FIPA Bill C-4 Part 4 line-by-line brief

Detailed review conducted by: Gage Smith

This is an abridged version. The full text can be found at:
https://fipa.bc.ca/bill-c-4-part-4-line-by-line-and-brief/

Abstract

A FIPA review and analysis considering the line-by-line implications of Bill C-4 An Act respecting certain affordability measures for Canadians and another measure – specific to Part 4.

Table of Contents

Bill C-4 Part 4 FIPA Line-by-line brief 1
Table of Contents 1
Intro 1
Recommendations 2
Analysis 2
- Definitions and purpose 2
- Privacy policies 3
- Activities related to personal information 4
- Application of provincial or territorial legislation 4
- Retroactivity 5

Charter analysis 7
About FIPA 10

Intro

Part 4 of Bill C-4[1] would significantly alter the legal framework regulating federal political parties' (FPPs) management of personal information. This analysis considers the differences between the current framework found in the *Canada Elections Act*[2] and the proposed amendments. For clarity, it is arranged by topic as opposed to section number. The analysis is based primarily on the plain text interpretation of the provisions and considerations of the likely intentions of parliament, in alignment with the modern approach to statutory interpretation.[3]

[1] *An Act respecting certain affordability measures for Canadians and another measure*. Link
[2] *Canada Elections Act*, S.C. 2000, c. 9
[3] *Rizzo & Rizzo Shoes Ltd (Re)*, [1998] SCJ No 2

Recommendations

We respectfully urge Members of Parliament to:

- Withdraw Part 4 from Bill C-4 immediately to prevent the passage of these regressive provisions.
- Support a comprehensive, standalone review of privacy obligations for political parties through public consultation and committee study.
- Ensure that political parties are subject to modern, enforceable privacy standards, overseen by an independent regulator such as the Office of the Privacy Commissioner of Canada.

Analysis

This section provides a plain language analysis and context for the changes that would be brought by Bill C-4. The simplest impact based on analysis.

Criteria	Tim Horton's	RCMP CSIS	FPP's Today	FPP's with Bill C-4 Part 4
This entity has an interest in collecting, using, and disclosing the personal information of people in Canada, and it routinely does so.	YES	YES	YES	YES
Federal or substantively similar provincial privacy laws apply to the collection, use, and disclosure of information by this entity.	YES	YES	YES	NOPE
While this entity can develop its own privacy policy, the policy must comply with the privacy principles embedded in federal or substantively similar provincial privacy laws when doing so.	YES	YES	YES	NOPE
This entity is held accountable for compliance with Federal or substantively similar provincial privacy laws by an independent Privacy Commissioner with powers of overisght, investigation, and complaint resolution.	YES	YES	YES	NOPE
Individuals have a legal right to request information about their personal information that is in the control of this entity. In some instances they may withdraw consent for its use.	YES	YES	YES	NOPE

Definitions and purpose

Overview

An update to the definition of "personal information," and the inclusion of the existing purpose statement.

Commentary

The definition of personal information in most of the CEA is incorporated from section 3 of the *Privacy Act*, which is: "information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing [...]".

The Bill C-4 definition makes two key changes: it omits the word "recorded" as a qualifier, and it includes no clarifying examples. In contrast, the *Privacy Act* definition lists 18 examples that explicitly do or do not meet the definition. These changes could make more room for parties to argue that records do not qualify as personal information. For example, they could argue that certain metadata, such as device logs or engagement metrics, are not "about" an individual, but about an interaction or system.

This amendment would also replace the existing privacy provisions in the CEA with a fully self-contained framework. This change is consistent with

the stated purpose of establishing a complete regime for federal political parties; the *Privacy Act* definition applies to others, while political parties occupy their own space and require their own definition.
The purpose statement in Bill C-4 is nearly identical to the existing purpose statement in section 385.2 (3) of the current CEA, and a substantive difference appears unlikely.

Privacy policies

Overview

New provisions set out the requirements for FPPs' privacy policies.

