BACKGROUNDER
Liberal Party of Canada v. The Complainants, 2024 BCSC 814

THE CONTEXT

In most democratic countries, the opportunities for political parties to capture and use personal information to identify and target voters are constrained by comprehensive privacy protection laws.[1] This is not the case in Canada. Canadian political parties are not generally covered by Canadian privacy legislation – either at the federal or provincial levels. Generally, individuals have no legal rights to learn what information about them is contained in party databases, to access and correct that information, to remove themselves from the systems, or to restrict the collection, use, and disclosure of their personal information. Parties can typically capture personal information from multiple sources, analyze it freely, and mobilize it to target messages on the doorstep, through email and text, and over social media platforms.[2]

A ten-year campaign to bring Canada's federal political parties (FPPs) under the umbrella of comprehensive federal privacy law, and the oversight of the Office of the Privacy Commissioner of Canada (OPC), has been met with stiff and generally unified resistance. Political parties are still the one category of organization in Canada over which individuals have few, if any, legal privacy rights.

This issue has been on the agenda for over 12 years.[3] Back in 2013, the Chief Electoral Officer recommended that all ten privacy principles in Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) be implemented by federal political parties (FPPs).[4] He repeated that call in his 2022 annual report.[5] In 2018, in response to the Cambridge Analytica

---

[1] Bennett, C.J. Voter databases, micro-targeting and data protection law: can political parties campaign in Europe as they do in North America? (Dec 2016) 6(4) *International Data Privacy Law* 261.

[2] Delacourt, S. (2016). *Shopping for votes: How politicians choose us and we choose them*. Madeira Park: D & M Publishers.

[3] Bennett, C. J., & Bayley, R. M. (2012). *Canadian federal political parties and personal privacy protection: A comparative analysis*. Gatineau: Office of the Privacy Commissioner of Canada.

[4] Elections Canada, *Preventing deceptive communications with electors: Recommendations from the Chief Electoral Officer of Canada following the 41st General Election* (2013) at: http://www.elections.ca/res/rep/off/comm/comm_e.pdf

[5] Elections Canada, *Meeting new challenges: Recommendations from the Chief Electoral Officer of Canada following the 43rd and 44th General Elections*, June 7, 2022 at: https://www.elections.ca/content.aspx?section=res&dir=rep/off/rec_2022&document=index&lang=e

scandal, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) recommended "that the Government of Canada take measures to ensure that privacy legislation applies to political activities in Canada, either by amending existing legislation or enacting new legislation."[6] The same was recommended by the Senate Legal and Constitutional Affairs Committee in 2023.[7]

The federal, provincial, and territorial Information and Privacy commissioners have jointly called on their respective governments to pass legislation "requiring political parties to comply with globally recognized privacy principles; empowering an independent body to verify and enforce privacy compliance by political parties through, among other means, investigation of individual complaints; and, ensuring that Canadians have a right to access their personal information in the custody or control of political parties."[8] In April 2019, the federal Privacy Commissioner and the Chief Electoral Officer issued joint guidance on the protection of personal information by the FPPs in response to amendments to the *Canada Elections Act* (CEA) which stipulated that all FPPs develop privacy policies as a condition of registration.[9]

Civil society organisations also exerted pressure. Most notably, Vancouver-based OpenMedia conducted a systematic comparison of the FPPs privacy policies against the national information privacy principles, and exposed the obvious inadequacies.[10] Media attention has increased. Whistleblowers have come forward.[11] And public opinion surveys have registered both a general

---

[6] House of Commons, Standing Committee on Access to Information, Privacy and Ethics (ETHI). (2018). *Addressing digital privacy vulnerabilities and potential threats to Canada's democratic electoral process: Report of the Standing Committee on Access to Information, Privacy and Ethics*. June 2018 at: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-16

[7] Senate Standing Committee on Legal and Constitutional Affairs, Fourteenth Report (June 2023) at: https://sencanada.ca/en/committees/LCJC/Report/117611/44-1

[8] Office of the Privacy Commissioner of Canada (OPC) (2018). *Securing trust and privacy in Canada's electoral process*. Resolution September 11-13, 2018.

[9] Office of the Privacy Commissioner of Canada (OPC) (2019). *Guidance for federal political parties on protecting personal information*, April 1, 2019. Pursuant to Bill C-76, the *Elections Modernization Act*, S.C. 2018, c. 31, s. 385.

[10] Open Media, "Federal Political Parties: Flunking the Privacy Law Test," (April 23rd, 2024) at: https://openmedia.org/article/item/federal-political-parties-flunking-the-privacy-law-test

[11] Newman, K. Podcast, *The Data on Us* (September 16, 2019)

surprise that political parties are not covered by our privacy laws, and strong support for bringing them within the regulatory framework.[12]

There is, therefore, widespread political and public support for bringing political parties into the ambit of Canada's privacy laws. But the campaign has confronted the daunting reality that any attempt to restrict political parties' control of personal information would also curtail their use of a key resource upon which they have become increasingly reliant for electoral success.

