Open Season on Personal Information: Report on Federal Political Parties' Privacy Policies

OpenMedia

15 April 2024

Kate Winiarz, JD Candidate, University of Ottawa Faculty of Law

Table of Contents

Executive Summary

In December of 2019, three residents of British Columbia submitted complaints to the Office of the Information and Privacy Commissioner of British Columbia (OIPC BC). The residents complained that four federal political parties' responses to their requests for information about how their personal information was being used and disclosed was inadequate under the requirements of BC's privacy law, the Personal Information Protection Act (PIPA).[1] Three parties, the Liberal Party of Canada (Liberal), the Conservative Party of Canada (CPC), and the New Democratic Party of Canada (NDP), took the position that PIPA did not apply to them, arguing that applying the provincial law to federal political parties would be unconstitutional.[2]

The OIPC BC found in 2022 that PIPA can apply to federal provincial parties.[3] The crux of the decision was that, in the absence of a single national, uniform, and complete privacy regime for federal political parties, BC's provincial privacy law applied to their activities.[4] In April of 2022, all three political parties applied for judicial review of the OIPC's decision.

While awaiting review of the decision, in June of 2023 the Liberal government passed Bill C-47 – a budget bill that contained an amendment to the *Canada Elections Act* tucked in at section 680. The amendment declared the privacy policy provisions under the *Canada Elections Act* to constitute the "national, uniform, exclusive and complete regime applicable to registered parties and eligible parties respecting their collection, use, disclosure, retention and disposal of personal information."[5]

Essentially, C-47 was an attempt to exempt federal political parties from BC's provincial privacy law and subject them only to their own privacy policies, written and published by the parties themselves. All policies must include certain elements in them, which the current federal policies already do, but that is the only requirement. There is no oversight of this framework.[6] Federal political parties quite literally write their own privacy rules, and have no penalties if they breach them. This creates massive privacy deficits for Canadians whose data is collected, used, and disclosed without any real applicable legal framework.

---

[1] *Conservative Party of Canada (Re)*, 2022 BCIPC 13 at paras 3-4, online: *CanLii* <https://canlii.ca/t/jmzsq>.
[2] *Ibid* at para 5.
[3] *Ibid* at para 208.
[4] Bill C-47, *Budget Implementation Act 2023 No 1*, 1st Sess, 44th Parl, 2023, cl 680.
[5] *Canada Elections Act*, SC 2000 c 9 at s 385.2(3).
[6] Senate of Canada, *Standing Senate Committee on Legal and Constitutional Affairs*, *Evidence*, 44-1, (2 May 2023) at 54:2 (Stéphane Perrault), online: <https://sencanada.ca/content/sen/committee/441/lcjc/54ev-56175.pdf> [C-47 Senate Study].

Since these policies are ostensibly the legal framework that federal political parties follow, it's important to compare them to federal and provincial privacy laws. This report analyzes the privacy policies of the five major political parties: the Liberal Party of Canada (Liberal Party), Conservative Party of Canada (CPC), the Bloc Québécois (Bloc), the New Democratic Party of Canada (NDP), and the Green Party of Canada (Green Party). Our analysis found that, if operating under their own privacy policies and exempt from any provincial or federal privacy law, federal provincial parties have given themselves permission to collect any type of personal information, in almost any way, with no oversight or penalties for breach. The legal compliance section of this report assesses compliance with BC's *Personal Information Protection Act* (*PIPA*) and Canada's federal private-sector privacy law, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), through the Office of the Privacy Commissioner's guidelines issued to federal political parties. Analysis found that the parties' policies alone (even without any evidence of practices) violate several essential privacy principles and laws, namely in the area of informed consent.

Further, we assessed the transparency and comprehensiveness of the policies as very low. While all policies contained illustrative examples of information they collect and how they collect it, each of those illustrative lists were all open-ended. This means that, despite a list of examples, parties are able to collect any information they please. All privacy policies are also written at a college or college graduate level, making them inaccessible to many Canadians.

Bill C-65, introduced on March 20th, 2024, is not yet in force, but would put some additional obligations on federal political parties for the protection of personal information, but they still do not meet the standards of either federal or provincial privacy law. While the Bill is an improvement on the status quo by introducing monetary penalties when parties violate their privacy policies, it still lacks oversight by a privacy office and does nothing to ensure parties get individuals' consent to collect their personal information.

Canadians deserve better than this. This report recommends that federal political parties handle personal information in line with Canadian privacy law, either by incorporating adequate privacy principles and oversight directly into the *Canada Elections Act*, or by clearly subjecting parties to existing federal privacy law. These recommendations echo ones from Senate study of federal political parties' privacy

compliance at the ETHI Committee,[7] the Office of the Privacy Commissioner (OPC),[8] and the Chief Electoral Officer.[9] Gaps in compliance with privacy law can be remedied by oversight of the political parties' personal data practices by the OPC and penalties for non-compliance with the parties' privacy policies.

To create this report, the privacy policies of each of the five major federal political parties that was active as of March 1, 2024 were analysed.[10] To note, the Bloc's policy is not called a privacy policy, but instead a policy on the protection of personal information. This is the most accurate description of all five policies: They do not centre on individuals' privacy rights, but instead on how political parties handle information once they already have it by any means they like.

