Canadian Journal of Law and Technology

Volume 16 | Number 2 Article 1

1-1-2016

Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations

Colin J. Bennett
University of Victoria, Department of Political Science, cjb@uvic.ca

Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations

Colin J. Bennett*

Abstract

In light of the revelations concerning Cambridge Analytica, we are now in an era of heightened publicity and concern about the role of voter analytics in elections. Parties in Canada need to enhance their privacy management practices and commit to complying with national privacy principles in all their operations. As shown in this article's comparative analysis of the privacy policies of federal and provincial political parties in Canada, policies are often difficult to find, unclear, and, with a couple of exceptions, do not address all the privacy principles. Accountability and complaints mechanisms are often not clearly publicized, and many are silent on procedures for the access and correction of data, and unsubscribing from lists. Vague and expansive statements of purpose are also quite common. However, this article shows that parties could comply with all 10 principles within the Canadian Standard Association (CSA)'s National Standard of Canada, upon which Canadian privacy law is based, without difficulty; though compliance will require a thorough process of self-assessment and a commitment across the political spectrum to greater transparency. The early experience in British Columbia (B.C.), where parties are regulated under the provincial Personal Information Protection Act, suggests that this process is beneficial for all concerned. In contrast to the system of self-regulation incorporated into the Elections Modernization Act, there is no inherent reason why parties could not be legally mandated to comply with all 10 principles, under the oversight of the Office of the Privacy Commissioner of Canada.

INTRODUCTION

Recent publicity concerning the activities of the company Cambridge Analytica in the 2016 United States (U.S.) presidential election and the United Kingdom (U.K.) Brexit referendum has raised to public and political consciousness the general question of how "Big Data" is, and should be, employed to influence voters and sway elections.[1] This company engaged in the

---

* Professor, Department of Political Science, University of Victoria. I acknowledge the very helpful research assistance of Lauren Yawney on this paper. My thanks to Fenwick McKelvey, Gary Dixon, and Christopher Prince for helpful comments on earlier drafts.

[1] Carole Cadwalladr, "The great British Brexit robbery: how our democracy was hijacked," *The Guardian* (7 May 2017), online: <www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>; Issie Lapowsky, "What did Cambridge Analytica Really do for Trump's Campaign," *Wired* (26 October

particularly controversial practice of psychographic profiling through attempted prediction of voting behavior based on the standard "Big-Five" psychological personality traits — openness, conscientiousness, extroversion, agreeableness, and neuroticism.[2] Together with investigative reports of the complex financing of the company and its links to American billionaire Robert Mercer, this publicity brought to public and media attention the larger question of the role of data analytics in the modern election campaign, and raised a series of searching questions about the implications for representative democracy.[3]

As the emergence of big data analytics has enabled organizations to target consumers in an increasingly granular manner, the same techniques have been used to influence voters, and thus "shop for votes."[4] Delivering the right message, at the right time, to targeted voters has the potential to shift the fate of modern election campaigns and influence results. Although there has been much hype about the importance of the "data-driven" election, and recent empirical work on the extent to which data analytics does indeed influence election outcomes,[5] the competitiveness of current elections continue to place enormous pressure on major political parties in most democracies to continue to use data analytics to gain any edge over their rivals.[6]

There are a number of international trends at work.[7] Parties are moving from stand-alone voter management databases to more integrated voter relationship management (VRM) platforms. They are increasingly using social media platforms such as Facebook and Twitter[8] to analyze issue trends and to

---

2017), online: <www.wired.com/story/what-did-cambridge-analytica-really-do-for-trumps-campaign/>.

2 Roberto J Gonzales, "Hacking the Citizenry: Personality profiling, 'big data' and the election of Donald Trump" (2017) 33:3 Anthropology Today 9.

3 See, e.g., UK Information Commissioner Office, "Democracy Disrupted: Personal Information and Political Influence," online: <ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf>.

4 Susan Delacourt, *Shopping for Votes: How Politicians Choose Us and We Choose Them*, 2nd ed (Madeira Park, BC: Douglas and McIntyre, 2015).

5 Eitan Hersch, *Hacking the Electorate: How Campaigns Perceive Voters* (Cambridge: Cambridge University Press, 2015); Daniel Kreiss, *Prototype Politics: Technology-Intensive Campaigning and the Data of Democracy* (New York: Oxford University Press, 2016); Kyle Endres & Kristin J Kelly, "Does microtargeting matter? Campaign contact strategies and young voters" (2018) 28:1 Journal of Elections, Public Opinion and Parties 1.

6 Colin J Bennett, "The politics of privacy and the privacy of politics: parties, elections and voter surveillance in Western democracies" (2013) 18:8 First Monday; Sasha Issenberg, *The Victory Lab: The Secret Science of Winning Campaigns* (New York: Random House, 2013).

7 Colin J Bennett, "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications" (2015) 13:3/4 Surveillance and Society 370.

8 Hsin-Chen Lin, "How Political Candidates' Use of Facebook Relates to the Election Outcomes" (2017) 59:1 International Journal of Market Research 77; Sanne Kruike-

reach out to precise segments of the electorate through "micro-targeting." Mobile applications increasingly place personal data applications in the hands of a multitude of volunteers and campaign workers. Digital campaigning through automated software programs or "bots" designed to mimic human communications has reached extraordinary prominence and levels of controversy.[9] Additionally, the full panoply of online behavioral marketing techniques employed in the consumer world are also available to candidates and their campaigns.[10] Thus, more data on voters are being captured, and those data are increasingly shared through a complicated network of organizations within the contemporary campaign ecosystem, involving some quite obscure companies that are beginning to play important roles as intermediaries within the democratic process.[11]

So far, understandably, the vast majority of journalistic and scholarly attention has focused on the United States. The range and sophistication of voter surveillance techniques in the U.S. are staggering, unprecedented, and unparalleled in other democratic states.[12] They are obviously facilitated by the absence of any comprehensive privacy protection law, by the First Amendment, which provides robust protections for freedom of communication and association for political purposes, and by a permissive campaign financing system that generally places no restrictions on how much money individual candidates may spend on their election campaigns, nor how much (in total) they may raise from individuals, groups, or corporations. This is not just a U.S. phenomenon, however. Assumptions about the importance of the "data-driven" election have also permeated the campaign strategies of parties and candidates in countries elsewhere.[13] Indeed, the export of these techniques owes a great deal to the influence of key individuals, like Jim Messina, who have worked on U.S. campaigns, and especially the 2008 and 2012 campaigns of Barack Obama. Start-

---

meier, Minem Sezgin & Sophie C Boerman, "Political Microtargeting: Relationship Between Personalized Advertising on Facebook and Voters' Responses" (2016) 19:6 Cyberpsychology, Behavior, and Social Networking 367; Porismita Borah, "Political Facebook use: Campaign strategies used in 2008 and 2012 Presidential elections" (2016) 13:4 Journal of Information Technology and Politics 326.

9 Fenwick McKelvey & Elizabeth Dubois, "Toward the responsible use of bots in politics" *Policy Options* (23 November 2017), online: < policyoptions.irpp.org/magazines/november-2017/toward-the-responsible-use-of-bots-in-politics/ > .

10 Jeff Chester & Kathryn Montgomery, "The role of digital marketing in political campaigns" (2018) 6:4 Internet Policy Review 1.

11 Daniel Kreiss, *Prototype Politics: Technology Intensive Campaigning and the Data of Democracy* (New York: Oxford University Press, 2016).

