THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Bill C-76, *Elections Modernization Act*

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION

November 2018

500–865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the Privacy and Access Law Section, with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Policy Committee and approved as a public statement of the Privacy and Access Law Section.

TABLE OF CONTENTS

Bill C-76, *Elections Modernization Act*

Bill C-76, *Elections Modernization Act*

I. INTRODUCTION

Although Canada now has a relatively comprehensive scheme for privacy protection in both public and private sectors, one area of public activity remains effectively unregulated—the collection, use and disclosure of Canadians' personal information by political parties.

Under current law, federal political parties are not subject to the *Personal Information Protection and Electronic Documents Act*[1] (PIPEDA), which applies to commercial activities except where an equivalent provincial or territorial law applies, or to the *Privacy Act*[2] which applies to public sector activities at the federal level. Canadian provinces and territories similarly lack regulation in this area. British Columbia's *Personal Information Protection Act*[3] is the only privacy legislation in Canada applying to political parties. This is a significant legislative gap that requires Parliament's attention. The Canadian Bar Association's Privacy and Access Law Section (CBA Section) is pleased to have the opportunity to comment on Bill C-76, *Elections Modernization Act*[4] on this issue.

The June 2018 report of the House of Commons Committee on Access to Information, Privacy and Ethics (ETHI Committee), "Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process" concluded that:

> Canadians would have greater confidence if they knew that their political parties were not exempt from privacy legislation and that they have legal responsibilities similar to those imposed on public and private organizations under the *Privacy Act* and PIPEDA. Any legislative amendment should obviously take the special activities of political parties into account so as not to entirely prevent the use of personal information, but rather to better regulate its collection and use and the transparency surrounding the management of such information.[5]

---

1 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5

2 *Privacy Act* , RSC 1985, c P-21

3 *Personal Information Protection Act,* SBC 2003, c. 63

4 Bill C-76, *Elections Modernization Act*

5 ETHI Committee, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process* (June 2018)

The CBA Section agrees and believes this can best be achieved by amending Bill C-76 to require political parties' privacy policies to comply with globally recognized privacy and data protection principles and to ensure compliance by granting the Privacy Commissioner of Canada authority to investigate complaints.

II. ANALYSIS OF BILL C-76

A. Compliance With Data Protection Principles

The websites for the three largest national political parties include privacy policy statements that commit to respecting privacy principles and identifying a privacy officer to address voter concerns. Yet not being subject to privacy laws means political parties operate in an environment without standards for privacy protection and with no recourse available to citizens. The fact that information can be collected by political parties about citizens without their informed consent and with no legal right to see it, control its distribution or to correct errors or remove it from parties' databases should they choose is increasingly out of step with broader legal and ethical norms. For more than ten years, Canada's Privacy Commissioners have advocated for the application of data protection principles to political communication activity.

Bill C-76 proposes to amend the *Canada Elections Act*[6] to require each political party to have a policy for the protection of personal information, to publish the policy on its website and to provide it to the Chief Electoral Officer.[7] This will create a framework and mechanism to inform citizens of the types of personal information political parties collect about them, and how that information is used and disclosed.

The CBA Section applauds the government's initiative to bring political parties into the privacy protection scheme, but offers suggestions to better reflect globally-accepted privacy and data protection principles. Political parties should also be subject to:

- limits on the direct collection of personal information;
- additional limits on the indirect collection of personal information;
- limits on retention of personal information;
- limits on the use of personal information;
- limits on disclosure of personal information;

---

6 *Canada Elections Act*, S.C. 2000, c. 9

7 *Supra* FN 4, Bill C-76, sections 254-260

- the requirement to obtain informed consent from individuals for all collection, use and disclosure of their personal information other than in specified circumstances;
- the right of individuals to withhold or withdraw consent to the collection, use and disclosure, and the corresponding obligation of parties to destroy and cease collecting personal data on request;
- a requirement to keep personal data secure (and to use secure destruction methods) and to notify affected individuals of security breaches that pose a risk of significant harm to them;
- accountability standards, including responsibility for personal data they have shared with third parties; and
- individual rights to access their personal data held by political parties, and to have data corrected or removed from the party's database.

We analyze some of these globally-accepted privacy and data protection principles below.

B. Indirect Collection of Personal Information

Bill C-76 proposes to add to subsection 385(2) of the *Canada Elections Act*:

> 385 (1) The leader of a political party may apply to the Chief Electoral Officer for the political party to become a registered party.
>
> (2) The application for registration shall include…
>
> ***(k) the party's policy for the protection of personal information, including***
>
> ***(i) a statement indicating the types of personal information that the party collects and how it collects that information***…

This amendment appears to require nothing more than a general statement without any direction or objective standard against which the sufficiency of the statement can be measured. A general statement does not suffice. More definition of the specifics required in the statement is needed.

