CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

SUBMISSION TO THE STANDING COMMITTEE ON PROCEDURE AND HOUSE AFFAIRS REGARDING BILL C-65, *AN ACT TO AMEND THE CANADA ELECTIONS ACT*

CANADIAN CIVIL LIBERTIES ASSOCIATION

Anaïs Bussières McNicoll | Director, Fundamental Freedoms Program and Interim Director, Privacy, Technology and Surveillance Program

Noa Mendelsohn Aviv | Executive Director and General Counsel

Timilehin Ojo | Privacy Coordinator

NOVEMBER 26, 2024

Canadian Civil Liberties Association
124 Merton St., Suite 400
Toronto, ON M4S 2Z2
Phone: 416-363-0321
www.ccla.org

Overview

The Canadian Civil Liberties Association ("CCLA") is an independent, national, nongovernmental organization that was founded in 1964 with a mandate to defend and foster the civil liberties, human rights, and democratic freedoms of all people across Canada. Our work encompasses advocacy, research, and litigation related to the criminal justice system, equality rights, privacy rights, and fundamental freedoms. Working to achieve government transparency and accountability with strong protections for personal privacy lies at the core of our mandate.

The right to privacy protects people's ability to keep their personal information and private life out of the public domain. This right is essential to the protection of our autonomy, dignity, and personal identity. Privacy is also a gateway right to all other fundamental rights. This means that without a robust protection of the right to privacy, all other rights suffer. For instance, privacy is integral to ensuring the integrity of—and public trust in—democratic processes such as elections. Privacy is thus nothing short of a cornerstone of our democracy.

In this submission, CCLA speaks to Bill C-65, *An Act to amend the Canada Elections Act* ("Bill"). While this Bill has a broad scope and introduces amendments related to several areas of the *Canada Elections Act* ("Act"), CCLA's submission focuses on sections 68, 69 and 71 of the Bill, which create new statutory requirements for federal political parties collecting individuals' personal information.

CCLA's overarching position is that federal political parties, like everyone else in Canada, must respect people's privacy rights. Unfortunately, this Bill falls unacceptably short in this regard, as it fails to subject federal political parties to basic and well-accepted privacy standards and duties already enshrined in other federal and provincial regimes. Through a series of seven recommendations detailed below, CCLA is urging the Standing Committee on Procedure and House Affairs to amend this Bill to ensure that federal political parties dealing with personal information are bound to transparency, accountability and statutory compliance.

Privacy Rights Issues

Privacy is a fundamental human right recognized both domestically and internationally through various frameworks.[1] In Canada, specific privacy protections are embedded in domestic laws, including the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[2]. This law establishes essential safeguards protecting individuals' personal information by regulating how it is collected, used, stored, and disclosed.

Unfortunately, to date, Parliament has chosen not to explicitly subject federal political parties to this legislation. Several federal political parties also refuse to accept that they can be bound by provincial privacy laws, and are appealing a recent court decision in this regard.[3]

Voters have a right to privacy. Federal political parties should not be allowed to collect, use, store and disclose personal information about individuals without being subject to basic, yet robust, privacy principles. Bill C-65, as the federal government's claimed response to this issue, is outright insufficient.

This Bill essentially requires that each federal political party (and their representatives) comply with a self-drafted policy on the protection of personal information.[4] The Bill lists a series of requirements that must form part of this policy.[5] Unfortunately, these requirements fail to implement several key privacy standards detailed below.

A. Necessity of the Collection

The necessity standard ensures that only the personal information that is strictly required for the collection's intended purpose is collected, reflecting a fundamental principle of data minimization. This principle protects individuals from overreach, unnecessary data retention, and potential misuse of their personal information, whether accidental or intentional.

Most federal and provincial regimes in Canada already set necessity as the threshold for collecting personal information.[6] These laws limit the scope of data collection to what is necessary for a specific and legitimate purpose. The Bill's failure to incorporate any substantial data minimization requirement purports to grant broad discretion to federal political parties in deciding what data they can collect.

Recommendation 1: Amend the Bill to provide that federal political parties' collection of personal information shall be limited to what is reasonably necessary for the purpose of the collection.