12 Ira Rubinstein, "Voter Privacy in the Age of Big Data" (2014) 5 Wis L Rev 861.

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

up companies offering a range of data-related services to the modern campaign have been observed in several European countries.[14]

In most other democracies, however, the opportunities to capture and use personally identifiable data to identify and target voters is more severely constrained by comprehensive data protection laws that define such information as highly sensitive, and therefore requiring express consent for processing. This is not the case in Canada. Political parties in Canada, like in the U.S., and unlike in Europe, are generally not subject to federal or provincial privacy laws. Therefore, the extent to which candidates and parties abide by commonly enforced principles of information privacy protection is largely a matter of choice, rather than compulsion. For the most part, individuals have no legal rights to learn what information is contained in party databases, to access and correct those data, to remove themselves from the systems, or to restrict the collection, use, and disclosure of their personal data. For the most part, parties have no legal obligations to keep that information secure, to only retain it for as long as necessary, and to control who has access to it.[15]

This patchwork of incomplete legislative requirements has reached the attention of certain parliamentary committees, regulatory agencies, civil society organizations, and the media. As a result of the "robocall scandal" during the 2011 federal election, and the ensuing investigation by Elections Canada, questions were raised about the larger role that data analytics plays in Canadian elections. Elections Canada subsequently recognized that the "absence of a legal framework governing how personal information is managed and protected by political parties and candidates is a matter of significance, considering that the intelligence compiled and accessed by political parties on the composition of the electorate is likely a key factor in the attraction to the use of devices such as robocalls to deceive targeted segments of the electorate."[16] The report concluded by recommending "that political entities become subject to the broadly accepted privacy principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, also enumerated in Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)."[17] In his review of the 1982 *Privacy Act*, the Privacy

---

[14] *Ibid.*

[15] Office of the Privacy Commissioner of Canada, *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis,* by Colin J Bennett & Robin M Bayley, online: <www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/#toc3a>; Elizabeth Judge & Michael Pal, "Privacy and the Electorate: Big Data and the Personalization of Politics," (Report delivered at the University of Ottawa Center for Law, Technology and Society, 10 February 2017) [online: <techlaw.uottawa.ca/sites/techlaw.uottawa.ca/files/judge_pal_privacyandtheelectorate_ksg_report_oct_14_final.pdf>].

[16] Elections Canada, "Preventing Deceptive Communications with Electors," online: <www.elections.ca/content.aspx?section=res&dir=rep/off/comm&document=index&lang=e>.

[17] *Ibid.*

Commissioner of Canada also advised Parliament to consider extending legislation to the information held by political parties.[18]

The pressure has mounted in 2017 and 2018. The House of Commons committee on Access to Information, Privacy and Ethics (ETHI), after a series of hearings into the vulnerabilities of Canada's democratic system arising from the breach of personal data involving Cambridge Analytica and Facebook, has 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."[19] Federal and provincial privacy commissioners have called for political parties to be brought within Canada's privacy laws.[20] Other outside organizations, such as the Canadian Bar Association, have also been increasingly vocal.[21] Further, a public campaign has also been launched by the Vancouver-based advocacy organization, Open Media.[22]

In response, the Government of Canada has introduced, as part of the *Elections Modernization Act* (Bill C-76), some modest provisions requiring parties to develop privacy codes of practice and to lodge them with Elections Canada. If passed, Bill C-76 would require registered political parties to have a publicly available, easily understandable policy describing the collection, protection, and sale of personal information, procedures for staff training, and the identity of a designated person to whom privacy concerns can be addressed. The submission of this policy would be a required part of their application for registration with Elections Canada.[23]

These provisions have been met with almost universal criticism for their incompleteness, vagueness, and lack of any real enforcement mechanism.[24] As

---

[18] Alex Boutilier, "Political Parties need rules for collecting Canadians data, says privacy watchdog," *Toronto Star* (2 November 2016), online: < www.thestar.com/news/canada/2016/11/02/political-parties-need-rules-for-collecting-canadians-data-therrien.html > .

[19] House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process* (June 2018) at 35.

[20] Office of the Privacy Commissioner of Canada (Remarks at presentation before the Senate Open Caucus, 30 May 2018). [online: < www.priv.gc.ca/en/opc-news/speeches/2018/sp-d_20180530/ >]; Ontario, Information and Privacy Commissioner, *Thirty Years of Access and Privacy Service, 2017 Annual Report* (Toronto: Office of the Information and Privacy Commissioner of Ontario, 2017).

[21] Letter from the Canadian Bar Association, to the Honourable Scott Brison, Acting Minister of Democratic Institutions (27 April 2018), online: < www.cba.org/CMSPages/GetFile.aspx?guid = dc9f96bf-8d1c-4a4a-9d75-22583a3fec4e > .

[22] Open Media, "Privacy Laws Should Apply to Political Parties," online: < act.openmedia.org/C76?utm_source = nom&utm_medium = slideshow&utm_campaign = 7144&tdid = 1690 > .

[23] Bill C-76, *Elections Modernization Act: An Act to amend the Canada Elections Act and consequential amendments*, 1st Sess, 42nd Parl, 2018 (first reading 30 April 2018).

[24] Colin J Bennett, "Election bill does little more than reinforce the status quo," *iPolitics* (7

will be demonstrated below, they simply reinforce the status quo, without substantially requiring political parties to do anything more than they do at the moment. In consultation with Elections Canada, the Privacy Commissioner has recommended amendments, in particular a specification that the privacy policies must be consistent with the principles set out in the *Model Code for the Protection of Personal Information*, found in Schedule 1 of *PIPEDA*, and that his office should be responsible for oversight.[25]

The body of this article examines the assurances already provided by the main federal parties about how they process the personal data under their control. In some cases, these claims are embodied within privacy policies, available (if not prominently) on the parties' websites. The analysis is conducted in comparison with the 10 privacy principles, embodied within the National Privacy Standard of Canada, and within *PIPEDA*.[26] These principles present the central obligations that any organizations need to address in developing a thorough privacy management program. Many, including the current Federal government, have argued that political parties are *sui generis*, and that privacy rules should not restrict their ability to interact with constituents.[27] Parties are, indeed, different from the commercial organizations for which the standard was originally constructed and to which *PIPEDA* applies. This analysis, however, confirms that these same principles can be applied (with adaptations) to capture data within the political realm. The initial experience in B.C., where parties are subject to the provincial *Personal Information Protection Act* (*PIPA*), supports this conclusion.[28]

Although there are some significant hurdles facing reformers who seek to bring parties within the ambit of existing privacy legislation, there are compelling arguments for a raising of the privacy standards, for a harmonization of policy across the federal and provincial political arenas, and for far greater transparency about how personal data is captured, used, and disclosed before, during, and after the modern election campaign. It is quite obvious that the questions raised by the data-driven campaign will only become more pressing,

---

May 2018), online: <ipolitics.ca/2018/05/07/election-bill-does-little-more-than-reinforce-the-status-quo/>; Teresa Scassa, "A federal bill to impose privacy obligations on political parties in Canada falls (way) short of the mark," Teresa Scassa (blog), online: <www.teresascassa.ca/index.php?option=com_k2&view=item&id=276:a-federal-bill-to-impose-privacy-obligations-on-political-parties-in-canada-falls-way-short-of-the-mark&Itemid=80.>.

[25] Office of the Privacy Commissioner of Canada, "Appearance before Standing Committee on Procedure and House Affairs on the study about Bill C-76, Elections Modernization Act," online: <www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180605/#amendments>.

[26] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[27] Elise von Scheel, "Government not ready to apply privacy laws to political parties," *CBC News* (2 April 2018), online: <www.cbc.ca/news/politics/government-privacy-laws-facebook-legislation-brison-1.4600104>.

[28] *Personal Information Protection Act*, S.B.C. 2003, c. 63.

and that Canadian political parties (federal and provincial) urgently need take their privacy responsibilities more seriously.[29]

I. POLITICAL PARTIES AND PRIVACY PROTECTION LAW IN CANADA

The vast majority of public and private organizations in Canada are regulated by federal and/or provincial privacy protection legislation — the fact that political parties are not is attributable to the piecemeal process through which these laws developed. Public sector bodies were regulated first, through the federal *Privacy Act* of 1982,[30] and subsequently through provincial freedom of information and protection of privacy laws, such as those in Ontario, British Columbia, and Alberta. With the exception of Quebec, legislation covering the private sector followed, through *PIPEDA*, and the essentially equivalent *Personal Information Protection Acts* in B.C. and Alberta. Unlike in many other countries that have passed comprehensive information privacy or data protection legislation in one package, Canada's experience was incremental, thus leaving some categories of organization largely unregulated.[31] Political parties stand as the principal example of those agencies that "fell through the cracks" of a privacy regime that regulates either public bodies or organizations involved in commercial activities.

