

The Best Data Wins: Assessing Policies that Regulate the Collection, Use, and Disclosure of Voter Data by Canadian Federal Parties

**by
Christina Coleman**

B.A. (English and Psychology), Mount Royal University, 2015

Project Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Public Policy

in the
School of Public Policy
Faculty of Arts and Social Sciences

© Christina Coleman 2022
SIMON FRASER UNIVERSITY
Spring 2022

Copyright in this work is held by the author. Please ensure that any reproduction or re-use is done in accordance with the relevant national copyright legislation.

Declaration of Committee

Name: Christina Coleman

Degree: Master of Public Policy

Title: **The Best Data Wins: Assessing Policies that Regulate the Collection, Use, and Disclosure of Voter Data by Canadian Federal Parties**

Committee:

Chair: Genevieve LeBaron
Professor, Public Policy

Sophie Borwein
Supervisor
Assistant Professor, Public Policy

Genevieve LeBaron
Examiner
Professor, Public Policy

Ethics Statement

The author, whose name appears on the title page of this work, has obtained, for the research described in this work, either:

- a. human research ethics approval from the Simon Fraser University Office of Research Ethics

or

- b. advance approval of the animal care protocol from the University Animal Care Committee of Simon Fraser University

or has conducted the research

- c. as a co-investigator, collaborator, or research assistant in a research project approved in advance.

A copy of the approval letter has been filed with the Theses Office of the University Library at the time of submission of this thesis or project.

The original application for approval and letter of approval are filed with the relevant offices. Inquiries may be directed to those authorities.

Simon Fraser University Library
Burnaby, British Columbia, Canada

Update Spring 2016

Abstract

Advances in data analytics and data-driven tools have significantly changed how federal parties campaign to win highly competitive election races in Canada. Despite these advances, federal parties are not currently regulated by data protection legislation, enabling the near unfettered collection, use, and disclosure of voter information. Consequently, there is growing concern among researchers and advocacy groups that data-driven campaign tactics infringe on individual privacy rights and undermine the democratic integrity of elections. This research examines these concerns through a literature review, expert interviews, and a jurisdictional scan. Contributing to original research, this research evaluates four policy options for regulating how federal parties campaign with voter data and data-driven tools. Currently, all major federal parties exhibit little political will to regulate themselves through data protection legislation; this research concludes by commenting on the political feasibility and potential for implementing data protection regulation.

Keywords: data-driven campaigning; big-data elections; democratic engagement; voter privacy; voter manipulation; Canadian federal parties

Dedication

This work is dedicated to those pursuing to uphold the most fundamental tenants of democracy despite its limitations. Never stop seeking respectful and stimulating dialogue, provoking new understandings of the world. Never stop leading with questions. Never stop calling others into conversation. Never stop pushing towards a version of democracy that better resembles a version we can be proud of.

In pursuit myself, this work is also dedicated to my Opa—who passed away in the middle of my graduate research. Your passion for democratic debate and open dialogue was infectious. Thanks for modelling your curiosity and showing me how to intellectually tinker. Thanks for supporting all the strong women in our family—women who navigate the world with integrity and say bold things even when there are costs.

Acknowledgements

This research would not have been possible without the support of a number of people who I would like to recognize and thank.

First, a big thanks to my supervisor, Sophie Borwein. Thanks for pushing me along when I was stuck. Thanks for chatting things through and challenging me to think about considerations that were not immediately clear to me.

Thanks to the School of Public Policy and to both former director Nancy Olewiler and current director Genevieve LeBaron. Nancy, thanks for admitting me to the program and giving me a chance to show others what I was capable of. Genevieve, thanks for your commitment to the program as an egoless learner—with really thought provoking questions as an examiner.

Thanks to my classmates—I did some of my best learning in late night ZOOM sessions with beverages and laughs.

This research would definitely not have been possible without its participants who opted-in and advanced meaningful contributions. Thanks for shaping my understanding of the policy area and the product of this research.

