CANADIAN BAR ASSOCIATION
ASSOCIATION DU BARREAU CANADIEN

May 29, 2026

Via email: PROC@parl.gc.ca

Mr. Chris Bittle, M.P.
Chair, Standing Committee on Procedure and House Affairs
Sixth Floor, 131 Queen Street
Ottawa ON K1A 0A6

Dear Mr. Bittle:

Re: 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 (Strong and Free Elections Act)

I am writing on behalf of the Canadian Bar Association's Privacy and Access Law Section (the CBA Section). We support Bill C-25's (the *Strong and Free Elections Act*) objective of strengthening electoral integrity and welcome its privacy-related amendments as a step toward greater accountability for federal political parties. However, in our view, the Bill does not address key structural gaps in the political party privacy regime, including the treatment of political data as sensitive, individual access and correction rights, and independent oversight.

The CBA is a national association of over 40,000 members, including lawyers, law students, notaries, and academics. Our mandate includes promoting the rule of law, improving access to justice, and advocating for effective law reform. The CBA Section comprises lawyers working in the public, private, and not-for-profit sectors across Canada with expertise in privacy, access to information, and data governance.

General Observations on Bill C-25

Bill C-25 amends a framework that does not adequately protect Canadians' right to see, correct, or independently challenge personal information held about them by the political parties that seek their votes. The privacy-related amendments to section 446.6, including security safeguards, breach notification, and transfer protections, are meaningful improvements. However, the CBA Section submits that these improvements, while welcome, do not resolve structural deficiencies embedded in the political party privacy regime enacted by the *Making Life More Affordable for Canadians Act*.[1] (Bill C-4). Bill C-25 builds upon an architecture that neglects to treat political opinion data as sensitive personal information, lacks independent oversight, and denies Canadians access and correction rights.

1 Bill C-4, **S.C.** 2026, c. 2.

The urgency of this work is not abstract. In late April 2026, a separatist group in Alberta publicly posted a searchable database of 2.9 million Albertans' names, home addresses, and phone numbers drawn from the provincial List of Electors. Alberta's own Privacy Commissioner confirmed her office has no jurisdiction over the political party that allegedly sourced the data, because the *Personal Information Protection, Act* in Alberta [2]does not apply to political parties. This is the structural gap the CBA Section is asking this Committee to close at the federal level, before the same failure occurs under the *Canada Elections Act*[3].

The following recommendations identify the four core areas which we suggest strengthen Bill C-25.

Recommendations

1. **The CBA Section recommends amending Bill C-25 to classify political opinion as sensitive personal information, subjecting it to proportionate consent and processing requirements consistent with international best practices.**
2. **The CBA Section recommends amending Bill C-25 to grant individuals explicit rights of access to, and correction of, personal information held by federal political parties, consistent with the Office of the Privacy Commissioner's 2019 Guidance for federal political parties[4].**
3. **The CBA Section recommends amending Bill C-25 to establish independent oversight of political party privacy practices by the Office of the Privacy Commissioner of Canada (OPC), rather than the Chief Electoral Officer.**
4. **The CBA Section recommends amending Bill C-25 to require political parties to provide transparency regarding the use of AI systems or automated decision-making for voter profiling and micro-targeting.**

The International Comparison: A Persistent Gap

The privacy regime applicable to federal political parties under the *Canada Elections Act* is an anomaly when measured against the standards adopted by comparable democratic states. The CBA Section is concerned that Bill C-25, while improving the mechanics of the self-regulatory framework, does not address this foundational gap.

Under the European Union's *General Data Protection Regulation* (GDPR)[5], Article 9 classifies data revealing political opinions as "special category" data. Processing this data is prohibited unless a specific exception applies, including the receipt of explicit consent. Similarly, the United Kingdom's Information Commissioner's Office (ICO) has issued dedicated "Guidance on Political Campaigning[6]" that treats political opinion data as sensitive, strictly regulates micro-targeting, and subjects political parties to ICO enforcement jurisdiction under the UK *Data Protection Act 2018*[7]. Registered UK parties may process political opinion data only where necessary for political activities, subject to a documented policy and an individual opt-out right.

---

2 SA 2003, c P-6.5.

3 S.C. 2000, c. 9.

4 Office of the Privacy Commissioner of Canada. (2019**). Guidance for federal political parties on protecting personal information:** see online.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data: online

6 Information Commissioner's Office (2021) *Guidance on the use of personal data in political campaigning*: online.

7 c. 12,: see online.

By contrast, the *Canada Elections Act*, even as amended by Bill C-25, does not classify political opinion data as sensitive. It imposes no heightened consent requirements for the collection or use of such data. The net result is that a Canadian voter's political beliefs, voting history, and demographic profile may be collected, used, inferred and retained by a federal political party under a self-certified privacy policy.

While the CBA Section recognizes the unique, constitutionally protected role that federal political parties play in Canadian democracy, requiring higher standards for the processing of sensitive data does not inhibit legitimate political communication. Rather, it protects voters from opaque profiling and unregulated micro-targeting. The UK and EU have reached the same conclusion without impairing democratic function.

The CBA Section recommends that the Committee consider whether the Bill should be amended to classify political opinion data as sensitive personal information, with proportionate consent and processing requirements, consistent with international best practices.

Erosion of Domestic Standards: The Access and Correction Void

The CBA Section submits that the most significant structural deficiency in the current political party privacy regime, namely, the denial of individual access and correction rights, is not addressed by Bill C-25 and creates a statutory paradox.

Bill C-25 introduces a definition of "significant harm" under subsection 446.6(3) and requires parties to notify affected individuals of a breach where there is a real risk of significant harm under paragraph 446.6(1)(g). However, subsection 446.4(2) of the *Canada Elections Act*, enacted by the *Making Life More Affordable for Canadians Act* (Bill C-4) and untouched by Bill C-25, explicitly exempts parties from granting access to, or correction of, personal information.