It is also, of course, likely that any attempt over the last 30 years to include political parties within public or private sector privacy legislation would have been met with stiff resistance from all political quarters. Canadian parties are highly competitive, but they are also entrenched and prone to collectively defend their interests against regulators. Indeed, there is some literature that suggests that they operate as a form of "cartel." MacIvor, for instance, has argued that the major Canadian parties in the 1990s colluded to exclude new parties from obtaining official party status, and have historically shaped the provision of state financial subsidies to benefit their own interests.[32] Similar cartel-like behavior has been observed in relation to regulations concerning ballot-access, and thus control of the degree of party competition.[33] In the case of privacy protection, there was no observable debate or conflict concerning the regulation of political

---

[29] Colin J Bennett, "Data Point: What political parties know about you," *Policy Options* (1 February 2013), online: < policyoptions.irpp.org/wp-content/uploads/sites/2/2013/02/data-point.pdf > .

[30] *Privacy Act*, R.S.C. 1985, c. P-21.

[31] See Office of the Privacy Commissioner of Canada, "Overview of Privacy Legislation in Canada," online: < www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/ > .

[32] Heather MacIvor, "Do Canadian Political Parties Form a Cartel?" (1996) 29:2 Canadian Journal of Political Science 317.

[33] Anika Gauja, "Building Competition and Breaking Cartels? The Legislative and Judicial Regulation of Political Parties in Common Law Democracies" (2014) 35:3 International Political Science Review 339.

parties under either federal or provincial privacy laws. It was generally assumed that parties would not be covered, even though many of their marketing activities could indeed be defined as "commercial" in character. The issue has simply not been on the agenda when federal or provincial privacy legislation has been passed over the last 30 years.

The exception to this trend is British Columbia, whose *PIPA* applies broadly to "organizations" (other than public bodies), regardless of whether or not they are engaged in commercial activity. The Office of the Information and Privacy Commissioner of British Columbia, therefore has jurisdiction over political parties, and has already conducted two investigations involving both the B.C. New Democratic Party (B.C. NDP) and the B.C. Liberals.[34] The office is currently engaged in a broader analysis of compliance with *PIPA* by all major political parties in British Columbia[35]

Canadian political parties do have legislative responsibilities for the protection of personal information mandated by the federal *Elections Act* (the "*Act*"), and provincial equivalents. The voter lists provided at election time to registered political parties, at both federal and provincial levels, are subject to quite strict rules concerning security, retention, unauthorized access, and so on. The *Elections Act* specifies at ss. 110 and 111, that parties, candidates, and MPs are expressly authorized to use the lists for communicating with electors, including for soliciting contributions and recruiting members. However, the *Act* also provides (at s. 111(f)) that no person may knowingly use personal information that is recorded in a list of electors for a purpose other than the one specified above or at a federal election (or referendum). Penalties for failing to comply with this provision are contained in Part 19 of the *Act*.[36] The problem, however, is that these regulations only apply to this one source of data, and, as described below, parties capture data from an increasing variety of other sources.

Some provincial election authorities have begun to insist that parties follow certain basic privacy practices if they wish to continue to receive voter lists. In British Columbia, for instance, a revision to the province's *Election Act* in 2015 required "all individuals and organizations who wish to access personal information available under the Election Act . . . to first file an acceptable privacy policy with the Chief Electoral Officer."[37] The Office of the Chief

---

[34] British Columbia, Office of the Information and Privacy Commissioner, "Summary of the Office of the Information and Privacy Commissioner's Investigation of the B.C. N.D.P.'s use of social media and passwords to evaluate candidates," P11-01-MS, online: <www.oipc.bc.ca/mediation-summaries/1399>; British Columbia, Office of the Information and Privacy Commissioner, *Sharing of Personal Information as Part of the Draft Multicultural Strategic Outreach Plan: Government of British Columbia and BC Liberal Party*, Investigation Report F13-04, online: <www.oipc.bc.ca/investigation-reports/1559>.

[35] Office of the Information and Privacy Commissioner for British Columbia, News Release, "Privacy Commissioner investigating political party compliance with PIPA" (21 September 2017), online: <www.oipc.bc.ca/news-releases/2077>.

[36] *Canada Elections Act*, S.C. 2000, c. 9, s. 275.

Electoral Officer has published a template, against which privacy policies are reviewed. The template only applies to personal information disclosed by Elections B.C. under the *Election Act* and contains a minimum set of stipulations on use, security, disposition, and access. Privacy policies may be reviewed on request, but there is no obligation that they be published, and the CEO has no authority to force them to be published.[38]

In June 2017, Elections Ontario published its *Guidelines for the Use of Electoral Products Ontario*. Ontario's *Election Act* also requires any registered political party to file a privacy policy with Elections Ontario, which has also offered a sample policy covering restrictions on use, tracking of distribution, loss and theft of personal information, and the responsibilities of candidates and MLAs.[39] Again, however, there is no responsibility to publish, nor to cover any information beyond that provided by Elections Ontario in the Permanent Register of Electors (PREO). These interventions by the B.C. and Ontario offices are welcome, but they do not address the broader problem, nor the full range of personal data that parties might capture, use, and disclose in the course of campaigning during an election, or indeed at any other time.

Political parties and other political entities are also exempted from the "Do Not Call List" (DNCL) procedures implemented through the Canadian Radio-telecommunications Commission (CRTC). As provided for in s. 41.7 of the *Telecommunications Act*, the National DNCL Rules do not apply in respect of a telecommunication made by a registered party, a party candidate, or a nomination or leadership contestant. They are obliged, however, to comply with some of the basic telecommunications rules for unsolicited calling, such as identifying the person on whose behalf the call is made, providing contact information, and displaying the originating phone number. They must also maintain an internal do not call list, but are not obliged to disclose this to callers.[40] Parties are also exempt from the Canadian Anti-Spam legislation (CASL) if the primary purpose of the message is to solicit a contribution, although, as discussed below, some say that they comply voluntarily by including an unsubscribe option at the end of an e-mail.[41]

---

[37] Elections British Columbia, "Privacy policy template for political parties," online: <elections.bc.ca/privacy/>.

[38] Correspondence, Elections BC, 3 March 2017.

[39] Elections Ontario, "Guidelines for the Use of Electoral Products," online: <www.elections.on.ca/content/dam/NGW/sitecontent/2017/resources/policies/Guidelines%20For%20the%20Use%20of%20Electoral%20Products.pdf>.

[40] Canadian Radio-television and Telecommunications Commission, "Rules for Unsolicited Telecommunications made on behalf of political entities," online: <crtc.gc.ca/eng/phone/telemarketing/politi.htm>.

[41] Canadian Radio-television and Telecommunications Commission, "Frequently Asked Questions about Canada's Anti-Spam Legislation," online: <www.crtc.gc.ca/eng/com500/faq500.htm>.

In the absence of regulatory guidance, therefore, political parties in Canada are essentially free to define their privacy obligations as they wish. Most have commitments that they label as a "privacy policy" made accessible through their websites. So, what do these statements say?

II. "YOUR PRIVACY IS IMPORTANT TO US": WHAT CANADIAN PARTIES' PRIVACY POLICIES DO, AND DO NOT, SAY

While there is no legal obligation to abide by standard privacy protection rules, all parties in Canada (to some extent) acknowledge that privacy is an important issue, and give at least minimal commitments to potential voters and donors.

We have analyzed the privacy policies of the main federal parties, and of the largest provincial parties in the four largest provinces — Ontario, Quebec, British Columbia, and Alberta.[42] We initially asked some very basic questions about the scope of the privacy policy, and about any references to particular laws or legal principles. We then compared the various commitments of the federal parties against the ten privacy principles contained in the CSA's *Model Code for the Protection of Personal Information* — the national standard upon which *PIPEDA* was based.[43]

Table One presents some basic information about the four main federal parties. Each has a privacy policy retrieved from the main party website. Interestingly, each applies that policy to "personally identifiable information" (PII) or "personal information," and there is, of course, a subtle but important difference between the two. The meaning is variable, depending on whether the information is captured from the individual, online or offline, publicly accessible, or provided under the authority of Canada's *Election Act* by Elections Canada. In terms of legislative commitments, the broadest commitment appears to be from the N.D.P., which acknowledges that it complies with the Canada *Elections Act* and "Canadian Privacy Principles." In no case does any party reference the 10 principles from the CSA's National Standard. In no case, is federal law referenced beyond Canada's *Elections Act*, which only directly applies to the data provided in the Voters List.

---

[42] The versions analyzed were those that were publicly available as of May 2018.

[43] Consumer Measures Committee, "Model Code for the Protection of Personal Information: A National Standard of Canada," online: <cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00076.html>.