Finally, I would like to thank my family. Thanks for understanding when I was scattered and for always making sure I was fed. A special thanks to my Aunt Peggy who inspired me to apply for the Master of Public Policy program at SFU. You are one of the smartest people I have ever known. Thanks for your continued guidance as a role model. I am proud to continue our pursuit of knowledge together. And, a particularly thanks to my mom who directly supported me along this journey—thanks for letting me move back home to be a student again at 30 years old. Thanks for forcing me to stand in front of the mirror like a bear and scream “I deserve to be here” when I was feeling discouraged or overwhelmed.

Table of Contents

Declaration of Committee	ii
Ethics Statement	iii
Abstract	iv
Dedication	v
Acknowledgements	vi
Table of Contents	vii
List of Tables	x
List of Acronyms	xi
Glossary	xii
Executive Summary	xv
Chapter 1. Introduction	1
Chapter 2. Data-Driven Campaigning	3
2.1. Defining Data-Driven Campaigning	3
2.2. Data-Driven Campaigning in Canada	4
2.2.1. Collection of Voter Data	5
2.2.2. Use and Disclosure of Voter Data	7
2.3. Balancing Democratic Engagement with Privacy Infringements and Voter Manipulation	10
Chapter 3. The Current Patchwork of Data Protection Regulations for Federal Parties 14	
3.1. Canada Elections Act	14
3.2. Anti-Spam Legislation	15
3.3. Privacy Legislation Regime	16
3.4. Self-Regulation	17
Chapter 4. Methods	19
Chapter 5. Jurisdictional Scan: Data-Driven Campaign Operations in the Anglosphere	20
5.1. Australia	20
5.1.1. Data-Driven Campaigning in Australia	20
5.1.2. Regulatory Environment for Parties in Australia	21
5.2. United Kingdom	22
5.2.1. Data-Driven Campaigning in the UK	22
5.2.2. Regulatory Environment for Parties in the UK	23
5.3. United States	25
5.3.1. Data-Driven Campaigning in the US	25
5.3.2. Regulatory Environment for Parties in the US	27
Chapter 6. Interview Findings	29
6.1. Data-Driven Campaign Practices Lack Transparency	29

6.2.	No Political Will to Include in Federal Parties in Data Protection Legislation	30
6.3.	Participants Differed on How to Approach Data Protection Regulation	31
6.4.	Data Operations are Relatively Small and Less Sophisticated as Compared to the US	32
Chapter 7. Policy Options		34
7.1.	Overhaul PIPEDA and Extend to Federal Parties	34
7.2.	Amend CEA: Apply GDPR Data Protection Principles to Federal Parties	36
7.3.	Amend CEA: Regulate Platform Accountability and Provide Voluntary Code of Practice	36
7.4.	New Legislation: Establish Singular Elections Canada Voter Database	37
Chapter 8. Evaluation Criteria & Measures		39
8.1.	Effectiveness	39
8.2.	Compliance Issues	41
8.3.	Administrative Complexity	41
Chapter 9. Evaluation of Policy Options		44
9.1.	Analysis 1: Overhaul and Regulate Parties – PIPEDA	45
9.1.1.	Effectiveness	45
9.1.2.	Compliance Issues	45
9.1.3.	Administrative Complexity	46
9.2.	Analysis 2: Regulate Data Practices of Parties – CEA	46
9.2.1.	Effectiveness	46
9.2.2.	Compliance Issues	47
9.2.3.	Administrative Complexity	48
9.3.	Analysis 3: Platform Accountability and Voluntary Code of Practice – CEA	48
9.3.1.	Effectiveness	48
9.3.2.	Compliance Issues	49
9.3.3.	Administrative Complexity	49
9.4.	Analysis 4: Elections Canada Database – New Law	49
9.4.1.	Effectiveness	49
9.4.2.	Compliance Issues	50
9.4.3.	Administrative Complexity	51
Chapter 10. Recommendation		52
Chapter 11. Limitations		54
Chapter 12. Moving Forward: Political Feasibility		55
References		57
Appendix A. Interview Participants		64
Appendix B. Sample Interview Questions		65