Section I: Data Handling Practices for Personal Information

Personal information is defined in all parties' privacy policies as information about an identifiable individual. The types and methods of collection of personal information are all virtually unlimited under the parties' privacy policies. Parties also collect "non-personal" information through cookies on their websites. No information is given as to whether this non-personal information is simply de-identified or actually anonymous, or if it can be combined with personal information in a way that can identify an individual.

i. What types of information do parties collect?

All five political parties' privacy policies use open-ended, non-exclusive lists when describing the types of information that the parties collect. This open-endedness means that when left to the terms of their own policies and not subject to privacy laws, political parties can lawfully collect any personal information they like, no matter how sensitive.

---

[7] House of Commons, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly: Report of the Standing Committee on Access to Information, Privacy, and Ethics* (December 2018) (Chair: Bob Zimmer), at 25, online (pdf): <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf > [ETHI Study].

[8] C-47 Senate Study, *supra* note 6 at 54:22 (Philippe Dufresne).

[9] *Ibid* at 54:3 (Stéphane Perrault).

[10] Archived links to the May 1, 2024 versions of the privacy policies: Liberal Party of Canada: <https://web.archive.org/web/20240405222107/https://www.liberal.ca/privacy/>; Conservative Party of Canada: <https://web.archive.org/web/20240301100731/https://www.conservative.ca/privacy-policy/>; Bloc Québécois: <https://web.archive.org/web/20240202063548/https://www.blocquebecois.org/politique-de-protection-des-renseignements-personnels/>; New Democratic Party of Canada: <https://web.archive.org/web/20240405122044/https://www.ndp.ca/privacy>; Green Party of Canada: <https://web.archive.org/web/20240406204413/https://www.greenparty.ca/en/privacy>.

All parties give illustrative examples of the types of information they collect, listed in Table 1 below. But, when coupled with the open-ended language in each party's policy, each illustrative list is essentially meaningless. Table 2 shows the open-ended language used by each party. The use of language is akin to saying "The information we collect includes but is not limited to: Name, address, and phone number." The reality of this language is that, while political parties have provided illustrative lists, without guardrails of privacy law, they are free to also collect personal information on ethnicity, religion, age, sexuality, and anything they might like to have.

Table 1: *Illustrative examples of data collected by political parties*

Information collected declared by all parties	Information collected declared by some parties	Information collected declared by only one party
● Name ● Address ● Email ● Telephone ● Donation information ● Financial information ● Any other information voluntarily shared with the party ● Non-personal information via cookies	● Social media contacts (Liberal, Bloc, Green) ● Political views (CPC, Green) ● Voting preferences (CPC, Liberal, Green)	● Language preferences (CPC) ● Residence (CPC) ● Family members (CPC) ● Issues that individuals communicate with the party about (Liberal) ● Demographic information (NDP)

Table 2: Open lists: types of personal information collected, by party

CPC	"Personal information" is information about an identifiable individual. It **includes** personal contact information that we collect **such as** an individual's name, address, email address and telephone number. We **may also collect information** regarding … [list of examples]... **and other information you choose to share with us."**
Liberal	"The information we collect **may include**… [list of examples]"
NDP	"Personal information" is information about an identifiable individual. It **includes information such as**… [list of examples].
Bloc	"Les renseignements retenus **peuvent inclure**: … [list of examples]...

	Toute information que vous partagez volontairement avec nous au cours de diverses campagnes. English: “Information retained **may include**… [list of examples]... **Any information that you voluntarily share** with us...”
Green	“The information we collect **may include**… [list of examples]”

ii. How the parties collect personal information

Political parties collect information in two broad ways: From the List of Electors provided by Elections Canada, and through the party’s data collection efforts, described below.

All political parties are eligible to receive the List of Electors from the Chief Electoral Officer.[11] This is reflected in all privacy policies of the five political parties. The list, which contains personal information like names and addresses of voters, may not be used for any purpose other than to communicate with electors.[12] The purpose of communication can include soliciting for donations or recruiting members of their party. Notably, provincial political parties have been found to merge information from the list of electors with information collected from other sources, like canvassing, social media, etc.[13] This information has then been used by some provincial political parties to create new information, such as voter profiling and scoring.[14] While there is no confirmation that federal provincial parties engage in this behaviour, if evidence were raised that the list of electors were being used in this way, it could constitute a violation of the terms of the *Canada Elections Act*.[15]

Similar to the *types* of information that parties collect, all five political parties have chosen to use open-ended language in their policies on how they may collect any other personal information. The policies all mention that they collect information that is “publicly available.” This term is well-defined under existing privacy laws, such as PIPEDA and PIPA, but without the formal guardrails of those statutes, parties are free to define what publicly available means. Under legal considerations below, this report addresses the difficulty in defining what is and is not “publicly available” information when no privacy laws apply.

---

[11] *Canada Elections Act*, *supra* note 5 at s 93(1).
[12] *Ibid* at 110(1.1).
[13] British Columbia, Office of the Information and Privacy Commissioner, “Investigation Report P19-01, Full Disclosure: Political parties, campaign data, and voter consent” (6 February 2019) at 14, online (pdf): <https://www.oipc.bc.ca/documents/investigation-reports/2156> [OIPC Report].
[14] *Ibid* at 22.
[15] *Canada Elections Act*, *supra* note 5 at s 485(1), s 56(e), s 110 & s. 500(3).