Comparison

A brief comparison of the existing framework to the proposed Bill C-4 framework:

- Filing and registration
  - Existing framework
    - Parties must file a privacy policy and website address with the CEO as part of registration.
  - Bill C-4 framework
    - Parties only must publish a policy on their own website and self-certify compliance in their election-expense return.
- Content of privacy policies
  - Existing framework
    - Policies must describe types of information, collection methods, safeguards, uses, circumstances for sale of data, employee training, practices regarding online data and cookies, and privacy officer's contact.
  - Bill C-4 framework
    - Policies must identify a privacy officer, provide their name and contact information, describe types of information collected, give examples of their activities, and describe training for employees and volunteers.
- Oversight and enforcement
  - Existing framework
    - The CEO has the authority to refuse to register or to deregister a party for failure to provide it with a compliant privacy policy.
  - Bill C-4 framework
    - Parties must comply with their own policies. Violations are treated as administrative offences. There is no independent review of the policy's adequacy, and no deregistration authority.

Commentary

These changes would further weaken a privacy policy regime that is already inadequate. They would reduce transparency, eliminate external oversight, and entrench self-regulation. Among others, we have identified the following main critiques:

- There are no substantive minimum standards for these privacy policies. They do not need to regulate safeguards, uses, retention periods, sale of data, or breach reporting. Parties remain free to draft permissive policies and then "comply" with them.

- Even if a party were to violate their own policy, independent oversight or enforcement is now virtually nonexistent. Oversight from the CEO and provincial privacy bodies were the only limited oversight for FPPs, which were already operating in a legislative void, exempt from privacy standards virtually all other organizations are subject to. There is no power for the CEO or a privacy commissioner to review the adequacy of policies, order changes, or sanction parties.

Activities related to personal information

Overview

FPPs now have the authority to carry out a broader range of activities related to personal information than most public bodies or private organizations.

Comparison

A brief comparison of the existing framework to the proposed Bill C-4 framework:

- Permitted activities relating to personal information
  - Existing framework
    - Parties may collect, use, disclose, retain, and dispose of personal information for the purpose of participating in public affairs by endorsing members as candidates and supporting their election.
  - Bill C-4 framework
    - Parties may "carry out <u>any activities</u> in relation to personal information, including collecting, using, disclosing, retaining and disposing of personal information" for the purpose of participating in public affairs by endorsing members as candidates and supporting their election.

Commentary

Bill C-4 would make the regime even more permissive for political parties. The current framework limits FPPs to specific activities related to managing personal information (collection, use, disclosure, etc.). These activities are consistent with those regulated by other FOI and privacy legislation.
The Bill C-4 change would permit FPPs to "carry out <u>any activities</u> in relation to personal information". On a plain text reading, this significantly broadens the scope of activities FPPs can carry out beyond those specified in most FOI and privacy laws (collection, use, disclosure, etc.). Further, in most frameworks, personal information management is limited to a specific purpose. But the purpose of "participating in public affairs" by supporting candidates for election is broad and undefined. It could potentially encompass all communications and outreach activities. There is no requirement that collection be necessary or proportional to that purpose.

Application of provincial or territorial legislation

Overview

Federal political parties purport to not be bound by provincial or territorial FOI and privacy legislation under these provisions even in instances where they are substantively similar to federal legislation.

Comparison

A brief comparison of the existing framework to the proposed Bill C-4 framework:

- Applicability of provincial privacy laws
  - Existing framework
    - S. 385.2(3) says the regime is national, uniform, exclusive and complete, but it does not explicitly bar provincial laws. Courts have held that provincial privacy statutes like BC's *PIPA* can still apply to federal parties.
  - Bill C-4 framework
    - S. 446.4(1) explicitly provides that political parties and their agents cannot be required to comply with any provincial or territorial law regulating personal information, unless their own policy requires it.
- Access and correction rights
  - Existing framework
    - The CEA is silent on access and correction, so individuals must rely on provincial or federal privacy laws. Under BC PIPA and FIPPA, individuals have a right to request access to personal information and seek corrections.
  - Bill C-4 framework
    - S. 446.4(2) states that parties cannot be required to provide individuals with access to personal information or to correct it, regardless of any other law.