Appendix C. Sample of Data Collected by Political Parties	66
Appendix D. Example of VRM Database Scale that Measures Levels of Voter Support	67

List of Tables

Table 2.1.	Selected Regulatory Standards for Artificial Intelligence (European Commission, 2020)	8
Table 7.1.	GDPR Data Protection Principles	35
Table 8.1.	Guidelines for Voter Privacy Reform (Judge & Pal, 2021)	40
Table 8.2.	Criteria and Measures	43
Table 9.1.	Summary of Policy Analysis	44

List of Acronyms

ALRC	Australian Law Review Commission
BC	British Columbia
BC PIPA	British Columbia's Personal Information and Protection Act
BOIE	Board of Internal Economy
CASL	Canada Anti-Spam Legislation
CCE	Commissioner of Canada Elections
CEA	Canada Elections Act
CEO	Chief Elections Officer
CIMS	Constituent Information Management System
CRTC	Canadian Radio-television and Telecommunications Commission
DPA	Data Protection Act
GDPR	General Data Protection Regulation
HAVA	Help America Vote Act
MPs	Members of Parliament
NDP	New Democratic Party
OIPC	Office of the Information and Privacy Commissioner for BC
OPC	Office of the Privacy Commissioner of Canada
PECR	Privacy and Electronic Communications Regulations
PIPEDA	Personal Information Protection and Electronics Documents Act
UK	United Kingdom
UK GDPR	UK General Data Protection Regulation
US	US
USD	US Dollars
VRM	Voter Relationship Management

Glossary

Algorithm	A series of instructions that tell a program how to interpret big-data sets.
Algorithmic Disgorgement	An enforcement tool that requires a private organization to destroy harmful or deceptive algorithmic systems (including artificial intelligence and machine-learning).
Algorithmic Transparency	An openness about the underlying purpose, design, and actions of algorithms used to make decisions or predictions about people.
Anglosphere	A group of English-speaking countries with ancestral, cultural, and historical ties to the United Kingdom.
Big-Data Analytics	The practice of examining large, diverse amounts of data to uncover insights so federal parties can make data-driven decisions about where and how to invest resources.
Canvassing Applications	An IOS or Android application often linked to VRM databases, used by party affiliates while canvassing to collect and use voter data.
Campaign Cycle	The cycle that federal parties campaign over, from pre-election period (assuming fixed election dates, starting on June 30 in the year of a general election and ending when the writs are drawn-up) to election period (starting when the writs are drawn-up and ending on election day) to in-between election periods.
Certification Mechanism	A government framework requiring algorithms used by federal parties to be registered and approved against defined assurances that systems used to make automated decisions are in compliance with applicable standards.
Commissioner of Canada Elections (CCE)	The person responsible for ensuring that federal parties comply with the <i>Canada Elections Act</i> , and for taking enforcement measures as required.
Chief Elections Officer (CEO)	The person that heads Elections Canada and is responsible for administering the <i>Canada Elections Act</i> , reporting directly to Parliament.
Data Broker	A company that aggregates voter data from a variety of public and non-public sources and then resells that data to other companies.
Data Analytics Companies	Companies like Cambridge Analytica and AiQ that are contracted by federal parties to run big data analytics on voter data for predictive modelling.