Table One: Federal Parties' Privacy Commitments

Parties	**Is there a policy available?**	**What kind of information does the policy apply to?**	**What is covered by "personal Information"?**	**Application to particular legal principles?**	***PIPEDA* principles?**	**Policy officer named?**
Liberal Party	Yes	Personally identifiable information	Information provided by the individual personally or through a volunteer or acquaintance	Canada *Elections Act* and Canadian anti-spam legislation	No specific reference	No reference; questions directed to assistance@liberal.ca and a mailing address
Conservative Party	Yes	Personally identifiable information	Information provided by the individual, either publicly accessible or obtained through Elections Canada	No specific reference	No specific reference	Yes; Trevor Bailey, Privacy Officer Conservative Party of Canada 1720 — 130 Albert St. Ottawa, ON K1P 5G4
New Democratic Party	Yes	Personally identifiable information	Information provided by the individual, collected through the website or obtained through Elections Canada	Canada *Elections Act* and "Canadian privacy principles"	No specific reference	No reference; questions directed to CanadasNDP-LeNPDduCanada@ndp.ca, phone number and mailing address
Green Party	Yes	No specific definition beyond "personal information"	Information provided by the individual	Canada *Elections Act*	No specific reference	No reference; directed to contact page

Tables 2 to 5 outline the practices of provincial parties in British Columbia, Alberta, Ontario, and Quebec. Most provincial parties have gone no further than to generate policies confined to their websites. The exception is British Columbia, of course, where s. 5 of *PIPA* obliges covered organizations to:

> (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,

(b) develop a process to respond to complaints that may arise respecting the application of this Act, and
(c) make information available on request about
  (i) the policies and practices referred to in paragraph (a), and
  (ii) the complaint process referred to in paragraph (b).[44]

They must also "designate one or more individuals to be responsible for ensuring that the organization complies with the Act."[45] Both the B.C. Liberals and the B.C. Green Party have developed general privacy policies that apply to the entirety of the information they collect. The B.C. NDP has published a "Data Use Policy." We analyze these commitments further below.

One further aspect of provincial policy is worthy of comment. The Ontario Liberal Party claims that the "handling of all personal information by the Ontario Liberal Party is governed by the *Freedom of Information and Protection of Privacy Act* (*FIPPA*)." In a legal sense, the party is not governed by *FIPPA*, but it is the only party in Canada that has declared adherence to a legislative standard that governs public bodies. The Office of the Information and Privacy Commissioner of Ontario has never adjudicated any claim or complaint against the party, and would not have jurisdiction in any case. The Progressive Conservative Party of Ontario has designed their privacy policy "to meet or exceed the requirements of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) and the ten principles found in the Canadian National Standard for the Protection of Personal Information." As with the Liberals' claims, however, it is not clear whether the policy applies solely to the website, or more broadly.

Table Two: B.C. Parties' Privacy Commitments

Parties	**Is there a policy available?**	**What kind of information does the policy apply to?**	**What is covered by "personal Information"?**	**Application to particular legal principles?**	***PIPEDA* principles?**	**Policy officer named?**
Liberal Party	Yes	Personal information that is not publicly available as denoted by *PIPA* or other policies; information provided by Elections	"Information about an identifiable individual but does not include his or her business contact information"; does not apply to publicly available	*PIPA* and the *Election Act*	Yes; sections specifically titled in accordance with *PIPEDA*	Yes; Kevin Tan privacyofficer@bcliberals.com BC Liberal Party PO Box 21014 Waterfront Centre Vancouver, BC V6C 3K3

[44] *Personal Information Protection Act*, *supra* note 28.

[45] *Ibid*, s. 4.

Parties	**Is there a policy available?**	**What kind of information does the policy apply to?**	**What is covered by "personal Information"?**	**Application to particular legal principles?**	***PIPEDA* principles?**	**Policy officer named?**
		B.C.	information or information on corporate or commercial entities			
New Democratic Party	No; data use policy and submitted policy to Elections B.C.	Information collected on the website and provided by Elections B.C.	Information provided by the individual; information provided by Elections B.C. (only covered by the submitted policy	"Endeavours to exceed the commitments of federal and provincial law"; B.C. privacy legislation and the *Election Act*	Some reference in section titles	No; questions directed to privacy@bcndp.ca
Green Party	Yes	All information collected by the party and provided by Elections B.C.	Information about an individual "Defined by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA)"; divided into private and sensitive private information	*PIPA* and the *Election Act*	Yes; sections specifically titled in accordance with *PIPEDA*	Yes; Michael Wheatley 1-888-473-3686 ext. 0 privacy@bcgreens.ca

Table Three: Alberta Parties' Privacy Commitments

Parties	**Is there a policy available?**	**What kind of information does the policy apply to?**	**What is covered by "personal Information"?**	**Application to particular legal principles?**	***PIPEDA* principles?**	**Policy officer named?**
New Democratic Party	Yes	Information collected on the website	Information collected on the website and provided by the individual	No reference	Some reference in section titles	No; questions directed to office@albertandp.ca or a mailing address
United Conservative Party	No	N/A	N/A	N/A	N/A	N/A
Liberal Party	No	N/A	N/A	N/A	N/A	N/A

Table Four: Ontario Parties' Privacy Commitments

Parties	**Is there a policy available?**	**What kind of information does the policy apply to?**	**What is covered by "personal Information"?**	**Application to particular legal principles?**	***PIPEDA* principles?**	**Policy officer named?**
Liberal Party	Yes	Information collected on the website	Information obtained on the website or electronically	*FIPPA*	No reference	No
Progressive Conservative Party	Yes	Information voluntarily provided on the website	"details about an identifiable individual" such as contact information, name, etc.	*PIPEDA* and "the ten principles found in the Canadian National Standard for the Protection of Personal Information"	specifically references compliance to *PIPEDA*	No
New Democratic Party	Yes; inaccessible Nov. 10, 2017	Information collected on the website	Information collected on the website and user provided information	No reference	Some reference in section titles	No; questions directed to info@on.ndp.ca or a mailing address

Table Five: Quebec Parties' Privacy Commitments

Parties	**Is there a policy available?**	**What kind of information does the policy apply to?**	**What is covered by "personal Information"?**	**Application to particular legal principles?**	***PIPEDA* principles?**	**Policy officer named?**
Liberal Party	Yes	Not specified	Information provided by the individual	Quebec *Elections Act* and "some additional provisions"	No reference	No; questions directed to info@plq.org
Parti Quebecois	Yes	Personal information; excludes navigational data	Information collected on the website and provided by the individual	No reference	No reference	No
Coalition Avenir Quebec	Yes	Information voluntarily provided	Information that may be used to identify an individual and provided by the individual	No reference	No reference	No; questions directed to info@coalitiona-venirquebec.org

III. FEDERAL POLITICAL PARTIES AND COMPLIANCE WITH THE TEN *PIPEDA* PRIVACY PRINCIPLES

We now analyze the various commitments of the federal political parties against the 10 privacy principles contained in the National Standard of Canada developed by the Canadian Standards Association. The CSA's *Model Code for the Protection of Personal Information* was developed by a 45-member group of stakeholders from business, government, civil society, and academia in the mid-1990s. Although these rules were originally developed for commercial organizations, they were framed in sufficiently general language to apply more broadly. Organizations in other sectors, such as public, non-profit, local, and national, have found them a useful template. The original conception was that different organizations would be able to take the standard and adapt it to their unique circumstances. It is also crucial to remember that this national standard is a document to which organizations can be properly certified, or registered, in a similar way to those issued by the International Standardization Organization (ISO). Registration or certification to standards requires organization to "say what they do; and do what they say."[46]

The standard was subsequently included as Schedule One of *PIPEDA*, and establishes the 10 principles around which most commercial organizations have to consider their responsibilities: Accountability; Identifying Purposes; Consent; Limiting Collection; Limiting Use, Disclosure and Retention; Accuracy; Safeguards; Openness; Individual Access; and Challenging Compliance. We examine these 10 principles in order, and give examples of how political parties in Canada have, or have not, expressed adherence to them. We concentrate in this section on the four main federal parties, and offer examples from their policies where relevant comparisons can be made.[47] In the next section, we contrast this experience with the statements and policies, generated by the pressure of regulation of the main British Columbia political parties.

Principle 1 (Accountability): ''An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles."