Not until the Centre for Digital Rights (CDR) initiated a series of formal complaints to regulators about the FPPs' practices, did they pay serious attention to the problem.[13] One of those complaints went to British Columbia's Information and Privacy Commissioner. Most provincial and federal privacy protection laws do not apply to political parties. There are two exceptions, BC and Quebec. BC's *Personal Information Protection Act* (PIPA) has always applied to provincial political parties, and the BC Commissioner has conducted several investigations.[14] But did the law also apply to the FPPs when they collect, use, or disclose personal information in BC? In 2019, and supported by the CDR, three BC citizens sought access to the personal information collected, used, or disclosed in BC by the federal Liberal, Conservative, New Democratic and Green parties.

Before the Information and Privacy Commissioner was able to begin his investigation, however, the Liberals, Conservatives, and NDP challenged his jurisdiction. The Commissioner's delegate, former BC Commissioner David Loukidelis K.C., then held formal hearings on the specific question of whether FPPs were organizations covered by the legislation, and whether or not federal law "ousted" BC's jurisdiction. In March 2022, he found the FPPs were organizations under *PIPA*, and that the law is constitutionally applicable to the collection, use and disclosure of personal information in BC by FPPs registered under the *CEA*.[15]

---

[12] Curry, B. (2019). Majority of poll respondents express support for extending privacy laws to political parties. *The Globe and Mail*, June 13, 2019; Boutilier, A. Canada's political parties are exempt from privacy laws. Voters say that needs to end. *Global News*, April 25, 2023 at: https://globalnews.ca/news/9649677/federal-parties-voters-privacy/

[13] Center for Digital Rights at: https://www.centrefordigitalrights.org/our-work/quinfecta

[14] British Columbia Office of the Information and Privacy Commissioner (2019). *Full disclosure: Political parties, campaign data and voter consent*. Investigation Report P19-01 at: https://www.oipc.bc.ca/documents/investigation-reports/2156

[15] British Columbia Office of the Information and Privacy Commissioner (2022). *Order P22-02. David Loukidelis QC. Conservative Party of Canada, Green Party of Canada, Liberal Party of Canada, New Democratic Party of Canada.*

The FPPs then jointly sought judicial review to quash the Loukidelis decision. After several delays, the case was heard in the BC Superior Court in April 2024. On May 14, 2024, BC Supreme Court Justice Weatherill issued his decision.[16]

JUSTICE WEATHERILL'S DECISION AND ITS IMPLICATIONS

Justice Weatherill's landmark decision held that Canada's FPPs and their personal information practices are, as they always should have been, subject to the privacy law requirements in BC's *PIPA,* when the FPPs operate in BC. *PIPA* applies to the FPPs, because it applies to all organisations, and the FPPs are organisations. The FPPs admitted as much. PIPA defines "organisation" as including unincorporated associations. The Liberal, Conservative and New Democratic parties all conceded that they were unincorporated associations. Therefore, as organisations under *PIPA,* the FPPs are subject to its requirements.

The federal government tried to pre-empt Justice Weatherill's decision in advance. In June 2023, Parliament amended the *CEA*, asserting that the requirement to comply with their own privacy policies constituted a "national, uniform, exclusive and complete regime" applicable to registered federal political parties.[17] Under Canada's Constitution, the argument went, federal law is paramount, and the amended *CEA* now precluded any province's privacy laws, including *PIPA,* from applying to the FPPs. The plan failed. The *CEA* amendments were window-dressing. They created no complete privacy regime. They did nothing to protect voters from the opaque data harvesting and messaging practices of the FPPs. They lacked an effective enforcement mechanism for the FPPs' privacy policies.

Justice Weatherill's decision underscores that *PIPA* does not conflict with, frustrate, or impair the *CEA*. He rejected all the constitutional arguments advanced by counsel for the FPPs. On the contrary, *PIPA* "has been designed to dovetail with federal laws", in Justice Weatherill's words.

The federal government is now trying to amend the *CEA* yet again, with Bill C-65,[18] introduced on March 20, 2024 and intended again to give the impression of a privacy regime for the FPPs that excludes provincial laws. But, like the June 2023 amendments, Bill C-65 does no such thing. Even if Bill C-65 becomes law, it will not necessarily oust *PIPA*'s application to the FPPs, given Justice Weatherill's ruling. If or when Bill C-65 becomes law, it may also be constitutionally invalid for trying to oust valid provincial laws that protect voters' quasi-constitutional privacy rights. It may also infringe on every Canadian's right to vote under s.3 of the *Charter of Rights and Freedoms*.

If the FPPs continue their litigation against BC *PIPA*'s application, it may needlessly risk sparking a constitutional crisis nationwide. As in BC, Quebec has provincial privacy law

---

[16] https://www.canlii.org/en/bc/bcsc/doc/2024/2024bcsc814/2024bcsc814.html

[17] Bill C-47. Amendments to Canada Elections Act. Sec. 680.