We know that political parties in Canada match voter list information with information acquired from data brokers and other third parties. Professor Colin J. Bennett has observed that:

> Thus, more data on voters are being captured and those data are increasingly shared through a complicated and dynamic network of organizations involving some quite obscure companies that play important roles as intermediaries between the voters and their elected representatives.[8]

8 Evidence from Professor Bennett, ETHI Committee, April 26, 2018

The political party's policy should be required to commit to providing details about the data elements collected, as well as the source and contact information for the supplier of that personal information.

Political parties purchase personal digital information about Canadians through companies specializing in this field, for example selling data on the consumption habits or debt levels of customers. These data brokers are commercial intermediaries that generate databases using various methods, then sell the information, almost always without users knowing it.

One current example is AggregateIQ, a Cambridge Analytica intermediary, that harvested personal information about users through a digital application linked to Facebook and resold that information to its clients to target voters and other segments of the population.[9]

Direct collection of personal information from the individual is the accepted practice in modern privacy laws and when done indirectly, the data subject must be notified. This standard should be reflected in Bill C-76.

C. Disclosure

Privacy policies of political parties should clearly explain the intended disclosure of personal information. Canadians are increasingly educated about the use and disclosure of their personal information, especially with the exponential advancement of technology. Common practices for disclosure requirements must apply to political parties so Canadians understand —and can make informed choices—about the intended disclosure of their personal information.

D. Breach Notification

Despite best intentions, like all other users of data, political parties can be subject to security breaches by reason of human or technological error. In fact, in June 2017, Canada's Communications Security Establishment identified political parties, politicians and media as uniquely vulnerable targets for cyber-attack:

> We expect that multiple hacktivist groups will very likely deploy cyber capabilities in an attempt to influence the democratic process during the 2019 federal election…we expect some influence activities will be well-planned and target more than one aspect of the democratic process.[10]

---

9 See CBA news online, Gap in privacy law leaves elections open to 'misuse' of personal information (Nov 1/18); also Daniel Therrien, Privacy Commissioner of Canada, ETHI Committee, November 1, 2018

10 Canada, Communications Security Establishment, *Cyber Threats to Canada's Democratic Process*, p. 4

This threat has been repeatedly realized in global elections in the last two years. There is a real risk that personal information in the hands of political parties will be the target of attacks by organizations attempting to unfairly influence the outcome of elections. Individuals whose personal information has been disclosed or improperly accessed should be informed where breaches pose a real risk of significant harm to them.

Mandatory reporting of a breach is accepted as a basic privacy protection principle, evidenced by PIPEDA amendments that took effect on November 1, 2018. Yet Bill C-76 does not require notification in the event of a breach. This basic standard should apply to political parties.

E. Training

Political parties can, and do, collect a significant amount and variety of information on Canadian citizens, the scope of which is only beginning to be understood. Exacerbating this is the fact that election campaigns are run by relatively few paid workers and thousands of others who volunteer their support for political parties and candidates. Given the nature of staffing campaigns, it is likely that a disparate and fluctuating number of employees and volunteers have access to extensive personal data with no guarantee they have undertaken privacy training.

Former BC Commissioner Elizabeth Denham issued several reports on political parties, including *Investigation Report F13-04 Sharing of Personal Information*. In that report, she observed:

> [Employees and volunteers] are not receiving sufficient training. Given the obvious potential for overlap of individuals who have, or had, government and party roles, I believe this to be a fundamental problem that government and the BC Liberal Party need to address. The lack of training increases the risk of employee misuse of the personal information of British Columbians and reflects a culture that is not placing enough importance on duties related to protection of privacy and access to information.[11]

Section 254 of Bill C-76 addresses the political party's privacy policy with respect to training political party *employees*. Given the structure and activities of political parties, Bill C-76 should be amended to require that the party's privacy policy indicate the privacy training to be given to volunteers, as well as employees, who could have access to personal information under the party's control.

11 Elizabeth Denham, *Investigation Report F13-04 Sharing of Personal Information* (August 2013), p. 23

F. Enforcement

The deregistration remedy in Bill C-76 for a breach of the *Canada Elections Act* is a very powerful remedy. We presume it would be rarely invoked. Privacy breaches are not all the same. Some breaches may involve thousands of voters and large datasets, others ambiguous wording in a privacy notice, inadequate privacy training, a lack of sufficient training materials for campaign workers or other less egregious circumstances. We recommend that the authority overseeing compliance with privacy requirements be equipped with a robust set of tools including educational measures, compliance agreements and other responsive measures to ensure that privacy breaches will be addressed appropriately.

G. Independent Oversight

Complaints about privacy violations should be reviewed and resolved externally, by the Office of the Privacy Commissioner, and not by the parties themselves according to their own internal policies or by the Chief Electoral Officer.