The first standard does not contemplate that the responsible person nominated should have exclusive responsibility over privacy, but that the person should be familiar with relevant legal obligations and be ready to handle requests from citizens about their privacy. This is now standard practice across democratic countries, and is required under the new European Union General Data Protection Regulation (GDPR) for any organization whose core activities require the processing of personal data on a large scale.[48] In many ways, this is one of the easiest responsibilities to fulfill.

The practice of Canadian political parties is sketchy. Only one, the Conservative Party, publishes a named individual with the title of "privacy officer" and a dedicated e-mail address: privacy@conservatives.ca. Some refer individuals to a generic e-mail address (e.g. assistance@liberal.ca or info@ndp.ca), or a general inquiry line. Responsibility for the implementation of the policy is, therefore, confusingly bound up with other issues about which the party might receive inquiries, such as membership and donations.

---

[46] Colin J Bennett, *Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association* (Rexdale: Canadian Standards Association, 1995).

[47] New Democratic Party of Canada, "Privacy Policy," online: < www.ndp.ca/privacy > ; Liberal Party of Canada, "Privacy Policy," online: < www.liberal.ca/privacy > ; Conservative Party of Canada, "Privacy Policy," online: < www.conservative.ca/privacy-policy > ; Green Party of Canada, "Important information and privacy policy," online: < www.greenparty.ca/en/privacy > .

[48] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ 2016, L119.

Principle 2 (Identifying Purposes): ''The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection."

Purpose specification drives many of the legal obligations behind *PIPEDA*, under the principle that organizations are expected to collect only personal data that is relevant to their core functions in society. This transparency about purpose establishes the basis of trust upon which individuals interact with those organizations. Large organizations might capture personal data for a number of legitimate purposes; political parties are no different.

The principle obliges organizations to reflect on why they need personally identifiable information in the first place. Most political parties seem to assume that the answer is obvious: to communicate with and try to persuade the electorate. The policies of the federal political parties rarely go beyond this assumption. The federal Liberal Party states: ''We also use your personal information to communicate with you about the Liberal Party and its activities, as well as to provide you with news and information. We use your financial information to process your contributions. If you have been a contributor, we may contact you again to seek your financial support."[49] The Conservative party merely says: ''We use your personal information to communicate with you. As a political party, we believe it is important to communicate with Canadians on a regular basis."[50]

The central point is that an open-ended and vague definition of purpose does not delimit the subsequent capture, use, and disclosure of the information. A blanket statement such as ''we use your personal information to communicate with you" imposes virtually no limitation on the range of information that might be collected to fulfil that purpose, and no limitation on the kinds of predictive analytical techniques that parties may use to profile the electorate.

Principle 3 (Consent): ''The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."

In the commercial context, a number of exceptions to the consent requirement have been articulated and developed as a result of guidance and rulings by the Office of the Privacy Commissioner (OPC). The ''except where inappropriate" disclaimer was originally included to exempt data that has to be captured for legal, health, or security reasons, or where there is no direct relationship with the individual. The principle is based on knowledge of the purposes for which the information is collected, as well as on the reasonable expectations of the individual. The standard is also based on a distinction between sensitive and non-sensitive categories of personal data, the former requiring explicit (rather than implied) consent. Most privacy protection laws

---

[49] Liberal Party of Canada, *supra* note 47.

[50] Conservative Party of Canada, *supra* note 47.

(including the new GDPR) consider information on political opinions to fall into the sensitive category.[51]

So, what do federal political parties say about consent? No party explicitly states that they only collect your personal information with consent, although one could interpret the phrase used by the Liberals ("we obtain the information that you choose to give us"[52]) as being synonymous. The federal NDP reminds the reader "if you submit your email address and/or personal information through ndp.ca, you consent to being added to our email and/or contact list."[53] Thus, if one makes an inquiry or registers a complaint through the website, these actions may also constitute "consent" to being contacted.

There are several critical questions that parties need to address when considering their commitments regarding the collection of information directly from constituents with their "knowledge and consent." Much of the issue centers on what party canvassers are actually told to tell constituents on the doorstep or telephone when they solicit sensitive information about political opinions and activities. Voter contact calling is, to some extent, administered by the CRTC, which now runs a Voter Contact Registry, and requires certain minimal rules of identification if the call is made through a service provider.[54] Practices on how to contact constituents on the doorstep, however, vary amongst the parties. Many constituents are, of course, only too willing to share their views, but many are not.

The question arises whether those who do share their views and intentions have a reasonable knowledge that their information will be stored in the voter management database and used to score and profile the electorate. The Conservative Party has run the Constituent Information Management System (CIMS) since 2004. The Canadian Liberal Party has a similar "voter identification and relationship management system" called Liberalist, originally based on the Democrats' Voter Activation Network platform. The NDP uses a system called Populus. There was heightened scrutiny of these systems during the October 2015 general election.[55] Each system takes the Voters List from Elections Canada, and then overlays data from a variety of other

---

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

[52] Liberal Party of Canada, *supra* note 47.

[53] New Democratic Party of Canada, *supra* note 47.

[54] Canadian Radio-television and Telecommunications Commission, "How to Contact Canadians the Right Way," online: < www.crtc.gc.ca/eng/phone/rce-vcr/guide-pol.htm > .

[55] Susan Ormiston, "Federal election 2015: How data mining is changing political campaigns," *CBC News* (3 September 2015), online: < www.cbc.ca/news/politics/federal-election-2015-how-data-mining-is-changing-political-campaigns-1.3211895 > ; Colin J Bennett, "They're spying on you: how party databases put your privacy at risk," *iPolitics* (1 September 2015), online: < ipolitics.ca/2015/09/01/theyre-spying-on-you-how-party-databases-put-your-privacy-at-risk > .

sources. Another relevant question is the extent to which equivalent provincial parties, such as the B.C., Ontario or Alberta N.D.P., or the Ontario Liberals or Progressive Conservatives, would have access to these federal databases, and vice versa.

We also know that all parties adopt scoring systems, of one kind or another. The federal Conservative party's CIMS database rates voters on a scale of -15 to +15 (complete with smiley faces). The federal Liberal Party uses a 10-point score.[56] It is likely that the average voter is unaware of these practices and might very well object to their use. An access to information request to the B.C. NDP for "numerical rating and score" was refused on the grounds that the disclosure "would reveal confidential commercial information that if disclosed, could, in the opinion of a reasonable person, harm the competitive position of the organization."[57]

The consent provision also embraces the principle that the individual may withdraw his or her consent to having their information collected at any time. Only the federal Green Party offers a general "opt-out" statement: "If you wish to have any of your personal information removed from our databases, or if you no longer want us to send any further communications to you, please send an e-mail to membership@greenparty.ca."[58] As noted above, parties are expected to maintain internal do-not-call lists but are not required to regularly update their lists against the national do-not-call list maintained by the CRTC. The only other party that explicitly acknowledges that voters might place their names on the internal do-not-call list is the NDP: "If you no longer wish to be contacted by us or wish to be placed on our internal Do-Not-Call list, please let us know by emailing dnc@ndp.ca. You may also unsubscribe from our communications by using the unsubscribe mechanisms contained in all of our electronic messages."[59]

The Liberals also explain their responsibilities under CASL, and note that "electronic messages that we send are generally either those soliciting donations, which are specifically exempt under the law, or are messages of a political, not a commercial, character."[60] The policy continues: "As a best practice, we have an unsubscribe mechanism for our electronic messages, even where the law does not require us to do so."[61] The Conservatives only undertake to remove an e-mail address if such a request is submitted through their website.

---

56 Delacourt, *supra* note 4 at 307-308.

57 *Personal Information Protection Act*, *supra* note 28 at s 23 (3)(b); Correspondence, NDP Chief Privacy Officer, 31 May 2017.

58 Green Party of Canada, *supra* note 47.

59 New Democratic Party of Canada, *supra* note 47.

60 Liberal Party of Canada, *supra* note 47.

61 *Ibid.*

Principle 4 (Limiting Collection): ''The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means."

The fourth principle obliges organizations to specify the types of personal information necessary to perform the stated purposes. They should not collect personal information indiscriminately. They should also not collect information by misleading or deceptive means.

We know from prior research[62] that political parties capture PII from seven separate sources:

(1) from direct contact with voters (on the doorstep, through polling, subscriptions, registrations, donations, petitions);
(2) from third parties such as volunteers or friends;
(3) from the Voters List provided by Elections Canada;
(4) through social media;
(5) through publicly accessible sources, such as phone and professional directories;
(6) from commercial data brokers; and
(7) through engagement on the party website.

