Submission to the Standing Committee on Procedure and House Affairs Regarding Bill C-25, Strong and Free Elections Act

Submitted by: BC Freedom of Information and Privacy Association

Executive Summary

The BC Freedom of Information and Privacy Association supports the objective of Bill C-25: strengthening Canada's democratic resilience against foreign interference, impersonation, unlawful political financing, deceptive practices, and misuse of electoral processes. 1

However, Bill C-25 does not achieve these objectives.

The bill makes some improvements to the political-party privacy provisions recently enacted through Bill C-4. It would require federal political parties to include additional privacy-policy commitments relating to safeguards, breach response, equivalent protection by third parties, misleading statements, sale of personal information, and harmful public disclosure. These are improvements on their face. But they do not create a meaningful privacy regime for federal political parties.2

The core problem remains structural. Federal political parties would still be left primarily to draft, interpret, monitor, and enforce their own privacy policies, rather than being subject to direct statutory duties, enforceable individual rights, independent privacy oversight, and meaningful remedies.

Privacy policies are not privacy rights. Recent Ipsos polling confirms that Canadians expect federal political parties to be subject to enforceable access and correction rights, independent oversight, breach accountability, and meaningful penalties. 3

FIPA recommends that Bill C-25 be amended to:

- convert political-party privacy-policy requirements into direct statutory obligations;
- restore enforceable access and correction rights for individuals;
- subject federal political parties to independent privacy oversight;
- create a meaningful individual complaint mechanism;
- remove the provincial pre-emption and retroactivity provisions introduced by Bill C-4;
- broaden restrictions on political-data sharing beyond sale;
- lower the breach-notification threshold for political and voter information;
- require full accountability for data transferred to vendors, consultants, riding associations, campaigns, candidates, volunteers, data platforms, and other third parties;
- require privacy impact assessments for high-risk political data practices; and

---

1Bill C-25, An Act to amend the Canada Elections Act and to enact An Act to change the names of certain electoral districts, 1st Sess, 45th Parl, 2026 (first reading 26 March 2026) [Bill C-25], online: Parliament of Canada <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-25/first-reading>.

2Ibid, cl 36, amending *Canada Elections Act*, SC 2000, c 9, s 446.6.

3Ipsos, Protections Wanted for How Federal Political Parties Use Personal Information (21 April 2026), online: Ipsos <https://www.ipsos.com/en-ca/protections-wanted-how-federal-political-parties-use-personal-information>.

- create meaningful penalties and remedies.

The recent Alberta elector-list incident demonstrates why this matters. Elections Alberta has publicly stated that the provincial List of Electors is sensitive data and that it took emergency steps after credible information suggested a political party's copy of the list had been made available to an unauthorized third party, the Centurion Project Ltd. That incident is not an abstract privacy problem. It is a warning about what can happen when political data moves outside accountable systems. 4

Political data can be used to profile, target, manipulate, intimidate, suppress, or mislead voters. It can also become a tool for foreign interference. Canada cannot protect democratic institutions while leaving voters' personal information exposed to weak rules and self-regulation.

About FIPA

The BC Freedom of Information and Privacy Association is a non-partisan, non-profit society established in 1991 to promote and defend freedom of information and privacy rights in Canada. FIPA's mission is to improve and defend privacy and transparency as vital components of a free and democratic society.

FIPA makes this submission because the privacy of voters is inseparable from democratic integrity. Political parties collect, infer, use, retain, disclose, and transfer information that may reveal or predict political beliefs, issue priorities, voting tendencies, donor behaviour, and personal vulnerabilities. Those practices require enforceable rights and independent oversight.

1. Bill C-25 must be read together with Bill C-4

Bill C-25 cannot be assessed in isolation. It amends something akin to a political-party privacy framework created only recently through Part 4 of Bill C-4.

Bill C-25 was introduced on March 26, 2026, as the *Strong and Free Elections Ac*t. It would amend the *Canada Elections Act*5 6

Those democratic-integrity objectives are important, but these provisions are built upon Bill C-4's unstable foundation.

Bill C-4 amended the *Canada Elections Act* to create what it describes as a national, uniform, exclusive and complete regime applicable to registered and eligible parties' activities involving personal information, including the collection, use, disclosure, retention, and disposal of personal information. It also provides that federal political parties and persons acting on their behalf cannot be required to comply

4Elections Alberta, UPDATE: Unauthorized Use of List of Electors (30 April 2026), online: Elections Alberta <https://www.elections.ab.ca/resources/media/news-releases/update-unauthorized-use-of-list-of-electors/>.