Much of the open-endedness of how political parties collect personal information stems from the understanding of the words "publicly available." For example, at the provincial level, the British Columbia New Democratic Party and Liberal Party were found to be collecting data on individuals' ethnicity, gender, and religion without their consent.[16] Ethnicity, gender, and religion, by BC's PIPA, are sensitive information and can only be collected with the consent of the individual.[17] If PIPA does not apply, as federal parties would prefer, canvassers and other party representatives may simply observe the "publicly available" information of someone's perceived ethnicity, gender, or religion, they are free to collect it.

Table 3: How political parties declare they collect information

Collection methods declared by all parties	Collection methods declared by some parties	Collection methods declared by only one party
● Online forms ● List of electors ● Signing petitions ● From publicly available sources ● From donations ● From memberships ● From event registrations ● In-person canvassing ● Non-personal information via cookies ● Phone calls	● Personal information about an individual provided by their friend or a volunteer (third parties can provide personal information without that individual's consent) (Liberal, Green) ● Through social media accounts or contacts (Liberal, Bloc, Green)	● Text messages (Liberal)

Table 4: Open lists: how personal information can be collected, by party policy

Liberal	"We also collect information from **publicly available** data sources, and through voter outreach activities, **such as** [list of examples]… We also obtain other information that you choose to give us. You may do so in a variety of ways, **including**: … [list of examples]"
CPC	"We may also collect personal information from **publicly available data** or sources… You may also choose to provide us with personal information on a voluntary basis, **such as**.. [list of examples]"

[16] OIPC Report, *supra* note 13 at 15-16.
[17] *Ibid*.

Bloc	"Nous recueillons également certaines informations **déjà publiques comme** [liste d'exemples] et nous en collectons également lors d'activités **comme** [liste d'exemples]." English: "We also collect certain information that is **already public**, **such as** [list of examples], and we also collect it during activities **such as**… [list of examples].
NDP	"We also collect certain information that is **already public**, **such as** [list of examples], and we also collect it during activities **such as**… [list of examples]."
Green	"We also collect information from **publicly available** data sources … and through voter outreach activities, **such as** [list of examples]… We also obtain other information that you choose to give us. You may do so in a variety of ways, **including**: [list of examples]"

ii. How the parties use personal information in their control

The lists of how the parties use the information are, however, some of the only closed lists that exist in the parties' policies, which satisfies privacy laws as long as they are not violating those policies in practice. Without investigative powers that stem from oversight by a privacy body like the Office of the Privacy Commissioner or British Columbia's Privacy and Information Commissioner (BC OIPC), evidence on how parties actually use personal information is either anecdotal or based on speculation.[18]

Under PIPEDA , the uses in Table 5 should be the only uses that any information the party collects is used for.[19] However, evidence from the BC OIPC suggests that provincial political parties in BC may already be using personal information to create voter profiles and scores.[20] The parties then use that new information to micro-target voters online. Use for voter profiling and/or scoring would be a violation of privacy law, and even of the parties' own policies. Unfortunately, even if parties were found to be using their collected data for undeclared purposes, because there is no oversight attached to the *Canada Elections Act* on protection of personal information, there is no recourse for individuals whose information is used for another purpose, and no penalty for parties that are misusing it.

[18] Sara Bannerman et al, "Privacy and Canadian Political Parties: The Effects of the Data-Driven Campaign on Elector Engagement" (2022) 55 Canadian Journal of Political Science 973 at at 876-877, online: <doi:10.1017/S000842392200066X>.
[19] Personal Information Protection and Electronic Documents Act, SC 2000 c 5 at Schedule 1 s 4.3.1 [PIPEDA].
[20] OIPC Report, *supra* note 13 at 23.

Table 5: How parties use personal information in their control

Uses of information declared by all parties	Uses of information declared by only one party
● Communication with voters, donors, volunteers, and members ● Fundraising ● Sent to third party services like hosting, processing donations, etc ● Shared with provincial/territorial offices and boards	● Google Ads (CPC)

All parties' policies feature a statement on the sale of information that the party holds. Two parties state that "under no circumstances is *any* information sold" (Liberal and Bloc), whereas two other policies state that no *personal* information is sold (NDP, Green). This is an important distinction, since all political parties state that they collect non-personal information via website cookies. By the wording of their policies, the NDP and Green party policies leave it open to sell cookie information that they view as non-personal.

iv. Measures in place to ensure data security and prevent unauthorised access.

The measures in place to protect personal information by each political party were vague but adequate for Canadian privacy law purposes. Some noted that servers were located in secure environments, some identified encryption, others noted that physical records are kept in locked cabinets. While there does need to be flexibility and some opacity in privacy policies to meet changing security needs, information on the parties' policies is sparse.

Only one party made any mention of procedures that the party will follow in the case of a breach of personal information, the NDP. Inclusion of this type of information would be a requirement under Bill C-65, if it passes.[21]

Section II: Assessing transparency and readability

Transparency and comprehensiveness

All five privacy policies lack transparency and comprehensiveness. Every single federal political party has an open-ended list of the types of personal information they collect

[21] Bill C-65, *Electoral Participation Act*, 1st Sess, 44th Parl,2024, cl 71, 444.4(1)(g).

and how they collect it in their privacy policies. The parties tend to use an illustrative list of examples of types of information they are collecting, accompanied by a word like "includes", which is to be read as "includes but is not limited to." Even when presenting what appears to be a transparent illustrative list, each party still allows itself to step out of that illustrative list and collect other unknown information. This lacks transparency at the most basic and fundamental level.