Commentary

The application of provincial and territorial FOI and privacy laws to federal political parties (FPPs) has always been ambiguous, and the issue has been the subject of recent litigation.

BC is the only province to expressly regulate the FOI and privacy practices of political parties. The FPPs argued that BC lacked the jurisdiction to regulate them. In 2024, the BC Supreme Court held[4] that FPPs were subject to provincial FOI and privacy legislation. It found that the provincial and federal laws were complementary, not in conflict, and that both jurisdictions apply to FPPs. This provision purports to end the ambiguity and have the opposite effect of the BC Supreme Court ruling.

Further, under the "for greater certainty" provision, FPPs purport to become expressly excluded from the jurisdiction of any FOI and privacy oversight body, including privacy commissioners and ombudspersons, across jurisdictions. Most organizations are presumptively subject to such oversight and are excluded only by fact-specific exemptions (where the information at issue includes, for example, ongoing law enforcement operations or privileged legal advice).

Retroactivity

Bill C-4 includes a retroactivity clause. "Most laws attach one or more legal effects to particular facts or conduct; once the facts are complete or the

[4] https://www.bccourts.ca/jdb-txt/sc/24/08/2024BCSC0814.htm

conduct has occurred, the legal effect is triggered. Legislation receives a retroactive application when the law applied to past facts or conduct is different from what the law actually was when the facts or conduct occurred."[5]

S. 49 provides that the headings before section 446.1 and sections 446.1 to 446.4 "are deemed to have come into force on May 31, 2000".

In other words, the provisions establishing the new privacy regime for FPPs would apply as if they had been in place since the CEA was enacted over two decades ago.

Ongoing litigation and complaints

Retroactive application could extinguish any claims based on provincial privacy statutes or common law privacy rights arising from parties' past data-handling practices. For example, in *Liberal Party of Canada v. The Complainants, 2024 BCSC 814*, the BC Supreme Court held that BC's *PIPA* applied to federal political parties; that ruling underpinned ongoing investigations and complaints.

By deeming the exclusive federal regime to have been in force since 2000, Bill C-4 purports to effectively overturn that decision and shield parties from liability for historical violations. Other ongoing claims could be similarly nullified. For example, any ongoing complaints about FPPs to provincial privacy commissioners could be moot, since they could no longer have authority to regulate FPPs.

Access to information

Retroactivity would prevent individuals from making access to information requests to FPPs, even regarding personal information that was collected or managed before the enactment of Bill C-4. Without retroactivity, an argument could potentially have been made that FPPs were subject to provincial regulation at the time of collection of the personal information, and the framework of the time should be enforced. But the retroactivity provision closes the door to this approach.

Rule of law

Retroactive legislation is rare. It "generally violates the norms underlying transitional law, fairness and the rule of law, often quite seriously."[6] The rule of law is a core concept in the legal system. It includes the idea that individuals should be able to know and understand the laws governing them to avoid negative consequences. "It is unfair to establish rules, invite people to rely on them, then change them in mid-stream, especially if the change results in negative consequences."[7]

---

[5] Halsbury's Laws of Canada - Legislation (2021 Reissue), 2021 Reissue. Ruth Sullivan. Retrieved from <https://plus.lexis.com/ca/document/?pdmfid=1537339&crid=0ee1057c-8b37-4178-a5f1-d4706d7e15e1&nodeid=AANAABAACAABAAB&nodepath=%2FROOT%2FAAN%2FAANAAB%2FAANAABAAC%2FAANAABAACAAB%2FAANAABAACAABAAB&level=5&haschildren=&populated=false&title=HLG-30%20Retroactivity.&docfullpath=%2Fshared%2Fdocument%2Fanalytical-materials-ca%2Furn:contentItem:63H6-CYC1-F4NT-X25H-00000-00&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials-ca%2Furn:contentItem:63H6-CYC1-F4NT-X25H-00000-00&ecomp=7t_k&prid=a0a77d85-29c5-4fbd-8373-b5047c0c71ff>

[6] *Ibid.*

[7] *Ibid.*

Strong justification is required for retroactive legislation, which appears absent from Bill C-4. Further, it is being invoked to advance the interests of lawmakers at the expense of the populace; it creates self-exemption from privacy frameworks that apply to virtually all other organizations.