Data-Driven Tools	A wide variety of analytic tools like applications, algorithms, and databases used to make sense of voter data to support federal party campaigns (e.g. Nationbuilder).
Digital Campaigning	Federal party campaigning that uses technology (e.g. email newsletters or social media platforms).
Echo Chambers	Environments where voters only encounter opinions or beliefs that validate and reinforce existing beliefs.
Filter Bubbles	As a result of algorithms that personalize voters' digital experience, voters only encounter opinions or beliefs that validate and reinforce existing beliefs.
Get-out-the-Vote	A campaign strategy aimed at increasing voter turnout.
Issue Information	Information on voters' opinions on political issues (e.g. childcare or housing), sought by federal parties through surveys or canvassing.
Microtargeting	A political marketing strategy that uses voter data and demographics to target small segments with personalized messages through the voter's preferred communication channel (e.g. Facebook).
Online Platforms or Social Media Platforms	Digital social-networking or micro-blogging sites where online communities gather to exchange ideas or content and federal parties attempt to engage voters through advertising or other methods (e.g. Facebook or TikTok).
Permanent Campaign	The idea that federal parties, who are able to constantly surveil voters in real time, are perpetually campaigning regardless of any defined election period.
Per-Vote Subsidy	Government payments to federal parties with a payment amount directly link to the amount of votes they received in the most recent election.
Platform Accountability	When platforms expand their role to manage and moderate the design of their sites in an effort to provide better transparency.
Political Consultants	People who advise or assist federal party campaigns, often as a kind of advertising expert who sells the idea of a person as a candidate.
Political Marketing	A variation of marketing where federal parties sell their candidates or platforms as a product to promote themselves to voters and win an election.
Privacy Commissioner	The person that heads the Office of the Privacy Commissioner and is responsible for administering the <i>Privacy Act</i> and the <i>Personal Information Protection and</i>

Electronics Document Act, reporting directly to Parliament.

Psychographic Profiling	A practice that divides voters into pre-determined segments using personality, values, lifestyles, and attitudes then markets to them based on their predicted preferences.
Swing Riding	An electoral riding with a close race that can be won or lost within 3-4% of the vote.
Voter Autonomy	The idea that voters can make choices about who to vote for, free from manipulation.
VRM databases	National databases that store collected voter data points, housing comprehensive profiles of voters.
Vote Efficiency	The party practice of allocating resources to capture votes in swing ridings rather than allocating resources in ridings the party can definitely win or definitely lose.
Voter Profiles or Voter IDs	Profiles held by federal parties on voters whether they support the party or not, containing a comprehensive list of data points collected from various sources.
Voter Manipulation	More than persuasion, the idea that voters are coerced into voting for a particular party as a result of structural nudging (altering the choices available to a decision-maker) and informational nudging (changing the information voters see).

Executive Summary

Technological advancements in big-data analytics and data-driven tools have significantly changed how federal parties collect, use, and disclose voter data to win elections. Other than an obligation to create a privacy policy, submit the policy to Elections Canada, and post the policy on their party websites, federal parties are unregulated by any data protection legislation. All the major federal parties (the Liberals, Conservatives, and the New Democrats) engage in data-driven campaign practices, but without regulatory oversight, the scale and sophistication of these operations are not entirely known. Incidences such as the Facebook-Cambridge Analytica¹ scandal show how data collection for psychographic profiling can be used to infringe on voter privacy and in attempts to change the outcome of an election or referendum. This has led concerned researchers and data protection advocates to argue for better regulatory safeguards, providing oversight to protect voter privacy and the democratic integrity of elections.

This paper contributes to original research by examining and evaluating four policy options that consider further data protection safeguards. The qualitative methods used in this study include a literature review, a jurisdictional scan, and 10 interviews with academic researchers (n=5), Conservative campaign officials (n=3), a lawyer, and a data protection advocate.

The jurisdictional scan revealed data-driven campaign practices are widespread, with countries outside Europe lagging to regulate political parties under data protection legislation. Three countries were identified as good comparators to Canada because they shared similar political-system features: Australia, the United Kingdom (UK), and the United States (US). The UK presented the best model for data protection regulation with political parties regulated under the UK General Data Protection Legislation. The US presented the least regulation and greatest scale of data-driven campaigning operations, with parties in Canada, the UK, and Australia buying data-driven tools designed and tested in the US context. Australia has federal party privacy exemptions

¹ First reported in 2015, Cambridge Analytica collected data belonging to millions of Facebook users without their consent to create psychographic profiling categories that were later used to try to persuade voters in Donald Trump's 2016 presidential campaign and other campaigns/referendums.

similar to Canada with fewer political financing regulations; a review is currently underway in Australia to modernize the *Australia Privacy Act* and potentially remove the political party exemption, which currently enables Australian political parties to collect, use, and disclose voter data with no restrictions.