This means that, while there are differences between each individual privacy policy's illustrative examples of information they collect, the types of information the parties gather is virtually unlimited without the guardrails of a comprehensive privacy law. One party noting that they collect social media information and another one not noting that means nothing. These are essentially policies to waive application of privacy law and give permission to act as parties please with personal information. For ranking of parties' performance later in this report, all parties receive the same score of zero.

Readability and Clarity

Readability of privacy policies is essential for individuals to be able to provide informed consent. Canadians can vote by the age of 18, meaning that many voters will not yet have attended post-secondary institutions. While 57.5% of Canadians 25-64 have graduated from some level of post-secondary education, 42.5% have not.[22] Not to mention Canadians aged 18-24, who are unlikely to have completed post-secondary education.

To conduct a uniform and unbiased assessment of each party's clarity and readability, this report uses the Flesch-Kincaid scoring system. This system assesses the readability of a work based on sentence length and number of syllables per word. It uses a 0-100 rating system. A lower score means a piece is more difficult to read, and a higher score means a piece is easier to read. Scores between 1-30 register as college graduate-level reading. 30-50 is best suited to readers with some level of college education, and 50-60 corresponds with the readability associated with those with a 10th-12th grade reading level.

To be accessible to the general public and be considered plain english, a score of 60 is the goal.[23] No party's privacy policy comes close to that. All privacy policies came in between a score of 24-35, as shown in Table 6. That said, social media privacy policies

[22] Statistics Canada, "Education - 2021 Census promotional material" (Accessed 11 April 2024), online: *Statistics Canada* <https://www.statcan.gc.ca/en/census/census-engagement/community-supporter/education>.
[23] Irene L, "It's not you; Privacy Policies Are Difficult to Read" (17 July 2018), online: *Common Sense* <https://www.commonsense.org/education/articles/its-not-you-privacy-policies-are-difficult-to-read>.

have been found to have very low mean Flesch-Kincaid scores of approximately 12.[24] That's a college graduate level that is even more difficult to read than any Canadian political party.

Canadian political parties are performing better than social media policies, but still have a long way to go to be readable as basic English (or French). They should all aim for a readability score of approximately 60 if they hope to be accessible to the majority of voting Canadians.

Table 6: privacy policies ranked from most-to-least readable

	Green	Liberal	NDP	CPC	Bloc
Flesch-Kincaid score	35 (college level)	35 (college level)	31 (college level)	24 (college graduate level)	N/A*
Words in privacy policy	1103	1284	934	967	1155

**The Bloc's policy is the only one that is available in only one language: French. The Flesch-Kincaid score is tailored to the structure of the English language, meaning that the readability score is unreliable in French. The Bloc's policy reads somewhere between the Liberal and CPC policies, but without a standard measure, their score has been omitted.*

Section III: Legal Compliance

None of Canada's five federal political parties are complying with established privacy laws in Canada. Of the ten privacy principles that guide PIPEDA, we estimate that political parties fail to meet at least six - and possibly more.

This illustrates that the provisions requiring federal political parties to publish privacy policies under the *Canada Elections Act* are completely insufficient. They allow parties to bypass the norms of both federal and provincial privacy laws despite obvious violation of multiple privacy law principles. While the policies need to contain certain information (types of information collected, how it's collected, how it's protected, etc), the use of open lists and indefinite policies provide essentially no guardrails - the very thing laws are supposed to do.

[24] Swarndeep Singh et al, "Assessment of App Store Description and Privacy Policy to Explore Ethical and Safety Concerns Associated with the Use of Mental Health Apps for Depression" (2023) 45(2):173 Indian Journal of Psychological Medicine 173 at 175.

Based on the OPIC's 2019 decision, British Columbia's PIPA applies to federal political parties, though appeals are proceeding.[25] Both Canada-wide privacy laws, *PIPEDA* and the *Privacy Act*, do not apply to federal political parties at this time.

Method of assessing federal political parties' privacy policies
In response to the lack of enforcement and oversight of federal political parties' privacy practices, the Office of the Privacy Commissioner recommended ten principles for privacy best practices.[26] These ten principles would ensure parties stay in line with privacy law domestically and internationally. Of those ten principles, federal political parties' policies each fail six – accountability, identifying purposes, consent, limiting collection, openness, and challenging compliance. These failures centre on lack of informed consent stemming from vague policies full of open-ended lists in ways that violate both PIPA and PIPEDA.

Three of the ten categories (limiting use, disclosure, and retention; accuracy; and individual access) may be violated based on practices of the parties, but this can't be confirmed without investigative powers into party practices. All five parties' policies fulfill exactly one principle: Safeguards. That is to say, their privacy policies say enough about safeguarding information under their control to satisfy this element.