In that latter category, information may be *required* (when creating a user account, or when donating), *volunteered* (freely given in the wider campaign process), *observed* (when a user's browser accesses the campaign website) or *inferred* (computationally derived from the analysis of those other data).[63] We also know that parties will use non-identifiable sources of data, such as census tract data, for the analysis of broad geo-demographic patterns and trends.[64] The sources of personal data within the modern campaign are complex, and no political party at the federal level has, ostensibly, considered these complexities and adopted transparent practices.

This is how the Liberal Party of Canada declares what they obtain, and how they obtain it:

> We obtain the information that you choose to give us. You may do so in a variety of ways including:
>
> - when you visit our website for the purpose of becoming involved with the party as a member, volunteer or donor;
> - when you subscribe to our communications;
> - if you register at an event or at a Party convention;
> - if you complete a registration or donation form either electronically or on paper;
> - if you complete any other form on a Liberal website, including online petitions;

---

62 Bennett & Bayley, *supra* note 15.

63 Rubinstein, *supra* note 12.

64 Bennett & Bayley, *supra* note 15.

> • it 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 with the Liberal Party.
>
> The information that we collect may include:
>
> • Contact and identification information, such as your name, address, telephone numbers, e-mail address and social media contacts.
> • Donation information such as date and amount of your donation.
> • Financial information that we need to process your donation e.g. payment methods and preferences, billing and banking information (e.g. credit card number and expiry date).[65]

And here is what the Conservative Party of Canada says:

> Elections Canada provides all political parties with a list of electors, including names and postal addresses. We collect other information from publicly available data. We collect personal information from donors and members when they contribute to our Party or purchase a membership. You may also choose to provide us with personal information on a voluntary basis, such as when registering for an event or signing a petition. We are required by law to keep records of donors for tax purposes.[66]

Both statements can be questioned. The Liberal party clearly does not collect only personal data "that you choose to give us." Similar wording is included in the NDP's policy. And the Conservative Party does not just collect "other information from publicly available data."

Are there any sources of personal data that would be strictly off-limits for a political party? One obvious source is the information that might be captured by an elected official in their capacity as an elected official. All parties will try to administer a strict firewall between a Member of Parliament (MP)'s constituency office, or a Ministerial office, and the party. When a constituent contacts an elected official with a concern or a complaint, it is reasonable for the constituent to expect that those data will not be used for party political purposes. In 2006, Conservative Party MP Cheryl Gallant sent birthday cards to her constituents using data from passport applications. In October 2007, Rosh Hashanah cards were sent by the Prime Minister's office to supporters with Jewish sounding names, many of whom were reportedly unsettled by this practice, and left wondering how such a list could be compiled.[67] It should be quite straightforward for parties to state unequivocally that they do not collect personal data that might be voluntarily surrendered to the constituency offices of Ministers or MPs.

---

[65] Liberal Party of Canada, *supra* note 47.

[66] Conservative Party of Canada, *supra* note 47.

[67] There are other cases discussed in Bennett & Bayley, *supra* note 15.

Principle 5 (Limiting Use, Disclosure, and Retention): ''Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes."

This principle links use, disclosure, and retention also to that of purpose specification. The broader the purposes communicated, therefore, the broader the potential uses and disclosures.

All federal political parties give commitments along these lines. The Liberals declare:

> We will not, without your consent, use your personal information for any purpose other than as described in this privacy policy, except where permitted or required by applicable legislation. For example, under the Canada Elections Act, we are required to provide Elections Canada with our donors' names, addresses and contribution amounts.
>
> We also use your personal information to communicate with you about the Liberal Party and its activities, as well as to provide you with news and information. We use your financial information to process your contributions. If you have been a contributor, we may contact you again to seek your financial support. Under no circumstances, however, do we sell your personal information.[68]

The Conservative party states: ''We use your personal information to communicate with you . . . As a national organization with a riding-based membership system, your personal information may also be disclosed to our local riding associations, candidates, nomination contestants and leadership contestants."[69] And the federal NDP will ''use your personal information to communicate with you about the NDP and our activities . . . As we are a federal party, we may share your information internally within our national organization, including with NDP riding associations."[70] A similar statement is included within the privacy policy of the federal Green Party, and the same question is relevant in their case as well. The NDP and the Green Party also acknowledge that they will need to comply with federal law with respect to the processing of donations.

Only the Liberal party acknowledges that it engages

> . . . third party providers to perform tasks on our behalf such as processing your donation, making phone calls and providing technical services to our website. When information is shared with third parties for these purposes, we include privacy protective clauses in written contracts to help safeguard personal information.[71]

---

[68] Liberal Party of Canada, *supra* note 47.

[69] Conservative Party of Canada, *supra* note 47.

[70] New Democratic Party of Canada, *supra* note 47.

[71] Liberal Party of Canada, *supra* note 47.

With respect to the retention of personal information, no federal political party makes any explicit commitment that they will only retain information for a specified period.

Principle 6 (Accuracy): ''Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used."

This principle is one in which the interests of the organization and those of the data subject typically overlap. The principle imposes three sets of obligations — accuracy, completeness, and contemporariness. Non-compliance with any one of those standards can severely affect the interests and rights of the individual.

Anecdotally, we know that the information contained in party databases can be inaccurate, incomplete and out-of-date. Much is entered during the frenzy of competitive election campaigns by a host of party workers and volunteers who may not have any training in privacy and security standards. Names can be misspelled, address numbers confused, responses inaccurately recorded and entered, and so on. The occasional attempts by individuals to exercise their access to personal information rights have revealed some extraordinary errors.[72]

The federal Conservative Party states, "we always try to keep your personal information accurate and up-to-date."[73] Very similar wording is used by the NDP The Green Party "strive to ensure that any personal information we retain and use is as accurate, complete and up-to-date as necessary for the purposes for which we will use it."[74]

Principle 7 (Safeguards): ''Personal Information must be protected by appropriate security relative to the sensitivity of the information."

The security principle embraces physical, organizational, and technological measures. The nature of the safeguards should vary depending on the sensitivity of the information. Since the standard was adopted, data breaches have become increasingly widespread and frequent. Recent regulations under the *Digital Privacy Act* oblige organizations to comply with certain notification provisions in the event of a data breach.

Political parties operate in a highly competitive environment and do take measures to protect the personal data under their control. They implement role-based access controls to their voter management databases, like CIMS, Liberalist, and Populus, and they claim to take appropriate security measures to safeguard those systems from unauthorized access, disclosure, or loss. Only the Green Party goes so far as to specify the kind of encryption used, and that it undergoes periodic security audits.

---

[72] Andrew McLeod, "NDP Collects Personal Data and Gets it Stunningly Wrong," *The Tyee* (23 January 2018), online: < thetyee.ca/News/2018/01/23/NDP-Collects-Personal-Information-Wrong/ > .

[73] Conservative Party of Canada, *supra* note 47.

[74] Green Party of Canada, *supra* note 47.

As far as we know, no federal political party in Canada has suffered a serious data breach or been subjected to a broad denial of service attack. There have, however, been reports at the provincial level. For example, it has been reported that the CIMS of the Progressive Conservative Party of Ontario was hacked in November 2016, through a ransomware virus, a fact that only came to light two months later.[75] More common are the anecdotal incidents where party workers inappropriately use party databases to find out how people they know have voted, or to satisfy their curiosity about the political affiliations of notable people who live in their riding. In the 2018 Ontario provincial election, one Conservative candidate resigned after accusations that he had illegally accessed customer data from the 407 ETR toll highway in Toronto.[76] Access to databases can, of course, also be used to encourage stalking behaviour.

All databases carry serious risks of abuse; party databases are no exception. In response to the global publicity regarding foreign influence in the U.S. presidential election, the Government of Canada asked the Communications Security Establishment (CSE) to conduct an overall security and risk assessment of cyber threats to Canada's democratic process. In its June 2017 report, the CSE identified the stealing or manipulation of party databases as one of the key vulnerabilities to hackers, cybercriminals, and cyber-espionage.[77] The CSE reportedly made its security consultants available to the main parties for advice on how to improve their security procedures.[78]

Principle 8 (Openness): ''An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.''

Organizations should be open about policies and practices. Individuals should not have to make unreasonable efforts to find out how an organization processes personal data. That information should be provided in an understandable format.