Interview participants highlighted several key themes. First, the absence of regulatory oversight has resulted in little transparency about the actual data-driven campaign practices used by federal parties in Canada. Second, participants questioned how much political will there is for federal parties to cover themselves with data protection regulations in the future. Third, participant responses varied significantly on how best to approach regulation in Canada moving forward—in some cases participants advocating for no regulation. Fourth, all Conservative campaign officials stressed the size of data-driven operations were relatively small compared to operations in the US, where data use and political financing is widespread.

This research proposes four policy options identified in the literature and in interviews. Option 1 proposes to overhaul the *Personal Information Protection and Electronics Documents Act* (PIPEDA)—applying the GDPR data protection principles—and to remove the current regulatory exemption for federal parties; however, this option also proposes to use a code of practice to provide federal parties with more flexibility than private organizations to democratically engage voters. Option 2 proposes to regulate federal parties with the same GDPR principles as Option 1 but under the *Canada Elections Act* instead of PIPEDA. Option 3 proposes to regulate better platform accountability and offers a voluntary code of practice between federal parties and Elections Canada. Option 4 proposes to establish a singular Elections Canada Voter Relationship Management (VRM) database that all parties are required to use instead of allowing parties to collect, use, and disclose granular data independently. These options were assessed against three societal and governmental objectives: effectiveness in data protection and democratic engagement, compliance issues, and administrative complexity. Ultimately, option 1 is recommended as the best approach for safeguarding voter privacy and the democratic integrity of elections; multiple interview participants suggested PIPEDA as the appropriate policy instrument to cover federal parties with data protection regulation, and it is already undergoing review. Since there are some concerns about federal parties having the political will required to remove their

exemption from PIPEDA, this research concludes with a consideration of political feasibility moving forward.

Chapter 1.

Introduction

Underpinned by the data revolution, modern campaigning is increasingly intermediated by online platforms, presenting new opportunities for election campaign strategists, and new challenges for voter privacy and the democratic integrity of elections. Recognizing the potential benefits, federal parties use data-driven tools (e.g. applications and algorithms) in an attempt to optimize the collection, use, and disclosure of voter data, taking advantage of the same big-data analytics techniques as data-driven marketing (Richardson, Witzleb, & Paterson, 2019). The Facebook-Cambridge Analytica scandal² exposed a darker side of data-driven campaign practices, spotlighting how psychographic profiling could potentially be used as an attempt to change the outcome of an election or referendum. Other than a privacy policy clause in the *Elections Modernization Act*, Canadian federal parties currently remain directly unregulated by any data protection legislation, enabling the near unfettered collection, use, and disclosure of voter data.³ Currently, federal parties receive a carve-out from privacy legislation on the basis that voter data serves an important democratic function by helping parties reach and engage voters. However, absent regulatory oversight and transparency, little is known about the intricacies and sophistication of data-driven campaigning in Canada. Some researchers and data protection advocates argue there should be regulatory safeguards in Canada to better protect voters⁴ from data-driven tactics that may infringe on privacy or the democratic integrity of elections (C. Bennett, personal communication, March 1, 2022; B. Hearn, personal communication, March 15; Participant D, personal communication, March 17, 2022). More regulation could also level the playing field and

² First reported in 2015, Cambridge Analytica collected data belonging to millions of Facebook users without their consent to create psychographic profiling categories that were later used to try to persuade voters in Donald Trump's 2016 presidential campaign and other campaigns/referendums.

³ Although not directly regulated, the data practices of federal parties are indirectly constrained by political financing regulations and the Personal Information Protection Electronics Document Act (K. Boessenkool, personal communication, Feb 11, 2022; Participant B, personal communication, February 15, 2022).

⁴ In this paper, "voters" means individuals (registered to vote or not) whose personal information is collected and used by federal political parties (Judge & Pal, 2021).

provide a clear set of rules for federal parties who compete in high stakes elections races where, arguably, the best data wins.