A full analysis of each party's compliance with the OPC's privacy principles is contained in Appendix A. The following are the glaring issues from the parties' privacy policies that are at the root of the violation of the principles.

i. On consent to collect information

Offenders: Liberal, CPC, Bloc, NDP, and Green parties
Privacy laws breached: PIPEDA, PIPA
All of Canada's relevant privacy laws require informed consent of the individual at or before the time of collection.[27] Informed consent in both Acts requires that individuals understand the purpose information is being collected for, how the information is being collected, what is being collected, and that only the information necessary is being collected.

All five political parties allow themselves to collect any information at all, through nearly any means, and share it with nearly any third party through the use of open lists. This complete lack of transparency means that even if a user reads the party's privacy policy,

[25] *Conservative Party of Canada (Re)*, *supra* note 1.
[26] Office of the Privacy Commissioner of Canada, "Guidance for federal political parties on protecting personal information" (1 April 2019), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/>.
[27] *PIPEDA*, *supra* note 19 at 6.1; *Personal Information Protection Act*, SBC 2003 C 63 at s 6-7 [*PIPA*].

it's possible that their personal information will be collected, used, and disclosed in ways that they did not consent to.

ii. On third parties providing personal information without consent

Offenders: Liberal and Green parties
Privacy Laws breached: PIPA[28], PIPEDA[29]
Both the Liberal and Green privacy policies list that the party collects "other information that you choose to give us," followed by a list. Within the list for both parties is a bullet point stating that "[i]t is also possible that your information could be provided to us by a volunteer or friend who thinks you would be interested in getting involved." This is contrary to the letter of our privacy laws. PIPA and PIPEDA both only allow collection without consent of the individual in cases where it is required by law.[30] Collection from a friend or volunteer violates both laws. Given that provincial political parties have been found to be collecting personal information by purchasing it from third party data brokers.[31] This kind of third party door in an open list in a privacy policy is even more worrisome.

iii. On social media contacts and publicly available information

Offenders: Liberal, Bloc, and Green parties
Privacy laws breached: *PIPA*, *PIPEDA*
All five parties declare that they collect information from "publicly available sources." Under *PIPA* and *PIPEDA*, the term "publicly available" has a very specific interpretation.[32] It does not simply mean that any publicly viewable data is free for the taking. Without the application of federal or provincial privacy law, that definition of what is and is not publicly available information does not apply to parties. Parties are free to define what they feel is publicly available, which could include any information that can be observed, like age, race, perceived income range, social media posts and contacts, and more.

When it comes to provincial political parties, the British Columbia NDP (BC NDP) were previously found to be using the Law Society of British Columbia's Lawyer Directory under the understanding that it was publicly available information.[33] However, PIPA dictates that the purpose of collection and use must be "what a reasonable person would consider appropriate in the circumstances."[34] In the case of a directory of lawyers

[28] *PIPA*, *supra* note 28, at s 7.
[29] *Supra* note 27.
[30] OIPC Report, *supra* note 13 at 8-9
[31] *Ibid* at 16-17.
[32] *Regulations Specifying Publicly Available Information*, SOR/2001-7, s 1.
[33] OIPC Report, *supra* note 13 at 24.
[34] *Ibid*.

that is accessible to the public, a reasonable person would expect that use and collection of lawyer directory data would be for the purpose of contacting lawyers for legal services. Instead, the BC NDP were using it to identify potential donors.[35] The OPIC identified this as an inappropriate use of publicly accessible information.

Similarly, though publicly visible, social media accounts and contact lists are not necessarily considered publicly available information. Under *PIPA*, information from them can only be collected with consent of the individual and used only for the purpose that they were collected for.[36] Yet, three parties state that they collect personal information from social media in their privacy policies.

The Liberal, Bloc and Green parties each list social media accounts or contacts as part of the information that they collect, without any note as to how consent is given by the individual to collect that information. Likely because consent is not given. Because all parties' lists of types of information they collect are open-ended, it's very possible that the CPC and federal NDP are also collecting social media information - but their policies do not actively declare it.

iv. On sharing personal information with provincial political parties

Offenders: NDP
Provincial and federal NDP parties have been found to share personal information on their parties' members.[37] The NDP's privacy policy states that personal information may be shared with provincial sections, but that only references sharing with sections of the federal party. It's unlikely that individuals who join the federal party are consenting to sharing their information with unique provincial NDP parties. However, information on non-members maintained by the federal and provincial parties is reportedly not shared between levels.[38]

Section IV: Considerations under Bill C-65

Introduced on March 20, 2024, Bill C-65 is another piece of legislation aimed at establishing the privacy policy rules under the Canada Elections Act as the "national, uniform, and complete privacy regime" that applies exclusively to federal political parties. While the Bill does introduce some form of penalties, they are infinitesimally

[35] *Ibid*.
[36] *PIPA*, *Supra* note 27.
[37] OIPC Report, *supra* note 13 at 24.
[38] *Ibid*.

small administrative monetary penalties, at $1500 for individuals and $5,000 for corporations or entities.[39]

The Bill adds to section 444 of the *Canada Elections Act* by expanding the list of requirements for privacy policies that already exist in the *Act*. It adds that parties should designate a privacy officer, use illustrative examples, note specifics on protection measures, make declarations on data breaches, ensure third party processors use safeguards, and provide annual training to designated privacy officers. Again, this is still not a privacy policy aimed at individuals, it's a policy on handling personal information once it's already under the party's control. This is the status quo with a few more requirements and no teeth. And yet, the existence of this Bill is being put forward to attempt to adjourn the appeal in British Columbia to determine if PIPA applies to federal political parties.[40]

Section V: Recommendations and conclusion

Every party's privacy policy does not come close to living up to general standards of Canadian privacy law. The provisions of the *Canada Elections Act* that declare party-written policies are instead permission slips for parties to collect, use, and disclose personal information with impunity. Something must be done. In line with recommendations from scholars, the Chief Electoral Officer,[41] and the Office of the Privacy Commissioner, political parties need to be tied to some form of privacy law and receive some sort of oversight. This can be accomplished in two general ways: by incorporation into the *Canada Elections Act* of the ten privacy principles used to analyze the policies in this report, or by subjecting the parties to existing privacy laws like *PIPEDA*.