There now exists considerable literature critiquing privacy policies, and helpful recommendations from privacy commissioners and others about how

---

[75] ''Ontario Progressive Conservative Party database hacked,'' *CP24 News* (28 January 2018), online: < www.cp24.com/news/ontario-progressive-conservative-party-database-hacked-sources-1.3779326 > .

[76] ''Ford says Ontario PCs looking into allegations involving candidate who resigned,'' *The Globe and Mail* (17 May 2018), online: < www.theglobeandmail.com/canada/article-ford-accepted-ontario-pc-candidates-resignation-after-learning-about/ > .

[77] Communications Security Establishment, ''CyberThreats to Canada's Democratic Process,'' online: < www.cse-cst.gc.ca/sites/default/files/cse-cyber-threat-assessment-e.pdf >

[78] ''Despite risk of cyber attacks, political parties still handle Canadians' data with no rules in place,'' *The Star* (19 June 2017), online: < www.thestar.com/news/canada/2017/06/19/despite-risk-of-cyber-attacks-political-parties-still-handle-canadians-data-with-no-rules-in-place.html >

best to frame and communicate these policies so that they do not confuse the individual. The 2014 guidelines by the OPC on consent, for instance, advise that:

> - Privacy policies should have a full description of what information is collected, for what purposes it is used, and with whom it is shared.
> - Privacy policies should be easily accessible, simple to read, and accurate.
> - Organizations should regularly review their privacy policies and update them as necessary.[79]

The regular "privacy sweeps" conducted by the Global Privacy Enforcement Network (GPEN) frequently find that privacy notices are "too vague and often inadequate."[80] Many, of course, are generated by automated "privacy policy generators" and are often designed to mitigate legal liability, rather than to provide clear and meaningful information to individuals about how their data is collected, managed, and disclosed. There is a "transparency paradox" at work: a tension between providing information about an organization's practices in sufficient detail to satisfy the relevant legal requirements and provide sufficient contextual information and giving information that the consumer will actually read.[81]

The privacy policies of the federal and provincial political parties do not suffer from that problem. They are generally quite brief and readable. The question, however, is whether or not they represent the public face of a more complex set of policies and procedures to which the ordinary citizen does not have access. Many companies that are subject to *PIPEDA* will generate a short form notice for their website, with appropriate links to more detailed policies which may be accessed if the individual is interested. Nothing like that is apparent for political parties in Canada. It seems that what you see, is what you get. Efforts to dig behind these policies to explore their deeper meaning and understand how they reflect actual practices are often met with considerable resistance. In the absence of a regulatory requirement to do so, the common practice is to say as little as possible, to dress up statements of policy in broad language, and to use the opportunity of engagement over privacy to solicit support.

---

[79] Office of the Privacy Commissioner of Canada, "Guidelines for Online Consent," online: < www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405/ > .

[80] Adam Stevens, "GPEN Sweep 2017 — International Enforcement operation finds website privacy notices are too vague and generally inadequate," *Global Privacy Enforcement Network* (24 October 2017), online: < www.privacyenforcement.net/node/906 > .

[81] Helen Nissenbaum, "A Contextual Approach to Privacy Online" (2011) 140:4 Daedalus 32.

Principle 9 (Individual Access): ''Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."

The access and correction principle is central to any privacy protection policy. The principle is, of course, subject to certain exemptions. The organization is also obliged to inform the individual of the organizations to which that information might have been divulged. The response should come within a reasonable time, and at minimal or no cost.

The only federal political party that has made a commitment to provide a right of access is the federal Green Party:

> We strive to ensure that any personal information we retain and use is as accurate, complete and up-to-date as necessary for the purposes for which we will use it. We do not routinely update personal information except where and as necessary for these purposes. If however our records regarding your personal information are inaccurate or incomplete, we will amend that information at your request. At your request we will provide to you a statement explaining the extent to which we hold personal information about you, and we will explain how that information has been used by us.[82]

The federal NDP will "aim to keep your information accurate and up-to-date. To update and correct the personal information you provide to us, please contact us at info@ndp.ca."[83]

Rights of access and correction are sometimes seen as a threat to political parties. They raise the prospect of frivolous and vexatious requests by opposition members during election campaigns, thus tying up or diverting crucial human and financial resources. In reality, political parties in Europe and in many other parts of the world are subject to these laws, and there is no evidence that they are abused for partisan purposes.

Principle 10 (Challenging Compliance): ''An individual shall be able to challenge an organization's compliance with the above principles to the designated individual or individuals accountable for the organization's compliance."

Whether or not an entity is legally required to implement these privacy protection standards, it has to accept the principle that the individual has rights of complaint and redress. This requires, of course, an acceptance of fact that personal information is a valuable resource that is provided to organizations for defined, limited, and transparent purposes. It also, of course, demands an organizational commitment to the assignment of responsibility to a designated individual, and to the establishment of a clear process through which complaints may be received and handled. That process requires more than the mere

---

[82] Green Party of Canada, *supra* note 47.

[83] New Democratic Party of Canada, *supra* note 47.

publication of an institutional e-mail address to which questions or concerns might be communicated, as seems to be the practice for most political parties in Canada.

IV. THE B.C. *PERSONAL INFORMATION PROTECTION ACT* AND POLITICAL PARTIES

Political parties in British Columbia are covered by *PIPA*, which, unlike its equivalents in Alberta and Quebec, defines an organization to include "a person, an unincorporated association, a trade union, a trust or a not for profit organization."[84] Its application is therefore not limited to commercial activities. However, it should also be noted that B.C.'s *PIPA* does not apply to "the collection, use or disclosure by a member or officer of the Legislature or Legislative Assembly of personal information that relates to the exercise of the functions of that member or officer."[85] Similar exemptions for provincial politicians appear in other provincial information and privacy statutes relating to the public sector.

It took a while, however, for B.C.'s political parties to fully accept both their obligations under the legislation and the jurisdiction of the Office of the Information and Privacy Commissioner of B.C. (OIPCBC). It wasn't until 2011 that the Commissioner investigated a complaint against the NDP, concerning the practice of requiring prospective leadership candidates to submit their passwords for any social networking services to which they were subscribed. The Commissioner found that the collection was excessive and used the case to issue broader guidance on social media background checks.[86] During the provincial election campaign of April 2017, the Acting Commissioner was asked to investigate a complaint from the B.C. Liberals about the sharing of supporters lists by the NDP The Commissioner refused to investigate, but instead announced a general investigation in September 2017 regarding whether the main political parties are in compliance with *PIPA*.[87] A further interesting dimension of the issue is the extent to which federal political parties are collecting personal information in British Columbia. The law is untested, and there has been no detailed legal analysis, but it can be argued that the federal parties are also acting as non-profit organizations under *PIPA*, and would therefore be subject to the various requirements of the B.C. legislation with regards to their personal information practices within British Columbia.

---

84 *Personal Information Protection Act*, *supra* note 28, s. 1.

85 *Ibid,* s. 3.

86 British Columbia, Office of the Information and Privacy Commissioner, "Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's use of social media and passwords to evaluate candidates," P11-01-MS, online: < www.oipc.bc.ca/mediation-summaries/1399 > .

87 Office of the Information and Privacy Commissioner for British Columbia, News Release, *supra* note 34.

As expected, therefore, the main B.C. political parties (NDP, B.C. Liberal and B.C. Green Party) have done somewhat more than their federal counterparts to demonstrate compliance, even if it has been late, and under pressure. Both the B.C. Liberals and the B.C. Green Party have published a "Privacy Policy" linked from their respective websites. The B.C. NDP has published a "Data Use Policy," although it is unclear to the casual reader whether this policy applies only to data collected through the website, or whether its scope is broader. With respect to accountability, both the B.C. Liberals and the B.C. Green Party name the official concerned. All three parties publish dedicated e-mail addresses for privacy.