This paper contributes to original research by examining and evaluating policy options that consider further safeguards for the regulation of Canadian voter data to protect privacy and the democratic integrity of elections. The findings of this analysis are intended to provide further insights on the future of policy adoption for researchers and policymakers. This research is primarily interested in how federal parties collect, use, and disclose voter data in ways that may threaten privacy and democratic integrity; for this reason, although data privacy concerns also often touch on data storage, storage considerations will be considered out of scope. This research proceeds as follows: Chapter 2 explores the literature on data-driven campaigning in Canada, including trade-offs among democratic engagement, voter privacy and voter manipulation; Chapter 3 reviews the current patchwork of data protection regulations; Chapter 4 discusses the methodology used in this analysis; Chapter 5 offers a jurisdictional scan, comparing the data-driven campaign practices and regulations in Australia, the United Kingdom (UK), and the United States (US); Chapter 6 provides a summary of key findings from interview participants; Chapter 7 summarizes proposed policy options; Chapter 8 describes the policy measures and criteria that will be used to analyze the proposed policy options; Chapter 9 evaluates policy options against the outlined criteria and measures; Chapter 10 provides recommendations; Chapter 11 identifies the limitations of this research; and Chapter 12 concludes with a discussion on the political feasibility for regulation moving forward.

Chapter 2.

Data-Driven Campaigning

2.1. Defining Data-Driven Campaigning

Data-driven campaigning is broadly defined as an election campaigning approach that uses big-data analytics to leverage the vast potential of social media and mobile applications as a way of reaching and engaging voters—which could be practices like digital campaigning practices to maintaining massive Voter Relationship Management databases (Bennett & Lyon, 2019). Essentially a method of surveillance, data-driven tools allow voters to be monitored and targeted continuously and granularly using techniques intricately linked with and taken from the commercial sector (Hankey, Morrison, & Naik, 2018). Voter data has historically been collected, used, and disclosed by federal parties in Canada as the backbone of campaigning operations; however, over the last two decades, tectonic shifts in technology, digitalization, and communications have altered political communication and expanded how voter data can be collected and used by political campaigns (Cohen, 2021). Current data strategist for the Liberals, Tom Pitfield, views data-driven campaigning as:

No different than what [parties] would have been doing in the 19th century...you identify where you can win seats, and you put the effort in there...what's changing because of the power of social media targeted advertising, in particular, is that the parties are able to target their advertising and organizational push in small geographic areas...And that's much more precise than what electoral tacticians would have been able to do in the 19th century (Heath-Rawlings, 2021).

New technological tools for data collection methods like polling have made it easier for federal parties to gauge the desires of voters and gain market intelligence (Turcotte, 2020); further, the rise of data-driven campaigning has been coupled with shifts in political marketing.⁵ Despite parties publicly positioning themselves along the political spectrum to reflect their ideologies in tandem, to meet the demands of the market and adopt a political marketing strategy, federal parties sometimes compromise their

⁵ Theories on political marketing suggest federal parties use commercial marketing principles to sell their product—or a collection of policies—to the demands of its market—or the desires of voters (Reid, 1988; Lees-Marshment, 2011).

ideologies and adapt products outside their core values to win votes (Y. Dufresne, personal communication, February 23, 2022). The increasing sophistication of data-driven campaigning in Western industrialized democracies underpins growing concerns over voter privacy and the democratic integrity of elections.