Charter analysis

Freedom of expression: Section 2(b)

Section 2(b) of the *Charter* guarantees the fundamental freedom of thought, belief, opinion, and expression, including freedom of the press[8] and political expression.[9] The Supreme Court of Canada has interpreted this right broadly, protecting virtually all forms of expression unless they involve violence or hate speech.

Lack of Access

Under Bill C-4, federal political parties cannot be required to provide access to personal information under its control, or information about that personal information.[10] If a person wants to know what personal information a political party has collected about them, how they collected it, or how they use it, that person could have no legal mechanism to do so. This provision likely offends section 2(b) of the *Charter*.

Section 2(b) does not establish a general right of access to information.[11] However, access may be required if that information is necessary for meaningful public discussion and criticism on matters of public interest.[12] Even if this necessity is demonstrated, access to the documents could still be denied due to other considerations. For example, access would be denied if the documents are privileged or if their disclosure would impair a government function.[13]

In this case, the documents at issue would concern the management of sensitive personal information by political parties. This issue is plainly of public interest. But is access to personal information under the control of political parties necessary for meaningful public discussion? The answer is likely yes.

One potential rebuttal could be that voters could glean insight into those information practices without direct access to their personal information. For example, parties could argue that their privacy policies must be posted publicly, which encourages public debate. However, these policies are often vaguely worded and contain little to no precise information about their internal information management systems[14]. The limited information available to the public only came to light after investigations of "high-

---

[8] *Denis v. Côté, [2019] S.C.J. No. 44.*

[9] *British Columbia Public School Employers' Assn. v. British Columbia Teachers' Federation*, [2005] B.C.J. No. 1719.

[10] Section 446.4(2)

[11] *Ontario (Attorney General) v. Fineberg* (1994), 19 O.R.

[12] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, 2010 SCC 23 at para 37.

[13] *Ibid* at 39-40.

[14] Voter Privacy and Big-Data Elections, (2021) 58 Osgoode Hall LJ 1 - 55

profile voter data incidents such as Cambridge Analytica"[15]. Further, these information management practices would likely be overhauled if Bill C-4 were enacted, as parties would presumably take advantage of their new authority. It is difficult to imagine how meaningful public discourse about political parties' information management practices could take place without transparency into what information is collected and how.

The parties could also counter that by disclosing this information, their ability to function would be impaired. For example, judges can issue publication bans regarding court proceedings if publication would cause a risk to a fair trial.[16] Political parties develop their information management systems to gain competitive advantages over other parties, and public disclosure of those systems could limit their ability to function in a competitive political environment.[17] However, the impact of any particular party to compete against others would likely be mitigated if all political parties were equally required to provide access to documents concerning their information management systems. Parties could also cite privacy or cybersecurity concerns.

To assess a s. 2(b) challenge due to lack of access to information, a court would likely balance two competing interests: the public interest in discourse regarding political parties' information practices, and the impact of the disclosure on parties' abilities to function in a competitive political environment. A court may consider the breadth of the restriction around access to information and the pressing public interest of this issue as a topic of open discussion. Further, all parties would equally be required to provide access, which could reduce competitive disadvantages for any particular party.

A pathway likely exists for a successful section 2(b) challenge due to lack of access.

Chilling Effect

Section 2(b) also protects against acts that deter or suppress protected expression, such as intimidation. For example, if a person is travelling to a peaceful protest, and a police officer searches their property because they intend to protest, that officer would likely be violating s. 2(b)[18].

Currently, federal political parties, like almost every public body, only have limited authority over personal information. They are subject to oversight from the Chief Electoral Officer and must comply with provincial privacy laws. Bill C-4, if enacted, would empower them to "carry out any activities in relation to personal information" without direct oversight from any regulatory body.[19] Parties could engage with this new framework in several ways that may violate s. 2(b) of the *Charter*.