---

[1] Privacy is safeguarded under various international covenants such as the Universal Declaration of Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), and regional agreements like the European Convention on Human Rights (Article 8). These instruments underscore the essential nature of privacy in protecting individuals from unwarranted intrusion by governments, organizations, or other entities.

[2] S.C. 2000, c. 5.

[3] *Liberal Party of Canada v The Complainants*, 2024 BCSC 814; Ontario Court of Appeal File No. CA49939.

[4] Bill C-65, s. 71, amending the Act to add s. 444.3.

[5] Bill C-65, s. 71, amending the Act to add s. 444.4(1).

[6] For example, PIPEDA's principle 4 requires that collection of personal information shall be based on what is necessary for the purpose of collection (s. 3 & 5(3) of PIPEDA; Clause 4.4 of Schedule 1, PIPEDA). British Columbia's *Personal Information Protection Act*, SBC 2003, c. 63 ("BC's PIPA"), only allows organizations to collect personal information that is reasonably necessary (s. 11, 14, & 17 of BC's PIPA).

B. Purpose for Collection

Under existing Canadian privacy regimes, regulated entities are obligated to establish clear, well-documented purposes for collecting personal information at or before the point of collection.[7] This ensures transparency with individuals whose data is being handled.

If the collected data is to be used for a new purpose that was not previously identified, regulated entities are usually required to notify the individual concerned and obtain their consent.[8] This standard is crucial in ensuring that personal data is not repurposed for unauthorized uses.

The Bill is, at best, vague regarding this standard. It does not demand that federal political parties provide clear, detailed justifications on the reasons why personal information is being collected, nor does it limit political parties' ability to use this information for additional purposes without further consent.[9]

***Recommendation 2*:** Amend Bill C-65 to require federal political parties to provide clear, detailed explanations of all purposes for which personal information is collected, used, and disclosed.

C. Consent

One of privacy law's foundational principles is that individuals must provide informed consent before their personal information is collected, used or disclosed by a third party. Informed consent means that individuals understand the purposes for which their personal information will be collected, used, or disclosed. Such consent should also clearly be revocable at any time.[10]

While the Bill introduces certain obligations on federal political parties to provide information about their data practices,[11] it lacks comprehensive provisions requiring that they obtain informed consent. The absence of such a requirement leaves room for ambiguity in how federal political parties handle individuals' data. This undermines transparency and diminishes individuals' control over their personal information.

Recommendation 3: Amend the Bill to require explicit consent for the collection, use, and disclosure of personal information. Ensure that consent is informed, not obtained through deception, and that individuals are informed and allowed to withdraw consent easily.

D. Openness and Access

Openness and access help ensure transparency and accountability in the handling of personal information. For instance, under PIPEDA, individuals have the statutory right to be informed of how their personal data has been used and disclosed.[12] They may request access to this data, and, subject to specific exceptions, regulated entities are required to provide accounts of its usage and of any third-party disclosure.[13] PIPEDA also allows individuals to request

[7] See for instance Clause 4.2.1 of Schedule 1, PIPEDA; s. 10 of BC's PIPA.
[8] Clauses 4.2.4, 4.5.1 of Schedule 1, PIPEDA.
[9] Bill C-65, s. 71, amending the Act to add s. 444.2 and 444.4(1) (c) and (h).
[10] Clause 4.3 of Schedule 1, PIPEDA.
[11] Bill C-65, s. 71, amending the Act to add s. 444.4(1)(c), (d) and (j).
[12] Clause 4.9 of Schedule 1, PIPEDA.
[13] Clauses 4.9, 4.9.1, and 4.9.3 of Schedule 1, PIPEDA.

corrections if their personal information is inaccurate or incomplete.[14] This ensures data accuracy, and protects individuals from harm caused by incorrect information.

The Bill fails to explicitly impose similar obligations on federal electoral parties. This omission limits transparency and accountability in how federal political parties handle personal information, and weakens individuals' control over their personal data.

Recommendation 4: Amend the Bill to provide for a right to be informed of the retention, use, and disclosure of personal information, as well as a right to access and request the correction of this personal information.

E. Retention and Secure Disposal

Another key privacy principle is that personal information should not be retained longer than necessary for the purpose for which it was collected. Upon the expiration of this period, personal information must be destroyed or anonymized. These safeguards help ensure data minimization and protection from privacy breaches and misuses (both accidental and intentional). The Bill fails to address this principle, contrasting with established privacy laws that include clear retention guidelines.[15]

Recommendation 5: Amend the Bill to include retention and secure destruction policies that align with best practices.