First, that the ten principles used as a basis for this report's analysis be adopted under the *Canada Elections Act* and overseen by the Office of the Privacy Commissioner.[42] This would bring a substantially similar framework directly into the *Elections Act* and conforms with recommendations from both Philip Dufresne, the current Privacy Commissioner of Canada, and Colin Bennet, a professor of political science at the University of Victoria.[43] Adding the amendments directly into the Elections Act would

---

[39] Bill C-65, *supra* note 21 at cl 71, 444.4(2) & cl 94, 508.5(1).
[40] Ian Campbell, "Liberals, Conservatives, and NDP to argue new electoral reform bill should delay voter data court case" (10 April 2024), online: The Hill Times <https://www.hilltimes.com/story/2024/04/10/liberals-tories-and-ndp-to-argue-new-electoral-reform-bill-should-delay-voter-data-court-case/417843/>.
[41] C-47 Senate Study, *supra* note 6 at 54:3 (Stéphane Perrault).
[42] *Ibid* at 54:22 (Philip Dufresne).
[43] Colin J Bennett, "Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations" (2016) 16:2 CJLT 196 at 225-226, online (pdf): <https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1230&context=cjlt>.

leave space for the unique nature of federal political parties and their relationship to democracy in Canada – while also ensuring parties have oversight and are compliant with privacy law principles.

The second option is to simply amend *PIPEDA* to explicitly include political parties in its purview, as recommended by the Standing Committee on Access to Information, Privacy, and Ethics.[44] While this option immediately subjects federal political parties to the same privacy policies as commercial entities in Canada, it may not respect the unique nature of federal political parties and their function in a democracy. It could, however, simultaneously apply privacy law to nonprofit entities in Canada, who are similarly not currently bound by meaningful privacy law.

Whichever route is pursued, one thing is clear: federal political parties need oversight and accountability by application of some form of actual privacy law. Experiences with elections in America and Cambridge Analytica show just how valuable personal information can be to political parties, lobbyists, and major donors alike. While federal political parties do occupy a specific and essential part in Canada's democracy, they need to be far more transparent and accountable to maintain trust in that democracy and respect the personal information of their voters. This is all the more important as artificial intelligence seems likely to allow a previously impossible level of micro-targeting of voters in the near future; limits and public disclosure of such activity will be necessary to safeguard Canadian democracy in the years ahead.

[44] ETHI Study, *supra* note 7 at 25.

Appendix A: Assessment of political parties' compliance with privacy laws

1. Liberal Party of Canada

Accountability	Fail	*Failures to Comply*: ● Does not comply with all ten privacy principles ● Does not inform individuals of the process after any breach of personal information *Successes*: ● Policy details ways that the party protects personal information. *Recommended adjustments*: ● Include information on handling of information in case of a breach ● Come into compliance with all ten privacy principles by following recommendations below
Identifying Purposes	Fail	*Failures to comply*: ● Uses open-ended list of reasons why personal information can be shared with third parties *Successes*: ● Use of a closed list of internal uses of personal information. *Recommended adjustments*: ● Create a closed list of reasons for third party sharing and note that the party will get informed consent before sharing personal information with third parties for any new purposes
Consent	Fail	*Failures to comply*: ● Uses open-ended list of types of personal information a party can collect ● Collection of social media contacts ● Collection of personal information from third parties without consent *Recommended adjustments*: ● Use only closed lists for collection of personal information ● Stop collecting social media information without consent ● Stop collecting personal information from third parties with the individual's consent ● Otherwise comply with all elements of the principle of consent
Limiting Collection	Fail	*Failures to comply*: ● Uses open-ended lists as to the amount and type of personal information gathered *Recommended adjustments*: ● Use closed lists, be transparent, and limit collection of personal information
Limiting use, disclosure,	Unclear	This principle deals with how the party actually uses or discloses personal information. Without an investigation into practices, it is

and retention		unclear if parties are violating this principle. *Recommended adjustments:* ● Add a public statement on retaining and destroying personal information
Accuracy	Unclear	This principle deals with how the party actually verifies accuracy. Without an investigation into practices, it is unclear if parties are violating this principle.
Safeguards	Pass	*Successes:* ● Lists various ways that information is protected ● Lists training of employees and volunteers. ● Limits access to personal information to different sensitivities ● Uses unique personal identifying accounts for anyone with access to collected personal information
Openness	Fail	*Failures to comply:* ● Uses open-ended lists liberally throughout the policy - not transparent ● No accountability mechanism beyond contacting the party *Recommended adjustments:* ● Use closed lists of types of personal information collected, collection methods, and uses (including third party) ● Ensure there is some oversight of the privacy practices of the party, ideally by being subject to PIPA or PIPEDA
Individual Access	Pass	*Successes:* ● Provides contact information for personal information in the party's possession This principle otherwise deals with how the party actually deals with privacy complaints or requests. Without an investigation into practices, it is unclear if parties are violating this principle.
Challenging Compliance	Fail	*Failures to comply:* ● Failed to provide information to complainants in British Columbia, inconsistent with PIPA *Recommended adjustments:* ● Ideally, federal political parties comply fully with PIPA or make themselves subject to PIPEDA