6Bill C-25, supra note 1.

with provincial or territorial privacy laws when participating in public affairs by endorsing and supporting candidates, unless the party's own privacy policy provides otherwise. 7 8

That structure is unacceptable. It gives federal political parties a privileged position that is not available to businesses, charities, non-profits, public bodies, or other organizations that handle sensitive personal information. It also deprives voters of rights that are essential to privacy protection: the right to know what information is held about them, the right to challenge inaccurate information, and the right to seek independent review.

Bill C-25 improves some of the language around party privacy policies, but it does not fix the architecture.

2. The core flaw: policy requirements are not the same as privacy rights

Bill C-25 would require federal political parties to include additional elements in their privacy policies. These include safeguards proportionate to sensitivity, breach-response measures, protections for transferred information, annual attendance at a privacy meeting with the Chief Electoral Officer, and prohibitions against certain forms of misleading conduct, sale, and harmful public disclosure. 9

These changes are better than the current void. They do not address the structural problem.

A meaningful privacy law imposes direct statutory obligations on regulated organizations. It gives individuals enforceable rights. It provides independent oversight. It includes complaint mechanisms, investigation powers, audit powers, orders, remedies, and penalties. These are most often embedded by mirroring 1996 CAN/CSA-Q830-96 *Model Code for the Protection of Personal Information* which is the foundation of Canadian privacy law. 10

Bill C-25 does not do that.

Instead, the bill continues to treat privacy largely as a matter of party policy content. A party must say certain things in its policy. It must comply with that policy. But voters are not given a full set of statutory rights against the party itself. Both the Chief Electoral Officer of Canada and the Commissioner of Canada Elections have expressed concerns 11 with the changes made in Bill C-4, and Bill C-25 does not appear to address those concerns.

7Ibid, adding s 446.4 to the Canada Elections Act.

8Bill C-4, An Act respecting certain affordability measures for Canadians and another measure, 1st Sess, 45th Parl, 2026, s 47, adding s 446.2 to the Canada Elections Act, SC 2000, c 9 (assented to 12 March 2026) [Bill C-4], online: Parliament of Canada <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-4/royal-assent>.

9 Bill C-25, supra note 1, cl 36, amending s 446.6.

10 Canadian Standards Association, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 (Etobicoke, Ont: Canadian Standards Association, March 1996), online: <https://simson.net/ref/1996/CSA_Privacy_Standard_CSA-Q830-96.pdf>

11 Elections Canada, "Remarks of the Chief Electoral Officer before the Standing Committee on Legal and Constitutional Affairs on the subject matter of Part 4 of Bill C-4",(February 12, 2026), online: < https://www.elections.ca/content.aspx?section=med&dir=spe&document=feb1226&lang=e>

This leaves Canadians with weaker privacy protection when dealing with federal political parties than when dealing with many businesses, provincial organizations, public bodies, or other institutions that handle personal information.

That is backwards. Political parties handle information that can reveal or infer political beliefs, issue priorities, affiliations, identity characteristics, donation behaviour, geographic vulnerabilities, and voter preferences. That information is not less sensitive than ordinary commercial data. In a democracy, it is often more sensitive.

3. Canadians reject political-party self-regulation and expect enforceable privacy rights

Bill C-25 should be assessed not only against the preferences of political parties, but against the expectations of Canadians whose personal information is being collected, used, inferred, disclosed, retained, and transferred.

Recent Ipsos polling conducted for FIPA, the Canadian Civil Liberties Association, the Centre for Digital Rights, and OpenMedia found that federal political parties are among the least trusted institutions when it comes to protecting personal information. Only 33% of Canadians said they trust federal political parties to protect their personal information, while 60% said they have not very much trust or no trust at all. The poll was conducted online between April 7 and 8, 2026, with a sample of 2,001 Canadians aged 18 and older, weighted by region, age, gender, and education. 12

The same poll found a significant public awareness gap. Seventy percent of Canadians were unaware that federal political parties are not subject to the same privacy laws as businesses and public-sector organizations in some provinces or across Canada. Seventy-two percent were unaware that individuals do not have the same rights to access and correct personal information held by federal political parties as they do with many other organizations. 13

Once informed, Canadians' expectations are clear. Ipsos found that: 14

- 85% agree Canadians should have the right to request correction or deletion of personal information held by federal political parties;
- 84% agree Canadians should have the right to access personal information held by federal political parties;
- 83% agree federal political parties should face significant penalties if data breaches or misuse occur;
- 80% agree federal political parties should follow the same privacy rules as businesses and public-sector organizations; and
- 80% agree federal political parties should be subject to independent review and oversight.