The Office of the Privacy Commissioner has 30 years of experience addressing public sector privacy issues and, since 2001, private sector privacy issues. Any federal statute that addresses privacy compliance by political parties should be overseen by the Privacy Commissioner. There is a risk of inconsistent and even conflicting interpretation of privacy requirements if privacy oversight is fragmented and divided among several officials. The lack of harmonization may also contribute to weaker compliance with privacy laws.

If Parliament determines that, notwithstanding this concern, oversight should remain exclusively with the Chief Electoral Officer, as currently proposed, it should consider a statutory requirement for consultation with the Privacy Commissioner if a breach or a privacy complaint comes to the attention of the Chief Electoral Officer.

Similarly, if a breach with the potential to impact the integrity and security of Canada's election system comes to the attention of the Privacy Commissioner, the Privacy Commissioner should have an obligation to inform the Chief Electoral Officer, so the Chief Electoral Officer has an opportunity to understand the nature, scope and risks of the breach and take steps to mitigate possible damage.

III. LESSONS FROM OTHER JURISDICTIONS

When the BC government introduced Bill 20 – *Election Amendment Act*[12] in March 2015, then-Privacy Commissioner Denham sent an open letter to the Attorney-General and Minister of Justice, expressing concerns about personal information, compiled by the Chief Electoral Officer for efficiently administering elections, being given to political parties for their unrestricted use. She recommended that:

- there be clear limitations on what constituted use of personal information for "electoral purposes";
- political parties be prohibited from using the information for commercial purposes or disclosing the information to any other organization or public body; and
- voter participation information disclosed under Bill 20 be destroyed following the election.

The BC Government introduced further amendments to Bill 20 that addressed in part the first two of these concerns.[13]

In the European Union, political parties are captured as "data controllers" under the General Data Protection Regulation (GDPR).[14] In the United Kingdom, the Information Commissioner issued Guidance for political parties campaigning or for promotional purposes[15] to supplement the inclusion of political parties under the scope of its *Data Protection Act*.[16] The Guidance was updated to include political parties and candidates after learning of complaints that some political parties were contravening the rules that led to the unlawful targeting of thousands of voters.[17] Recently the U.K. Commissioner at the Institute of Directors Digital Summit spoke about the office's investigations into political parties' use of personal information and the importance of this issue.[18]

---

12 Bill 20, Election Amendment Act, 2015

13 Statement from B.C. Information and Privacy Commissioner regarding proposed amendments to Bill 20 (Election Amendment Act) (May 2015)

14 European Union, General Data Protection Regulation

15 U.K. Information Commissioner's Office, Guidance For Political Parties for Campaigning or for Promotional Purposes

16 U.K., *Data Protection Act* (1998)

17 Council of European Union, Data Protection (April 2016)

18 Institute of Directors Digital Summit, 2017

In 2011, the Irish Data Protection Commission[19] cautioned political parties in advance of a general election to communicate with voters by text, email or phone only if they have the voter's consent to the collection of contact information. The Irish Commissioner was particularly concerned with political parties collecting personal information through third parties and using the information to send campaign messages.

From 2012 to 2015, the Office of the Hong Kong Privacy Commissioner for Data Protection received 97 inquiries and 200 complaints related to electioneering activities. This led to the Commissioner's office updating its Guidance Note on Electioneering Activities to furnish candidates with guidance on compliance with the Personal Data (Privacy) Ordinance.[20]

Although political parties are exempt from the Australian *Privacy Act*, the Australian Law Reform Commission recommended in *For Your Information: Australian Privacy Law and Practice* that:

In the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community. Unless there is a sound policy reason to the contrary, political parties and agencies and organizations engaging in political acts and practices should be required to handle personal information in accordance with the requirements of the Privacy Act.[21]

IV. CONCLUSION AND RECOMMENDATIONS

The CBA Section has considered a number of options for best applying globally-accepted privacy and data protection principles to political parties, including administrative options, amending existing privacy legislation to apply to political parties, enacting stand-alone privacy legislation for political parties, and amending the *Canada Elections Act*. In light of Bill C-76 and the additions to the *Canada Elections Act,* we believe the most efficient way of ensuring the privacy of personal information in the hands of political parties is to amend Bill C-76 to:

- Require that political parties establish privacy policies which, at a minimum, meet the standards in Schedule 1 to PIPEDA.
- Revise the proposed new subsection 385(2) of the *Canada Elections Act* after paragraph (j) to read:

  (k) the party's policy for the protection of personal information must reflect and be consistent with the *Model Code for the Protection of Personal*

19 Irish Data Protection Commission

20 Guidance Note on Electioneering Activities, Office of the Privacy Commissioner for Personal Data, Hong Kong

21 For Your Information: Australian Privacy Law and Practice (August 2008)

Information (Schedule 1 to the *Personal Information Protection and Electronic Documents Act*); and

- Grant the Office of the Privacy Commissioner authority to investigate complaints relating to the collection, use and disclosure of personal information by political parties.