2. Conservative Party of Canada

Accountability	Fail	*Failures to Comply:* ● Does not comply with all ten privacy principles ● Does not inform individuals of the process after any breach of personal information

		Successes: ● Policy details ways that the party protects personal information. *Recommended adjustments:* ● Include information on handling of information in case of a breach ● Come into compliance with all ten privacy principles by following recommendations below
Identifying Purposes	Fail	*Failures to comply:* ● Mentions that the party works with third parties but lists no purposes for which information is shared with them *Successes:* ● Use of a closed list of internal uses of personal information. *Recommended adjustments:* ● Create a closed list of reasons for third party sharing and note that the party will get informed consent before sharing personal information with third parties for any new purposes
Consent	Fail	*Failures to comply:* ● Uses open-ended list of types of personal information a party can collect *Recommended adjustments:* ● Use only closed lists for collection of personal information ● Otherwise comply with all elements of the principle of consent
Limiting Collection	Fail	*Failures to comply:* ● Uses open-ended lists as to the amount and type of personal information gathered *Recommended adjustments:* ● Use closed lists, be transparent, and limit collection of personal information
Limiting use, disclosure, and retention	Unclear	This principle deals with how the party actually uses or discloses personal information. Without an investigation into practices, it is unclear if parties are violating this principle.
Accuracy	Unclear	This principle deals with how the party actually verifies accuracy. Without an investigation into practices, it is unclear if parties are violating this principle.
Safeguards	Pass	*Successes:* ● Lists various ways that information is protected ● Lists training of employees and volunteers.
Openness	Fail	*Failures to comply:* ● Uses open-ended lists liberally throughout the policy - not

		transparent ● No accountability mechanism beyond contacting the party *Recommended adjustments:* ● Use closed lists of types of personal information collected, collection methods, and uses (including third party) ● Ensure there is some oversight of the privacy practices of the party, ideally by being subject to PIPA or PIPEDA
Individual Access	Pass	*Successes:* ● Provides contact information for personal information in the party's possession This principle otherwise deals with how the party actually deals with privacy complaints or requests. Without an investigation into practices, it is unclear if parties are violating this principle.
Challenging Compliance	Fail	*Failures to comply:* ● Failed to provide information to complainants in British Columbia, inconsistent with PIPA *Recommended adjustments:* ● Ideally, federal political parties comply fully with PIPA or make themselves subject to PIPEDA

3. Bloc Québécois

Accountability	Fail	*Failures to Comply:* ● Does not comply with all ten privacy principles ● Does not inform individuals of the process after any breach of personal information *Successes:* ● Policy details ways that the party protects personal information. *Recommended adjustments:* ● Include information on handling of information in case of a breach ● Come into compliance with all ten privacy principles by following recommendations below
Identifying Purposes	Fail	*Failures to comply:* ● Mentions that the party works with third parties but lists no purposes for which information is shared with them *Successes:* ● A closed list of internal uses of personal information. *Recommended adjustments:* ● Create a closed list of reasons for third party sharing and note that the party will get informed consent before sharing personal information with third parties for any new purposes
Consent	Fail	*Failures to comply:* ● Uses open-ended list of types of personal information a party can collect ● Collection of social media account information *Recommended adjustments:* ● Use only closed lists for collection of personal information ● Stop collecting social media information without consent ● Otherwise comply with all elements of the principle of consent
Limiting Collection	Fail	*Failures to comply:* ● Uses open-ended lists as to the amount and type of personal information gathered *Recommended adjustments:* ● Use closed lists, be transparent, and limit collection of personal information
Limiting use, disclosure, and retention	Unclear	This principle deals with how the party actually uses or discloses personal information. Without an investigation into practices, it is unclear if parties are violating this principle. *Recommended adjustments:* ● Add a public statement on retaining and destroying personal information
Accuracy	Unclear	This principle deals with how the party actually verifies accuracy.

		Without an investigation into practices, it is unclear if parties are violating this principle.
Safeguards	Pass	*Successes:* ● Lists various ways that information is protected ● Lists training of employees and volunteers ● Uses unique personal identifying accounts for anyone with access to collected personal information
Openness	Fail	*Failures to comply:* ● Uses open-ended lists liberally throughout the policy - not transparent ● No accountability mechanism beyond contacting the party *Recommended adjustments:* ● Use closed lists of types of personal information collected, collection methods, and uses (including third party uses) ● Ensure there is some oversight of the privacy practices of the party, ideally by being subject to PIPA or PIPEDA
Individual Access	Pass	*Successes:* ● Provides contact information for personal information in the party's possession This principle otherwise deals with how the party actually deals with privacy complaints or requests. Without an investigation into practices, it is unclear if parties are violating this principle.
Challenging Compliance	Fail	This principle otherwise deals with how the party actually deals with privacy complaints or requests. Without an investigation into practices, it is unclear if parties are violating this principle. The Bloc was not part of the BC OIPC's investigation that affected all other parties.

