PRIVACY AND THE ELECTORATE

Big Data and the Personalization of Politics

*Professor Elizabeth F. Judge & Professor Michael Pal**

Faculty of Common Law, University of Ottawa

Table of Contents

Key Messages 3

Executive Summary 4

Context 5

Implications 6

Results 6

State of Knowledge 7

Regulatory Environment 7

Voter Databases and Voter Management Systems 11

Self-Regulation 20

Voter Privacy Breaches 23

Legislative Lacuna and Reform 25

Approach & Methodology 26

Additional Resources 26

Further Research 27

Gaps in the Law 27

Gaps in the Scholarship 27

Gaps in Knowledge Regarding Technology 28

Knowledge Mobilization 28

Conclusion 28

References and Bibliography 30

Appendices 36

Appendix A : Privacy Policy of the Conservative Party of Canada 36

Appendix B : Privacy Policy of the Green Party of Canada 38

Appendix C : Privacy Policy of the Liberal Party of Canada 43

Appendix D : Privacy Policy of the New Democratic Party of Canada 46

Appendix E : Leak from the Jeb Bush Presidential campaign 49

Appendix F : Recommendations by the Information and Privacy Commissioner for BC 50

Appendix G : Fair Information Principles 51

Appendix H : Liberalist iPhone/iPad app 53

Appendix I : Donald Trump Privacy Policy 54

Appendix J : Hillary Clinton Privacy Policy 57

Appendix K : Table of Relevant Legislation 62

Appendix L : List of Known Data Intermediaries 67

Appendix M : Images from CIMS database 72

Key Messages

- Political parties collect, store and analyze significant amounts of data about individual Canadians, which includes sensitive and personal information. Data can be collected from a variety of sources, including in-person and on-line voter contact, social media, mobile applications or "apps," as well as the Registry of Electors. Such data is then stored in voter management systems.

- Federal privacy legislation applicable to the private and public sectors does not currently cover the activities of political parties. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*),[1] applicable to the private sector, does not appear to cover political activities because they are likely excluded from the definition of "commercial activities" in the legislation. Political parties are excluded from the definition of "government institutions" in the *Privacy Act*,[2] the public-sector privacy legislation. The *Canada Elections Act* (*CEA*)[3] does not significantly oversee the practices of political parties with regard to the collection, use, storage, and analysis of data about voters and donors. Numerous private sector entities are involved by collecting, analyzing, and selling voter data to political parties. It is unclear how the legislative framework applies to them or what privacy rules they apply to their own activities.

- Political parties engage in voluntary, self-regulation of their practices around the collection, use, storage, and analysis of data and their use of new technologies. They have crafted their own privacy policies. These policies, however, are voluntary and lack any independent oversight or enforcement mechanism. It is unclear how they are interpreted and applied. There are significant risks to privacy attendant in the self-regulation model. These risks have been highlighted by multiple recorded breaches of reasonable expectations of privacy by political parties.

- New technologies are constantly emerging, which shift political activities and have consequences for the protection of privacy. New technologies may exacerbate the possibility and severity of voter data leaks.

- There are significant knowledge gaps around the use of new technologies and big data analytics by political parties, the functioning of the existing legal framework with regard to parties and the private data companies they cooperate with in procuring and analyzing

*Elizabeth Judge is Full Professor and a member of the Centre for Law, Technology and Society at the Faculty of Law at the University of Ottawa. Michael Pal is an Assistant Professor and Director of the Public Law Group at the Faculty of Law at the University of Ottawa. The authors would like to thank the Social Sciences and Humanities Research Council for funding this research through a Knowledge Synthesis Grant, the team administering the Grant for their kind and professional assistance, and to Amìr Korhani for outstanding research assistance.

[1] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (*PIPEDA*).

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

[3] *Canada Elections Act*, S.C. 2000, c. 9 (*CEA*).

data, international best practices, and the options for legal and institutional reforms to ensure compliance with generally accepted privacy principles.

Executive Summary

Big data and new technologies have changed politics, with serious implications for the protection of personal privacy. Political parties now hold large amounts of sensitive, personally identifiable information about the individuals from whom they seek political contributions and, at election time, votes. Pursuant to the *Canada Elections Act*, parties are privy to basic information about voters from the Registry of Electors. This basic information is augmented by the fact that candidates, nomination contestants, leadership contestants, Members of Parliament, political staffers, and volunteers now collect and record personal information that is stored in political party databases. This data is key to the activities of political parties. It is used for a variety of purposes, including voter contact and turnout, fundraising, honing of political messaging, and micro-targeted communications designed specifically to appeal to small sub-sets of voters. It is well-recognized in the media and academic debates that data, and the techniques of big data analysis, are central to the operation of parties and the conduct of politics in 2016.

The legal implications for the protection of personal privacy and fair information principles are less well known. Federal political parties are not subject to the national privacy legislation that applies to the public and private sectors. Neither the *Privacy Act*, which protects personal information that the federal government and public bodies hold, nor the *Personal Information Protection and Electronic Documents Act* (hereinafter *PIPEDA*), which applies to the private sector, cover the activities of political parties. Not labeled as "government institutions" under the *Privacy Act*, and not engaging in "commercial activities" as defined under *PIPEDA*, political parties fall outside of the ambit of either piece of legislation. The *Canada Elections Act* provides political parties with a right to obtain basic information about the electorate, but does not regulate the political parties' collection and use of personal information about voters.

Cognizant of regulatory silence on their data collection practices, political parties have crafted their own privacy policies. These policies, however, are voluntary and lack any independent oversight or enforcement mechanism. It is unclear to what extent the political parties' voter management systems, including the Conservative Party of Canada's "Constituent Information Management System" (CIMS), the Liberal Party of Canada's "Liberalist," and the New Democratic Party's "Populis," are subject to internal rules around privacy protection. Several incidents over the last few years involving the misuse or disclosure of sensitive personal information by political actors have highlighted the risks of continued voluntary self-regulation by parties. Voter management systems have evolved rapidly over the course of several elections. Initially conceived as voter databases, they are now integrated with data analysis software which then culminates in sophisticated micro-targeting techniques aimed at attracting more voters. These practices are rapidly evolving, based on the introduction of new technologies and importation of political practices from other jurisdictions, such as the United States.

This Knowledge Synthesis Report summarizes the current state of knowledge around the collection, storage, and use of personal information by political parties and the legal framework around voter privacy. This Report then identifies several knowledge gaps, including in the law, in the use of technology and data by political parties, and in the scholarship around these questions. The presence of these knowledge gaps is significant because of the now routinized use of personal information about voters by political parties, the risks of misuse, and the serious consequences for individual Canadians.