Furthermore, when the B.C. parties were required to think more seriously about what personal information they collect and why they collect it, they came up with a far longer list. For instance, the privacy policy of the B.C. Liberal Party (BCLP) contains an explicit "Purpose" principle:

> BCLP collects your personal information for the following purposes:
>
> - to authenticate your identity;
> - to send you any communications relating to BCLP, including, without limitation, BCLP newsletters, promotional materials, campaign materials and fundraising emails, unless you state that you do not wish to receive these communications. If you do not want to receive such communications send an email at any time to privacyofficer@bcliberals.com;
> - to facilitate your participation as a volunteer and/or a member of BCLP;
> - to determine which topics of discussion may be of particular interest to you;
> - to provide and administer an online ideas sharing forum, including without limitation to provide you with the ability to post ideas, comments and information on the website, and to personally identify you as the contributor of such ideas, comments and information;
> - to protect BCLP, yourself and others from fraud and error;
> - when accessing and using our website, we will use web statistics and Internet Protocol (IP) addresses for internal and system improvement purposes, in order to find web browser trends, gather broad demographic information and administer the website. Data will not be compiled on your personal information and the site logs will be deleted on a monthly basis.[88]

The B.C. Green Party say this:

> We will only collect constituent information that is necessary to fulfill the following purposes:
>
> - To verify identity;

---

[88] The Liberal Party of British Columbia, "Privacy Policy," online: < www.bcliberals.com/privacy-policy >.

- To identify constituents' preferences;
- To understand the needs of our constituents;
- To open and manage an account;
- To deliver requested pertinent information and services;
- To enroll the constituent in a program;
- To send out Green Party membership information;
- To contact our constituents for fundraising;
- To ensure a high standard of service to our constituents;
- To meet regulatory requirements;[89]

These statements reflect the fact that political parties capture personal data on different categories of individuals (voters, volunteers, donors), and the purposes for collection are subtly different in each case.

The B.C. parties have also begun to grapple with the question of consent. Here is the statement of the B.C. Liberal Party:

> BCLP will obtain your consent to collect, use or disclose personal information except where BCLP is authorized or required by PIPA or other law to do so without consent.
> Your consent may be express or implied, or given through your authorized representative.
> Consent may be provided orally, in writing, electronically, through inaction (such as when you fail to notify BCLP that you do not wish your personal information collected/used/disclosed for optional purposes following reasonable notice to you) or otherwise. For example, oral consent could be expressed over the telephone at the time information is being collected; electronically when submitting an agreement, online submission or request for services or other information; or in writing when signing an agreement.
> You may withdraw your consent at any time, subject to legal or contractual restrictions, provided reasonable written notice of withdrawal of consent is given by you to BCLP. Upon receipt of your written notice, BCLP will inform you of the likely consequences of the withdrawal, which may include the inability of BCLP to give you access to the website or provide certain services for which the delivery of that information is a prerequisite.[90]

The B.C. Green Party offers a similar statement, but also adds:

> We may collect, use or disclose personal information without the constituent's knowledge or consent in the following limited circumstances:
>
> - When the collection, use or disclosure of personal information is permitted or required by law;

---

[89] The Green Party of British Columbia, "Privacy Policy," online: < www.bcgreens.ca/privacy > .

[90] Liberal Party of British Columbia, *supra* note 88.

- In an emergency that threatens an individual's life, health, or personal security;
- When the personal information is available from a public source (e.g., a telephone directory);
- When we require legal advice from a lawyer;
- For the purposes of collecting a debt;
- To protect ourselves from fraud;
- To investigate an anticipated breach of an agreement or a contravention of law.[91]

A further notable difference is in each party's commitment to allowing rights of access and correction. The B.C. Liberal Party, "upon written request and authentication of identity . . . will provide your personal information under its control. BCLP will also provide you with information about the ways in which that information is being used and a description of the individuals and organizations to whom such information has been disclosed."[92] They acknowledge that they may charge a "minimal fee," that they will respond within 30 days, and that exemptions may apply. The B.C. Green Party make very similar commitments. The B.C. NDP commits that "any time, individuals may request access to, correction, or deletion of their personal information *as retained by any of the features discussed above*."[93] This last qualifier signifies an essential difference in the NDP's approach. Their "Data Use Policy" is not structured around the common set of privacy principles, but around the processes through which the NDP might capture personal data: donations; joining the NDP; email campaigns; petitions; "tell us your story"; share your ideas; send a message; volunteer and job applications; request an election sign; contests; sharing content on social media sites; e-newsletters; and cell phone information. A recent test of access request by a local journalist, however, revealed delays in response, and a very partial provision of personal information, by only one party.[94]

A final interesting difference is the reference in two of the B.C. policies to social media. The B.C. Liberal Party, for instance, addresses the question of personal information shared through the "Sharethis" or other social media icons on their website, and is careful to indicate that the party is not responsible for their privacy and data gathering practices. The B.C. NDP acknowledges that it "tracks the volume of sharing" but "at no time does the B.C. NDP collect the personal information of senders or recipients."[95] No political party

---

91 Green Party of British Columbia, *supra* note 89.

92 Liberal Party of British Columbia, *supra* note 88.

93 New Democratic Party of British Columbia, "Data Use Policy," online: <www.bcndp.ca/data-use>.

94 This experience reflects earlier attempts at access to personal requests by the author. Andrew MacLeod, "BC's Parties Mum on What They Know About You" *The Tyee* (16 January 2018), online: <thetyee.ca/News/2018/01/16/BC-Parties-What-They-Know-About-You/>.

95 New Democratic Party of British Columbia, *supra* note 93.

acknowledges, however, that it will capture the information of Facebook friends or Twitter followers. Yet, these are presumably very valuable indicators of support, or potential support. And no political party acknowledges that it, or its candidates, might use the services of third party platforms such as *Nationbuilder* for outreach programs.

The initial B.C. experience is instructive. These initial privacy policies may still be critiqued for vagueness and incompleteness, and they are currently under review by the OIPCBC. Yet, they do signify the results of some careful internal analysis. They prove that comprehensive assessments of political parties' collection, use, and disclosure practices are possible and potentially valuable, and they raise the bar for political parties of all ideological persuasions across the rest of Canada.

CONCLUSIONS

Political parties may capture personal information from a variety of different sources on voters, donors, candidates (and prospective candidates), and employees and volunteers. They capture those data for a variety of purposes. None of this activity is necessarily controversial or nefarious. Some data (on donors) has to be collected and reported by law. Parties have a duty in our democracy to educate voters about their policies and promises, and to encourage them to participate in the system. The public interest on the other side of the privacy equation is a very important one.

That said, parties' privacy policies are often difficult to find. Their scope is often unclear. With a couple of exceptions, they do not address all 10 privacy principles. Accountability and complaints mechanisms are often not clearly publicized. Many are silent on procedures for the access and correction of data and unsubscribing from lists. Vague and expansive statements of purpose are quite common.

Yet, there is evidence, mainly in British Columbia and as a result of regulatory pressure, that parties have begun to comprehensively and seriously consider the range of obligations that adherence to contemporary privacy standards entails. This process of self-assessment and reflection is beneficial to any organization. It allows the organization to investigate their own systems and processes, and determine their desired privacy management practices. There are now a smattering of commitments and acknowledgements at both the federal and provincial level, a marginally greater level of transparency, an acceptance of broad responsibility to manage personal data responsibly, and certain new accountability mechanisms. That said, this analysis suggests two broad conclusions.

First there should be a harmonization of policy and practice across the political spectrum. The analysis above demonstrates quite clearly that the 10 principles can be adapted and applied to the electoral context. There is no obvious reason why registered political parties should be making different commitments with regard to these basic principles. The scattered approach,

however, reflects a quite minimalist approach and attitude, and a reluctance to think through what information is captured, why it is captured, who has legitimate access to it, and so on. It is also probably the case that parties already do much to protect the personal information under their control, but have not conveyed those activities carefully and transparently to the public. We know, for instance, that all parties implement access controls over their party management databases, with different levels of ''role-based'' access depending on the need to know. None of those clear commitments appear as public statements in the privacy policies.

The second general plea is for more transparency. Organizations typically face backlash and sanctions regarding privacy protection when they are caught engaging in activity about which they have not been transparent. The natural competitiveness of the electoral arena should not generate knee-jerk secrecy and suspicion. Canada is only one of a handful of democracies where parties do not have to abide by basic privacy obligations. Evidence from other countries suggests strongly that parties can abide by privacy protection rules without difficulty.

The political party is a different breed of organization. They have unique needs, roles, and cultures. They need personal data. They also need the trust of the citizenry. Although it may be difficult in the foreseeable future to contemplate the extension of federal privacy legislation to political parties, there is much that can, and should, be done to promote self-regulation. The 10 privacy principles contained in the national standard of Canada, and in *PIPEDA*, are the obvious starting-point.