4. New Democratic Party of Canada

Accountability	Fail	*Failures to Comply*: ● Does not comply with all ten privacy principles *Successes*: ● Policy details ways that the party protects personal information ● Includes information on handling of information in case of a breach *Recommended adjustments*: ● Come into compliance with all ten privacy principles by following recommendations below
Identifying Purposes	Fail	*Failures to comply*: ● Uses open-ended list of reasons why personal information can be shared with third parties *Successes*: ● Use of a closed list of internal uses of personal information. *Recommended adjustments*: ● Create a closed list of reasons for third party sharing and note that the party will get informed consent before sharing personal information with third parties for any new purposes
Consent	Fail	*Failures to comply*: ● Uses open-ended list of types of personal information a party can collect *Recommended adjustments*: ● Use only closed lists for collection of personal information ● Otherwise comply with all elements of the principle of consent in practice
Limiting Collection	Fail	*Failures to comply*: ● Uses open-ended lists as to the amount and type of personal information gathered *Recommended adjustments*: ● Use closed lists, be transparent, and limit collection of personal information
Limiting use, disclosure, and retention	Unclear	This principle deals with how the party actually uses or discloses personal information. Without an investigation into practices, it is unclear if parties are violating this principle. *Recommended adjustments:* ● Add a public statement on retaining and destroying personal information
Accuracy	Unclear	This principle deals with how the party actually verifies accuracy. Without an investigation into practices, it is unclear if parties are violating this principle.
Safeguards	Pass	*Successes:*

		● Lists various ways that information is protected ● Lists training of employees
Openness	Fail	*Failures to comply*: ● Uses open-ended lists liberally throughout the policy - not transparent *Successes*: ● Designates a privacy officer who is accountable to individuals *Recommended adjustments*: ● Use closed lists of types of personal information collected, collection methods, and uses (including third party) ● Ensure there is some oversight of the privacy practices of the party, ideally by being subject to PIPA or PIPEDA
Individual Access	Pass	*Successes*: ● Provides contact information for personal information in the party's possession ● Designates a privacy officer who is accountable to individuals This principle otherwise deals with how the party actually deals with privacy complaints or requests. Without an investigation into practices, it is unclear if parties are violating this principle.
Challenging Compliance	Fail	*Failures to comply*: ● Failed to provide full information to complainants in British Columbia, inconsistent with PIPA Recommended adjustments: ● Federal political parties should comply fully with PIPA or make themselves subject to PIPEDA

5. Green Party of Canada

Accountability	Fail	*Failures to Comply*: ● Does not comply with all ten privacy principles ● Does not inform individuals of the process after any breach of personal information *Successes*: ● Policy details ways that the party protects personal information *Recommended adjustments*: ● Include information on handling of information in case of a breach ● Come into compliance with all ten privacy principles by following recommendations below
Identifying Purposes	Fail	*Failures to comply*: ● Uses open-ended list of reasons why personal information can be shared with third parties *Successes*: ● Use of a closed list of internal uses of personal information. *Recommended adjustments*: ● Create a closed list of reasons for third party sharing and note that the party will get informed consent before sharing personal information with third parties for any new purposes
Consent	Fail	*Failures to comply*: ● Uses open-ended list of types of personal information a party can collect ● Collection of social media contacts ● Collection of personal information from third parties without consent *Recommended adjustments*: ● Use only closed lists for collection of personal information ● Stop collecting social media information without consent ● Stop collecting personal information from third parties with the individual's consent ● Otherwise comply with all elements of the principle of consent
Limiting Collection	Fail	*Failures to comply*: ● Uses open-ended lists as to the amount and type of personal information gathered *Recommended adjustments*: ● Use closed lists, be transparent, and limit collection of personal information
Limiting use, disclosure, and	Unclear	This principle deals with how the party actually uses or discloses personal information. Without an investigation into practices, it is unclear if parties are violating this principle. *Recommended adjustments:*

retention		• Add a public statement on retaining and destroying personal information
Accuracy	Unclear	This principle deals with how the party actually verifies accuracy. Without an investigation into practices, it is unclear if parties are violating this principle.
Safeguards	Pass	*Successes:* • Lists various ways that information is protected • Lists training of employees and volunteers • Limits access to personal information to different sensitivities
Openness	Fail	*Failures to comply*: • Uses open-ended lists liberally throughout the policy - not transparent • No accountability mechanism beyond contacting the party *Recommended adjustments*: • Use closed lists of types of personal information collected, collection methods, and uses (including third party) • Ensure there is some oversight of the privacy practices of the party, ideally by being subject to PIPA or PIPEDA
Individual Access	Pass	*Successes:* • Provides contact information for personal information in the party's possession This principle otherwise deals with how the party actually deals with privacy complaints or requests. Without an investigation into practices, it is unclear if parties are violating this principle.
Challenging Compliance	Fail	*Failures to comply*: • Failed to provide information to complainants in British Columbia, inconsistent with PIPA *Recommended adjustments*: • Ideally, federal political parties comply fully with PIPA or make themselves subject to PIPEDA