These findings are directly relevant to Bill C-25. The bill recognizes that political-party privacy practices require stronger safeguards, breach-response obligations, third-party protection requirements, and

12 Ipsos, supra note 3.

13 Ibid.

14 Ibid.

penalties. But it leaves the core accountability structure in the hands of the political parties themselves. That does not reflect public expectations.

The Committee should treat the Ipsos findings as evidence that the current approach lacks public legitimacy. Canadians are not asking Parliament merely to require better party privacy policies. They expect Parliament to create enforceable privacy rights, independent oversight, breach accountability, and meaningful remedies.

4. There is still no independent privacy regulator

Bill C-25 leaves privacy enforcement primarily within the election-law framework.

The Chief Electoral Officer may verify whether party privacy policies contain required elements. The Commissioner of Canada Elections may investigate and enforce violations of the *Canada Elections Act.* Those roles are important, but they are not a substitute for privacy-law oversight.

Privacy oversight requires privacy-specific jurisdiction and expertise. A privacy regulator assesses whether an organization is collecting only what is necessary, using information for appropriate purposes, limiting disclosure, retaining information only as long as needed, safeguarding information appropriately, responding properly to breaches, and respecting individual access and correction rights.

Bill C-25 does not create that structure. It does not create a full individual complaint mechanism for voters whose personal information has been collected, inferred, used, shared, retained, transferred, or breached by a federal political party. It does not give an independent privacy regulator authority to audit party databases, compel records, investigate systemic practices, order corrective measures, or provide remedies to affected individuals.

This is a central defect. As mentioned, political parties access and handle sensitive data that can reveal a voter's political leanings, their contribution habits, and expose them to location-based vulnerabilities among other things. That information is deeply sensitive in a democratic society. It should not be regulated only through party-written policies and election-law compliance mechanisms.

FIPA recommends that federal political parties be subject to independent oversight by the Privacy Commissioner of Canada or an equivalent independent privacy regulator, with authority to:

- receive individual complaints;
- conduct audits and systemic investigations;
- compel records and evidence;
- investigate collection, use, disclosure, retention, transfer, breach, and deletion practices;
- issue findings or binding orders;
- require corrective action;
- recommend or impose penalties where appropriate; and
- coordinate with Elections Canada and the Commissioner of Canada Elections where privacy issues overlap with electoral-integrity concerns.

Privacy cannot be treated merely as a sub-component of election administration. It is a quasi-constitutional rights-protection issue in its own terms.

5. Access and correction rights must be restored

Access and correction rights are foundational to privacy protection.

Without access rights, individuals cannot know what personal information a federal political party holds about them. Without correction rights, they cannot challenge inaccurate, outdated, misleading, or improperly inferred information. Without independent review, they cannot obtain a meaningful remedy when a party refuses access, delays a response, provides an incomplete answer, or declines to correct inaccurate information.

In the political context, these rights are especially important. A party may hold information about a person's political views, perceived ideological leaning, demographic characteristics, issue interests, donation history, canvassing responses, neighbourhood profile, likelihood of voting, or responsiveness to particular messages. That information may shape whether and how a voter is contacted, targeted, excluded, profiled, or treated.

The current structure created by Bill C-4, and left largely intact by Bill C-25, moves in the wrong direction. It allows access and correction to depend on what a party chooses to include in its own privacy policy, rather than on rights guaranteed by statute. That leaves voters with weaker rights in relation to federal political parties than they often have in relation to businesses, public bodies, charities, non-profits, or other organizations that handle personal information.

That is inconsistent with the expectations reflected in the Ipsos polling. Large majorities of Canadians support access rights, correction or deletion rights, independent oversight, significant penalties for data breaches or misuse, and privacy rules for political parties that are comparable to those applying to other organizations. 15

FIPA recommends that Bill C-25 be amended to guarantee individual rights to:

- access personal information held by federal political parties;
- receive information about how that information has been collected, used, disclosed, retained, and transferred;
- request correction of inaccurate, incomplete, outdated, or misleading personal information;
- require annotation where a correction request is disputed;
- request deletion where information is no longer required or was improperly collected, used, or retained; and
- seek independent review of refusals, delays, incomplete responses, or inadequate corrections.

A privacy regime that denies enforceable access and correction rights is not a meaningful privacy regime. For voters, these rights are not administrative conveniences. They are the practical means by which individuals can understand, challenge, and control how political actors use information about them.