The above creates an untenable situation. It is incoherent that a Canadian voter only gains visibility into the data a political party holds about them after that data has been compromised. True privacy protection must be proactive (access), not merely reactive (breach notification). The breach notification right introduced by Bill C-25 is operationally undermined by the access denial embedded in the *Making Life More Affordable for Canadians Act.*

The CBA Section further notes that this gap is inconsistent with the OPC's own published guidance. The OPC's April 2019 Guidance for federal political parties explicitly encourages parties to grant individuals access to their personal information and the ability to correct inaccuracies as a best practice. Bill C-25 does not incorporate these recommendations and does not repeal or amend subsection 446.4(2).

This creates a two-tiered system of privacy rights for Canadians. Individuals generally have statutory rights to access and correct personal information held about them by commercial organizations. Federal political parties, by operation of the *Canada Elections Act*, are explicitly exempted from these individuals' rights. The result is that a Canadian's personal information held by their local grocery store is subject to stronger access protections than the same information held by a registered political party.

Consider a concrete example where a voter receives a breach notification under paragraph 446.6(1)(g) informing them that their personal information has been compromised. They want to know what the party holds: their inferred voting history, demographic segment, donation capacity score, or contact records. Under subsection 446.4(2), they have no right to ask. The breach notification tells them damage was done but they have no tool to assess the extent of it, correct errors in it, or know when it was compiled.

The CBA Section recommends that subsection 446.4(2) be repealed and that Bill C-25 be amended to provide individuals with a right of access to and correction of their personal information held by federal political parties.

Independent Oversight: The Annual Meeting Is Insufficient

Bill C-25 amends paragraph 446.6(1)(i) to require that a party's privacy officer attend at least one meeting per calendar year relating to the protection of personal information held by the Chief Electoral Officer. The CBA Section does not oppose this requirement but submits that it does not constitute meaningful independent oversight.

The Chief Electoral Officer is an officer of Parliament responsible for the administration of federal elections. The OPC is the independent statutory body with the mandate, expertise, investigative powers, and enforcement tools to oversee compliance with privacy obligations. While the Chief Electoral Officer is expertly positioned to monitor campaign finance and electoral fairness, the CEO does not possess the specialized technical infrastructure required to audit complex data architecture, algorithmic micro-targeting, or cybersecurity safeguards. That specific technical mandate belongs exclusively to the OPC.

The structural inadequacy of the current model is made plain by the contrast within Bill C-25 itself. The Bill simultaneously grants the Commissioner of Canada Elections significant new investigative powers for election law violations under section 510.002. Yet political party privacy practices continue to operate under a self-certification model: a party certifies its own compliance annually under section 407(1)(c) of the *Canada Elections Act*. There is no independent audit mechanism, no power of inspection, and no proactive enforcement framework. The OPC possesses investigative powers under both the *Privacy Act*[8] and the *Personal Information Protection and Electronic Documents Act*[9] (PIPEDA). The investigative reach has not been extended to the political party context.

The Alberta breach demonstrates where self-certification leads: a political party granting database access to outside vendors, no independent auditor with jurisdiction to intervene, and a Privacy Commissioner publicly acknowledging she cannot act.

The CBA Section recommends that Bill C-25 be amended to vest oversight of political party privacy practices in the OPC, with appropriate investigative and enforcement powers, including the power to receive and investigate complaints, conduct audits, and issue binding orders.

Transparency in AI Driven Campaigning

The CBA Section recommends that Bill C-25 be amended to require federal political parties to provide clear and meaningful transparency regarding the use of artificial intelligence (AI) systems or automated decision-making tools for voter profiling, sentiment analysis, and micro-targeting.

Modern political campaigning increasingly relies on sophisticated algorithms to process vast datasets, often referred to as "voter files", to predict voting intentions and deploy highly personalized messaging. Without explicit transparency requirements, these "black box" systems operate without public accountability, risking the spread of misinformation and the manipulation of democratic discourse.

---

8 R.S.C. 1985, c. P-21 see online.

9 SC 2000, c 5 see online.

The urgency of this recommendation is underscored by recent regulatory trends and the CBA's own advocacy. In recent submissions concerning AI and automated decision-making in Immigration Law, the CBA has argued that to align with democratic values, while safeguarding human rights, fundamental freedoms, and individual privacy the design and use of AI must respect transparency as a cornerstone of responsible AI[10]. The public must understand the capabilities and limitations of systems that impact their fundamental rights. The OPC's 2019 Guidance for federal political parties already encourages parties to inform individuals about the use of "inferences or predictions" made about them. As AI capabilities have accelerated since 2019, transitioning these best practices into a statutory requirement is essential for electoral integrity.

The CBA Section submits that requiring parties to disclose the use of such tools and provide a high-level explanation of how voter data is utilized by them, is a proportionate measure that enhances voter trust without hindering legitimate political communication.

Conclusion

The CBA Section supports the objective of Bill C-25 to strengthen Canada's electoral integrity framework. The privacy-related amendments to section 446.6 of the *Canada Elections Act* represent a meaningful step toward greater accountability for federal political parties in their handling of Canadians' personal information.

However, the CBA Section submits that these improvements do not cure the fundamental structural gaps in the political party privacy regime. Without the classification of political data as sensitive, access and correction rights, and independent oversight, the framework will continue to fall short of the standards Canadians expect and that comparable democracies have already adopted.

The CBA Section would welcome the opportunity to appear before the Committee to provide further assistance on these issues.

Yours truly,

(original letter signed by Julie Terrien for Christiane Saad)

Christiane Saad
Chair, Privacy and Access Law Section

---

10 CBA Submission, January 2025, online.