F. Training

Canadian privacy laws usually require that organizations train staff to comply with data protection protocols. Effective privacy management includes ensuring that employees and any relevant individuals are fully trained on their legal obligations and the security practices they must follow to safeguard personal data.[16]

Unfortunately, the Bill falls short from requiring robust standards for such training, and merely requires political parties to *describe*, in their policy, the training provided to employees and volunteers.[17] This vague obligation leaves a significant gap in ensuring that those handling sensitive personal information within federal political parties are adequately prepared to protect it.

Recommendation 6**:** Amend the Bill to require comprehensive training on data protection practices (with regular updates) for all employees and volunteers who handle individuals' personal information.

---

[14] Clause 4.9.5 of Schedule 1, PIPEDA

[15] PIPEDA mandates that personal information be retained only as long as necessary for the fulfillment of its purpose. Organizations must establish minimum and maximum retention periods and retain information that is subject to a request long enough for individuals to exhaust any recourse available to them. When no longer needed, personal information must be destroyed, erased, or anonymized. See Clauses 4.5, 4.5.2, and 4.5.3 of Schedule 1, PIPEDA.
Under s. 35 of BC's PIPA, organizations must retain personal information used to make a decision affecting an individual for at least one year, ensuring the individual has an opportunity to access it. Once the information is no longer required for legal or business purposes, it must be destroyed or anonymized.

[16] Clause 4.1.4 of Schedule 1, PIPEDA.

[17] Bill C-65, s. 71, amending the Act to add s. 444.4(1)(e).

G. Lack of Regulatory Oversight

The Bill tasks the Chief Electoral Officer with reviewing each party's privacy policy, receiving a statement certified by each party's privacy officer that "the party complies with its policy", and meeting with each party's privacy officer once a year.[18] The Bill leaves it to each political party to designate an internal privacy officer to be tasked with the responsibility of ensuring compliance with the party's privacy policy,[19] and does not require federal electoral parties to proactively report privacy breaches to an independent regulator.

This means that policy implementation and privacy breaches will not be subject to meaningful and independent monitoring and oversight. As a result, each federal political party will essentially be left to self-monitor on these issues.

When the same body is tasked with both creating and enforcing its very own policies, there is an inherent risk of bias, lack of transparency, and weakened oversight, as the entity is effectively policing itself. Recent years have shown that reliance on self-regulation is inadequate and risky. The 2018 Facebook-Cambridge Analytica data scandal revealed how self-regulation failed to protect user data, resulting in significant privacy breaches and loss of public trust.[20] Similarly, the 2017 Equifax data breach exposed vulnerabilities in self-regulatory practices, leading to the unwanted disclosure of millions of individuals' personal information.[21]

To build trust and ensure consistency across all political parties, it is critical that the Bill incorporate an external and independent oversight framework typically seen in Canadian privacy laws that will enforce compliance and ensure meaningful accountability.[22]

***Recommendation 7**:* Amend the Bill to establish an independent oversight mechanism to monitor, investigate and enforce compliance of all political parties with the Act.

Conclusion

The CCLA is urging the Standing Committee on Procedure and House Affairs to amend this Bill so that federal political parties are explicitly and unquestionably subject to a robust and effective national regime protecting the personal data they process.

---

[18] See Bill C-65, s. 68 and s. 71.

[19] Bill C-65, s. 71, amending the Act to add s. 444.4(1).

[20] Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, April 25, 2019, online at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/.

[21] Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information, April 9, 2019, online at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/.

[22] PIPEDA, for instance, is enforced by the Office of the Privacy Commissioner of Canada, which provides independent oversight and can investigate complaints, conduct audits, and make binding recommendations (see s. 10.1 (1), 11(1), 12(1), PIPEDA).
BC's PIPA similarly designates the Office of the Information and Privacy Commissioner for British Columbia as responsible for ensuring compliance and imposing penalties on organizations that fail to protect personal data (see s. 36 and 46 of BC's PIPA).
Both PIPEDA and BC's PIPA provide clear mechanisms for holding organizations accountable for breaches of privacy standards, ensuring that failures will be met with financial consequences.