6. The Alberta elector-list substantiates a worst-case scenario

The recent Alberta elector-list incident should be treated as a concrete warning for Parliament.

15Ibid.

Elections Alberta stated on April 30, 2026 that it was taking seriously the unauthorized use of the Republican Party of Alberta's copy of the List of Electors by the Centurion Project Ltd. It emphasized that the Alberta *Election Act* governs the contents, distribution, protection, and use of the provincial List of Electors, and described the list as sensitive data.16

Elections Alberta further reported that it had obtained an ex parte emergent injunction from the Alberta Court of King's Bench and that the injunction required the respondents to identify every person or entity to whom the list, or any portion of it, had been provided or made accessible.17 As this situation unfolds reports are indicating that Elections Alberta may have known as early as March 31st but failed to act at that time leaving the data exposed.18

This is exactly the kind of cascade risk that enforceable privacy law can and must prevent.

Once voter information leaves an authorized environment, it can be copied, retained, merged, analyzed, transferred, or exploited. Even if a court orders removal or return, the practical reality is that digital data can be difficult or impossible to fully retrieve.

The potential harms are not limited to identity theft or fraud. Political data can be used to profile voters, target disinformation, suppress participation, intimidate individuals or communities, identify politically vulnerable groups, manipulate issue-based concerns, support foreign interference activity, and undermine confidence in democratic institutions.

Bill C-25's foreign-interference provisions must therefore be linked directly to political privacy. Foreign interference is not only about money, impersonation, or deceptive communications. It is also about access to data.

A hostile actor does not need to control an election system to influence voters. Access to voter data, political profiles, contact information, and behavioural inferences can be enough to enable targeted manipulation.

7. The real risk of significant harm threshold is too weak for political data

Bill C-25 creates breach notification obligations where there is a real risk of significant harm. That is an improvement over no breach notification duty at all. But it is not sufficient for political data.

The bill provides that relevant factors include the sensitivity of the personal information involved in the breach and the probability that the information has been, is being, or will be misused. It defines significant harm to include bodily harm, humiliation, damage to reputation or relationships, loss of employment,

16Elections Alberta, supra note 4.

17Ibid.

18 SCOOP: Jen Gerson: Elections Alberta's massive failure could have put people in danger. I tried to warn them. https://www.readtheline.ca/p/scoop-jen-gerson-elections-albertas?r=1ntoc8&triedRedirect=true

business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property. 19

That test places too much discretion in the hands of the party responsible for the breach. It asks the party to assess sensitivity, likelihood of misuse, and seriousness of harm. But the party may not know the full context of risk for affected individuals.

For political data, harm may be difficult to quantify in advance. It may not appear as immediate financial loss. It may appear as manipulation, targeting, exclusion, intimidation, reputational harm, chilling of political participation, or vulnerability to foreign influence.

FIPA recommends a lower and clearer breach-notification standard for political data. At minimum:

- all material breaches involving voter information, elector-list information, political opinions, inferred political views, party-support data, donor data, canvassing data, or voter-contact records should be reported to an independent privacy regulator;
- affected individuals should be notified unless the independent regulator determines notification is unnecessary;
- parties should be required to notify the regulator even where they believe the risk to individuals does not meet the significant harm threshold; and
- breach notices should identify what information was affected, when the breach occurred, who received or accessed the information if known, what mitigation steps were taken, and how individuals can exercise their rights.

8. The prohibition on sale is too narrow

Bill C-25 would prohibit the sale of personal information under a party's control. That is necessary. But it is too narrow. 20

Political data can be misused without being sold. It can be exchanged, licensed, pooled, matched, donated, transferred, uploaded, made accessible through shared systems, disclosed to aligned entities, or processed by vendors and consultants.

A prohibition on sale alone may leave the most important data flows untouched.

FIPA recommends that Bill C-25 prohibit unauthorized:

- disclosure;
- transfer;
- exchange;
- licensing;
- access;
- pooling;
- matching;
- sharing;

19Bill C-25, supra note 1, cl 36, adding ss 446.6(2)-(3).

20Ibid, cl 36, adding subpara 446.6(1)(j)(ii).

- publication;
- making available; and
- use for a purpose inconsistent with the original collection purpose.

The law should also make parties accountable for information transferred to third parties. Contractual safeguards are not enough unless they are backed by statutory duties, audit rights, breach reporting, enforcement, and remedies.