[18] Bill C-65. An Act to amend the Canada Elections Act. Secs. 444.1- 444.5

requirements (including rights to access and correct personal information) — specifically, in the *Civil Code of Quebec* (articles 35, 37-40) and the *Quebec Charter of Human Rights and Freedoms* (article 5) – that Quebec courts could apply to the FPPs. Moreover, both Alberta (which has a longstanding provincial private sector privacy law currently under consultation for updating) and Ontario (which in 2021 signalled its intention to pass its own modern provincial private sector privacy law) have the constitutional authority to enact provincial privacy laws applicable to political parties (both provincial and federal) if they so choose.

WHY DOES THIS DECISION MATTER FOR CANADIANS?

Justice Weatherill began his decision with a compelling endorsement of the significance of privacy for democratic values. He began: "The ability of an individual to control their personal information is intimately connected to their individual autonomy, dignity and privacy. These fundamental values lie at the heart of democracy." He went on: "These proceedings concern the collection and use of the personal information of Canada's citizens by Canada's federal political parties ("FPPs"). The rapid advancement of technological tools allowing for the harvesting of private information for the purpose of profiling and micro-targeting voters has created risks of misuse of personal information that could result in the erosion of trust in our political system."

That is the essence of the issue. Justice Weatherill's ruling affords BC voters personal privacy rights while allowing the FPPs to continue playing their crucial role in Canada's democracy. But we are now in the untenable situation that those rights are enjoyed by individuals in BC, but not in the rest of the country (except partially in Quebec).

Therefore, the federal government should now stop the current legal challenge against the application of BC's *PIPA* to FPPs operating in BC, and instead develop a robust, effective, and enforceable national privacy regime applicable to all FPPs. It can easily achieve this end by accepting amendments to the *Consumer Privacy Protection Act* (Bill C-27), currently in clause-by-clause analysis by the House of Commons Industry Committee. Failing that, it should develop, in consultation with the Chief Electoral Officer and the Office of the Privacy Commissioner of Canada, a truly effective and enforceable national regulatory scheme for the protection of personal information with meaningful accountability and oversight.

Most other democratic countries have applied privacy protection statutes to political parties and have done so for many years. There is no evidence, despite assertions by counsel for the Liberal Party, that compliance with these laws hinders political engagement, or otherwise constrains political parties from communicating their messages. On the contrary, in most other democracies where privacy laws apply to political parties, voter turnout (probably the most important measure of engagement) is higher than in Canada.

There is also no credible reason why Canadians should enjoy privacy rights with respect to government agencies and commercial organizations, but not with respect to political parties. Political parties *do* have special responsibilities in democratic societies to mobilize voters and communicate about their policies. But those functions can be performed whilst respecting

privacy rights – as they are in the EU, the UK, New Zealand, and, of course in BC, which has successfully conducted several hotly contested elections since PIPA was enacted.

The uniform application of such a national privacy protection law will establish a more level playing field and slow the incessant drive for more and more refined data used to profile Canadian voters, which typically benefits the larger and better resourced parties. It will also add much-needed clarity about what constitutes appropriate collection, use and disclosure of voters' personal information – for party employees and volunteers, and for the huge network of companies that operate within the campaigning ecosystem (which must comply with commercial privacy laws).

A genuinely effective and enforceable national privacy protection law would also enforce some transparency onto the entirely opaque Voter Relationship Management systems operated by each of the federal parties, which have grown incrementally and in competition with one another. They have become more sophisticated, interactive, integrative, and efficient as new generations of digital and database technology, typically developed for US political campaigns, have been deployed here in Canada.

Privacy protection law can also establish clearer rules about data security, and about best practices in the event of data breaches and cyberattacks. We have already witnessed a number of data breaches from political parties.[19] They are only likely to continue.

Finally, the Office of the Privacy Commissioner of Canada should have primary responsibility for oversight. The OPC, and its provincial and territorial counterparts, have the resources and the expertise to oversee privacy law, and to give appropriate guidance about best practices. That oversight can, and should, be exercised in collaboration with Canada's Chief Electoral Officer, as it is in BC.[20]

At root, this issue is not just about privacy rights. It is about the health and resilience of our democracy, and about restoring the trust of Canadians in their political institutions – including political parties. The application of privacy law across the campaigning environment will assist in enforcing transparency and in rebuilding trust. Political campaigning is changing dramatically as elections increasingly become more data-driven, and as voter analytics, predictive modelling, and artificial intelligence tools drive campaign communications. The need to develop and apply a strong and consistent set of enforceable privacy rules is urgent.

---

[19] Canada's Political Party Privacy Hall of Shame (January 17, 2024) at: https://openmedia.org/article/item/canadas-political-party-privacy-hall-of-shame

[20] BC OIPC and Elections BC. Guidance Document: Political Campaign Activity (August 2022) at: https://www.oipc.bc.ca/documents/guidance-documents/2537