator is only one aspect of effective oversight. As Mr. Harvey remarked, "oversight is not only a question of who oversees compliance but also what is overseen and how the oversight takes place."[123] In his view, "there are serious deficiencies with respect to oversight, given the self-regulatory nature of the provisions."[124] Professor Bennett added that the current regime does not include a clear complaint handling process.[125]

Mr. Hatfield emphasized the need for meaningful penalty powers to enforce privacy violations. Currently under the CEA, the maximum penalty is $1500 for an individual and $5000 for an entity.[126] "We need to have actual deterrents here, and we simply don't,"[127] Mr. Hatfield stated. He acknowledged that high financial penalties could have a disproportionate impact on small political parties, but suggested that this could be addressed by setting penalty amounts "relative to the membership or financing of the party."[128]

The Broader Privacy Landscape

In addition to imposing meaningful privacy standards and oversight on federal political parties, the committee heard about the need to modernize privacy laws more generally. As Mr. Dufresne noted, the *Privacy Act* was adopted in the early 1980s, PIPEDA in 2000, and both are due for reform. "To this day, I do not have

---

[121] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

[122] Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.

[123] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Michael Harvey, Commissioner, Office of the Information and Privacy Commissioner for British Columbia).

[124] Ibid. Similarly, Mr. Dufresne remarked that enforcement powers are "only as strong as the policy is, and that is in the hands of the political parties." LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

[125] Colin J. Bennett, Professor Emeritus, Department of Political Science Associate Fellow, Center for Global Studies University of Victoria, Brief submitted to LCJC.

[126] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Caroline Simard, Commissioner of Canada Elections *Office of the Commissioner of Canada* Elections). CEA, s. 508.5(1). Bill C-25 would increase these amounts to $25,000 and $100,000 respectively (see clause 67).

[127] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Matthew Alexander Hatfield, Executive Director, OpenMedia).

[128] Ibid.

order-making powers or fine-making powers, and we stand out in terms of international comparators,"[129] he stressed.

Mr. Hatfield pointed out that under the current law, private entities are legally allowed to engage in extensive data collection and profiling. "PIPEDA is not nearly restrictive enough,"[130] he opined. Professor Bannerman explained: "[O]ur current privacy basis is based on individual privacy and consent, whereas we're now living in a world of big data, where extrapolations and data about one person can allow inferences about another."[131]

Conclusion

The evidence received by the committee during this short study exposed what the majority of the committee views as critical threats to Canadian democracy and national security, and to the rights of individual Canadians.

The committee agrees with those witnesses who suggested that the privacy obligations of federal political parties should be set out in a uniform national regime. However, the majority of committee members remain concerned that the current regime under the CEA falls far short of the minimum standards required to protect the individual and national interests of Canadians, at a time when global developments and emerging technologies point to increasing risks.

The majority of the committee urges the government to give this issue the serious consideration it deserves, and to act without delay to establish a robust legislative framework governing the privacy obligations of federal political parties that fully reflects the proposals received in this study and outlined in this report.

Respectfully submitted,

DAVID M. ARNOT

Chair

---

[129] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 3* (Philippe Dufresne, Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada).

[130] LCJC, *Proceedings : Evidence of 12 February 2026, Meeting 2* (Matthew Alexander Hatfield, Executive Director, OpenMedia).

[131] Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance, Brief submitted to LCJC, 11 December 2025.

Appendix A – Witnesses

Thursday, February 12, 2026, at 10:30 a.m.

Jim Balsillie, Founder (Centre for Digital Rights)

Sara Bannerman, Professor and Canada Research Chair of Communication Policy and Governance (As an Individual)

Cathy Hawara, Assistant Secretary to the Cabinet, Machinery of Government and Democratic Institutions (Privy Council Office)

Bill Hearn, Principal, HearnLaw, External General Counsel to Centre for Digital Rights (Centre for Digital Rights)

Rachel Pereira, Director, Electoral and Senatorial Policy Unit, Democratic Institutions (Privy Council Office)

Jason Woywada, Executive Director (BC Freedom of Information and Privacy Association)

Thursday, February 12, 2026, at 1:30 p.m.

Matthew Alexander Hatfield, Executive Director (OpenMedia)

Carmela Allevato, Senior Counsel, Allevato Quail and Associates (New Democratic Party of Canada)

Elizabeth Denham, Former Information and Privacy Commissioner of the United Kingdom and British Columbia (As an Individual)

Tamir Israel, Director, Privacy, Surveillance and Technologies Program (Canadian Civil Liberties Association)

Alexis Levine, Outside Counsel, Blake, Cassels and Graydon LLP (Federal Liberal Agency of Canada)

Michael Wilson, Outside Counsel, Goodmans LLP (Conservative Fund Canada)

Thursday, February 12, 2026, at 4:15 p.m.

Michael Bisson, Deputy Commissioner, Operations (Office of the Commissioner of Canada Elections)

Philippe Dufresne, Privacy Commissioner of Canada (Office of the Privacy Commissioner of Canada)

Michael Harvey, Commissioner (Office of the Information and Privacy Commissioner for British Columbia)

Stéphane Perrault, Chief Electoral Officer (Elections Canada)

Caroline Simard, Commissioner of Canada Elections (Office of the Commissioner of Canada Elections)

Josée Villeneuve, Deputy Chief Electoral Officer, Regulatory Affairs (Elections Canada)

Appendix B – Briefs

The committee received the following briefs during this study:

Brief from the Centre for Digital Rights

Brief from Sara Bannerman

Brief from Colin J. Bennett

Brief from Bill Hearn

Brief from Michael Geist

Brief from Andrew Clement

Brief from Alberta Enterprise Group

Brief from the BC Freedom of Information and Privacy Association

Brief from Jim Balsillie

Brief from the Digital ID and Authentication Council of Canada

Brief from the Centre for Digital Rights

sencanada.ca