9. PROC should conduct dedicated study of the privacy provisions

PROC should conduct a dedicated study of Bill C-25's privacy provisions.

Bill C-4's political-party privacy provisions were studied in the context of a finance bill, despite their direct implications for democratic rights, privacy, elections, federalism, and public trust. That process was not adequate for provisions that attempted to displace provincial privacy protections and define the privacy rights of voters in relation to federal political parties.

Bill C-25 gives PROC an opportunity to correct course.

FIPA recommends that PROC hear from:

- the Privacy Commissioner of Canada;
- the Chief Electoral Officer;
- the Commissioner of Canada Elections;
- provincial and territorial privacy commissioners;
- constitutional and federalism experts;
- civil society organizations working on privacy, democracy, civil liberties, and digital rights;
- technical experts in political-data systems, voter relationship management platforms, microtargeting, and AI-enabled profiling; and
- representatives of federal political parties responsible for voter databases and privacy compliance.

A dedicated study would assist the Committee in determining whether Bill C-25 meaningfully protects voters, or merely improves the wording of a self-regulatory framework.

10. Recommended amendments

FIPA recommends that Parliament amend Bill C-25 as follows.

1. **Convert privacy-policy requirements into direct statutory duties**
   Federal political parties should be legally required to comply with substantive privacy obligations, not merely required to include language in their policies.
2. **Restore access and correction rights**
   Individuals should have enforceable rights to access, understand, correct, and challenge personal information held by federal political parties.
3. **Create independent privacy oversight**
   Federal political parties should be subject to oversight by the Privacy Commissioner of Canada or an equivalent independent privacy regulator with appropriate expertise, powers, and remedies.

4. **Create an individual complaint mechanism**
   Canadians should be able to complain to an independent privacy regulator about party collection, use, disclosure, retention, transfer, breach, denial of access, or refusal to correct personal information.
5. **Remove Bill C-4's provincial pre-emption and retroactivity provisions**
   Parliament should not retroactively eliminate provincial privacy rights without replacing them with a substantively equivalent or stronger federal regime.
6. **Lower the breach-notification threshold for political data**
   Political and voter data should be treated as inherently sensitive. Material breaches should be reported to an independent regulator and affected individuals, subject only to limited exceptions determined by that regulator.
7. **Broaden restrictions on data transfers**
   The law should prohibit unauthorized disclosure, exchange, licensing, pooling, matching, transfer, access, publication, or making available of personal information, not only sale.
8. **Strengthen third-party accountability**
   Parties should remain legally accountable for information handled by vendors, consultants, riding associations, candidates, volunteers, platforms, and other third parties.
9. **Require privacy impact assessments for high-risk practices**
   Privacy impact assessments should be required for voter profiling, microtargeting, AI-enabled inference, data matching, use of third-party datasets, and large-scale voter-contact systems.
10. **Require retention and deletion limits**
    Federal political parties should not retain personal information indefinitely. They should be required to justify retention, publish retention schedules, and securely delete information when no longer required.
11. **Create meaningful penalties and remedies**
    Penalties and remedies should reflect the sensitivity of the information, the number of affected individuals, whether the breach or misuse was preventable, whether the party delayed reporting, and whether the party failed to cooperate with oversight.

Conclusion

Bill C-25 is presented as legislation to strengthen Canadian democracy. FIPA supports that goal. But a democracy cannot be strengthened while voters' personal information remains subject to weak, self-regulatory rules.

The bill's privacy provisions are improvements at the margins. They are not a proper privacy regime. They do not provide direct statutory rights. They do not provide independent privacy oversight. They do not provide a meaningful complaint mechanism. They do not restore access and correction rights. They do not remove Bill C-4's provincial pre-emption. They do not fully address the risks created when political data is transferred, copied, matched, profiled, or misused.

The Alberta elector-list incident shows the stakes. Sensitive voter information can move from a political recipient to an unauthorized actor, trigger emergency legal intervention, and create uncertainty about who has accessed or received the data.

At the federal level, the risks are magnified by national party databases, voter relationship management systems, third-party vendors, predictive analytics, generative AI, and foreign interference threats.

Canadians expect political parties to play by the same privacy rules as everyone else. They expect access rights, correction rights, independent oversight, breach accountability, and meaningful safeguards. They expect Parliament to protect voters, not merely protect parties from scrutiny.

FIPA therefore urges the Committee to amend Bill C-25 so that it creates real privacy rights for voters and real accountability for federal political parties.

Respectfully submitted,

BC Freedom of Information and Privacy Association