



THE CANADIAN
BAR ASSOCIATION
L'ASSOCIATION DU
BARREAU CANADIEN

April 27, 2018

Via email: di.minister-ministre.id@pco-bcp.gc.ca; terry.mercer@sen.parl.gc.ca; ciec-ccie@parl.gc.ca; info@elections.ca

The Honourable Scott Brison, P.C., M.P.
Acting Minister of Democratic Institutions
House of Commons
Ottawa, ON K1A 0A6

The Honourable Terry M. Mercer
Senate of Canada
Ottawa, ON K1A 0A4

Mr. Mario Dion
Office of the Conflict of Interest and Ethics
Commissioner
Parliament of Canada
Centre Block, P.O. Box 16
Ottawa, ON K1A 0A6

Mr. Stéphane Perrault
Acting Chief Electoral Officer
Elections Canada
30 Victoria Street
Gatineau, QC K1A 0M6

Dear Minister Brison, Senator Mercer, Commissioner Dion and Acting Chief Electoral Officer Perrault:

Re: Bill C-50 – Privacy Protection for Canadian Electors and *Canada Election Act* Amendments

I am writing on behalf of the Canadian Bar Association Privacy and Access Law Section (CBA Section), in connection with Bill C-50, *An Act to amend the Canada Elections Act*, and the need to enhance privacy protection for Canadian electors.

The Canadian Bar Association is a national association of 36,000 members, including lawyers, notaries, academics and students across Canada, with a mandate to seek improvements in the law and the administration of justice. The CBA Section comprises lawyers across Canada with an in-depth knowledge of privacy and access to information law and policy.

The CBA Section has closely followed the development of Bill C-50 and supports enhanced openness and transparency for political fundraising. However, conspicuously absent from the Bill are any amendments aimed at giving Canadian electors robust privacy protection. We encourage you to consider ways, including possible amendments to the *Canada Election Act* (CEA), to fix the legislative gap for the unregulated collection, use and disclosure of Canadians' personal information

by political parties. The recent media reports about Cambridge Analytica and AggregateIQ's unauthorized access and use of Facebook user profiles to build voter profiles ahead of the US elections and Brexit campaigns highlights the necessity of protecting Canadians' privacy rights.

Current application under Canadian law

Political parties are not subject to federal privacy laws. Neither the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to commercial activities of private sector entities, nor the *Privacy Act*, which applies to federal institutions, covers political parties. This legislative gap is significant, considering the vast amount of personal information of Canadians that federal political parties currently collect, use and disclose without their consent. Basic privacy protections that apply in virtually all other aspects of Canadians' lives do not apply to political parties, including data breach guidelines and anti-spam laws. Voter intelligence has become big business and data and privacy protection laws need to keep up. The allegations against Cambridge Analytica, Facebook and AggregateIQ only underscore this reality.

Professor Colin Bennett at the University of Victoria has considered the subject of privacy protection and voter surveillance in detail. In *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis*, he remarks that:

parties are managing vast databases within which a variety of sensitive personal information from disparate sources is processed. For the most part, individuals have no legal rights to learn what information is contained therein, 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.

Canada's Privacy Commissioner has also identified the need for legislated privacy protection¹ in the context of political parties and has recently launched a formal investigation, jointly with the Privacy and Information Commissioner of British Columbia, into Facebook and Aggregate IQ's compliance with privacy laws.² Recently, Canada's Communication Security Establishment, in its report, *Cyber Threats to Canada's Democratic Process*³, identified political parties and politicians as being uniquely vulnerable to cyberattack, given the intimate and private personal details that are collected and stored.

Application to the *Canada Elections Act*

The CBA Section has considered a number of options to address the legislative gap. One option is to amend the CEA to limit the collection, use and disclosure of personal information in the context of

¹ See Office of the Privacy Commissioner of Canada, "Appearance before the Standing Committee on Access to Information, Privacy and Ethics on Reform of the Privacy Act (Ottawa: March 2016), available [online](#), and Office of the Privacy Commissioner of Canada, "Facebook allegations underscore deficiencies in Canada's privacy laws" (Ottawa: March 26, 2018), available [online](#).

² See Office of the Privacy Commissioner of Canada, "BC, federal Privacy Commissioners initiate joint investigations into Aggregate IQ, Facebook" (Ottawa: April 5, 2018), available [online](#) and "Privacy Commissioner launches Facebook investigation" (Ottawa: March 20, 2018), available [online](#)

³ *Cyber Threats to Canada's Democratic Process* (Ottawa: Communications Security Establishment, June 2017), available [online](#).

political activities. The CEA offers only minimal privacy protections of personal information, limited to the narrow writ period. On the whole, the CEA grants broad authorization for collection and use of personal information. For example, pursuant to section 110 of the CEA, registered parties are expressly authorized to use the list of electors for soliciting contributions and memberships.⁴

The CBA Section recommends that political parties be subject to enhanced privacy principles and that these protections extend beyond the writ period. Political parties have an interest in collecting a significant amount of information on Canadian citizens, only some of which is openly understood and regulated by the CEA. What's more, given the nature of political staffing campaigns, a significant number of employees and volunteers have access to extensive personal data with no guarantee of privacy training. Canadians deserve better protection.

Elections Canada, in its report, *Preventing Deceptive Communications with Electors*, expresses similar concerns and recommends amending the CEA to:

provide a mechanism by which the application of privacy protection principles governing most Canadian institutions and organizations would be extended to political parties. The Act should also be amended to require that political parties demonstrate due diligence when giving access to their voter databases.

As Parliament considers amendments to the CEA, the CBA Section encourages considering additional amendments to Bill C-50. We also encourage further study to ensure that effective data protection mechanisms are developed that promote democracy and protect the privacy rights of Canadian electors.

We trust that our comments are helpful, and would be pleased to discuss this matter in more detail.

Yours truly,

(original letter signed by Gillian Carter for Suzanne Morin)

Suzanne Morin
Chair, CBA Privacy and Access Law Section

⁴ S.C. 2000, c. 9, s. 110.