---

[15] *Ibid.*

[16] Note: These publication bans still must be justified under s. 2(b). *Dagenais v. Canadian Broadcasting Corp.*, [1994] S.C.J. No. 104.

[17] *Bennett & Bayley, Canadian Federal Political Parties and Personal Privacy Protection*

[18] *Figueiras v Toronto (City) Police Services Board*, 2015 ONCA 208

[19] See: Commentary, Activities Related to Personal Information

For example, parties could surveil voters' attendance in political demonstrations or protests without consent. They could then compile detailed profiles about individual voters, which they could use internally for any purpose, or potentially publicize or share with other organizations. Voters could experience a chilling effect, where their ability to participate in protected political expression is stifled by fear of overcollection or misuse of their personal information. This chilling effect could amount to intimidation, which would violate s. 2(b). Whether a challenge on this ground would succeed would be highly fact-dependent, but the pathway likely exists.

Democratic Rights: Section 3

Section 3 of the *Charter* protects individuals' rights to vote and to run for office in the House of Commons or provincial legislative assemblies.[20] This right extends to the ability to meaningfully participate in the electoral process, even where that participation does not directly impact the actual outcome of an election.[21] For example, a law that denies voters the information needed to cast an informed vote could be subject to a constitutional challenge.

Voter Suppression

Bill C-4, if enacted, would broadly empower federal political parties to collect and use personal information without independent oversight. Even today, parties gather data about individual voters to assign them "persuadability scores" to determine which voters to contact, what communication methods to use, and how much effort is put into convincing them to vote.[22] These individuals become subject to "micro-targeting"; where political parties use their detailed profiles of individual voters to tailor messaging specifically to the individuals.

If these data-driven practices can be used to mobilize voters, they could also be used for voter suppression.[23] Parties could use micro-targeting to spread misinformation or disinformation to prevent voters from making informed choices on election day, on an individual level. Bill C-4 would likely aggravate this issue, as voters would have no right to access data about them or know how they are being targeted. Voters could reasonably feel intimidated by or misled about the election process, dissuading them from participating.

Reasonable Limits on *Charter* Rights: Section 1

Any limitation of a *Charter* s. 2(b) or 3 right can be saved by s. 1. To do so, the limit must be reasonable and demonstrably justifiable in a free and democratic society. The *Charter* limit must be rationally connected to a pressing and substantial objective, and the infringement must be proportionate to that objective. Part of the analysis involves whether the

[20] Halsbury's Laws of Canada: HCHR-29: Democratic rights in the Charter.
[21] Halsbury's Laws of Canada: HCHR-33: Rights to meaningful participation in the electoral process.
[22] Voter Privacy and Big-Data Elections, (2021) 58 Osgoode Hall LJ 1 - 55
[23] *Ibid.*

infringement "minimally impairs" the *Charter* right; if there is a way to achieve the objective while reducing the *Charter* violation, then the infringement is not minimally impairing and is not saved by s. 1.
The language of Bill C-4 is very broad. It effectively prevents all direct requests for access to personal information held by federal political parties. It grants political parties more authority to manage personal information without oversight than even emergency management agencies or many law enforcement bodies.

For this reason, it appears unlikely that any of the above concerns would be entirely saved by s. 1. It is difficult to imagine how the government could argue that Bill C-4 minimally impairs *Charter* rights when the current framework satisfies its objectives without these particular infringements. Federal political parties can already gather sufficient information to compete in the democratic environment without these broad powers, while subject to independent oversight. Provincial and territorial parties will also continue to function under their current frameworks with less power and more oversight.

About FIPA

The BC Freedom of Information and Privacy Association (FIPA) is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. While we are based in BC, our membership extends across Canada, and we regularly partner with organizations throughout the country.
Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform. We are one of very few public interest groups in Canada devoted solely to the advancement of freedom of information and privacy rights.