2.2. Data-Driven Campaigning in Canada

Data-driven campaigning practices and commercial data brokers⁶ have been used to win federal elections in Canada since the 2000s. Considering the high stakes of elections, federal parties use data-driven campaign practices to gain a perceived advantage over competitors. To evaluate the effectiveness of data-driven tools, K. Boessenkool suggests it is useful to consider which parties win swing ridings (i.e. ridings won within 3 the 4 percentage points of the vote) (personal communication, February 11, 2022). In both 2019 and 2020, the Liberals lost the popular vote but were still able to win the election because they won more swing ridings. The concept of “vote efficiency” is used to describe a campaign approach where parties choose to spend resources in close ridings rather than in less competitive ones to capture votes. On September 21, 2021 (election night), after the Liberals claimed another win, a Liberal election strategist at the time, Gerald Butts tweeted, “Vote efficiency isn’t accidental. All three Trudeau Liberal campaigns were among the most efficient in history. The unsung team of super geniuses put together and led by @tompitfield at Data Sciences deserves a lot more credit than they’ve ever received” (Butts, 2021). Data-driven tools have changed the ways federal parties collect, use, and disclose voter data because they provide insights into which ridings offer the best efficiency, as well as, which issues matter the most to constituents. Beyond identifying the level of support in ridings, federal parties collect, use, and disclose voter data to fundraise for donations and gain comprehensive issue information—data obtained through surveys, canvassing, and inference that explains which political issues matter most to individual voters.

⁶ Commercial data brokers who apply “their experience collecting, analyzing, cross-referencing and segmenting vast amounts of consumer information into various classifications to support political campaigns have been around since as early as 2006” (Bennett & Bayley, 2018).

2.2.1. Collection of Voter Data

In British Columbia (BC), provincial and municipal parties are regulated by the *Personal Information Protection Act* (BC PIPA), which allows the Office of the Information and Privacy Commissioner (OIPC) to investigate their collection, use, and disclosure practices.⁷ A 2019 investigation report showed that provincial parties in BC collect a significant amount of voter data, including: email address, income, LinkedIn ID, issues of interest, credit card signatures, how the voter cast their ballot in the last election (either in advanced polls or on election day), party membership, and if the voter is a prospective member—see Appendix C (Table C.1.) for a comprehensive list (McEvoy, 2019). Parties also collect data that is classified as sensitive by Europe’s General Data Protection Regulation (GDPR) such as voter ethnicity, age, gender, and religion. Because federal parties are covered by fewer data protection laws than provincial parties in BC, it is likely they are collecting the same types of voter data; however, no definitive reporting has uncovered exactly what federal parties collect.

Data can be collected a number of ways. First, data can be collected from a variety of sources for free, including from: the voter list, the census, polling company reports, cookie web-scraping, donor information, and surveys sent to voters directly by a federal party. Most of this data is publicly available or offered directly by voters. However, sometimes free data is inferred by canvassers who record observations about voters. For example, a door-to-door volunteer might make inferences about voters depending on the car in their driveway or if kids are in their house (Participant B, personal communication, February 15, 2022). Second, parties may also collect data by purchasing it from data brokers but the scale of this kind of secondary data market is unknown. Some interview participants suggested that purchasing data in Canada is not always worthwhile because companies that sell data are required to make it de-identifiable, pursuant to the *Personal Information Protection and Electronic Documents Act*, which effectively regulates parties indirectly (Participant B, personal communication, February 15, 2022; Participant C, personal communication, February 23, 2022). Third, federal parties can collect data via agreements with social media websites such as

⁷ As of April 2022, Quebec is the only other province in Canada to regulate political parties under a provincial privacy legislation as a result of an amendment that ascended September 22, 2021.

Facebook and Twitter. All parties collect data continuously and regardless of whether or not they are in an election period.

Data-driven tools like Voter Relationship Management (VRM) databases and canvassing applications have optimized data collection. VRM databases contain “hundreds if not thousands of fields...combined into a giant assemblage made possible by fast computers, speedy network connections, cheap data storage, and ample financial and technical resources” (Rubinstein, 2014, p. 879). In Canada, VRM databases use the National Register of Electors (or the voter list)—supplied to federal parties by Elections Canada—as a foundation, and then they layer additional data points to create comprehensive voter profiles. In 2004, the Conservatives developed the first Canadian centralized voter data management system, the Constituent Information Management System (CIMS)—modelled after the American Republican Party’s Voter Vault software. To later prepare for the 2019 campaign, the Conservatives launched Medallion—a platform supported by Nationbuilder—to interact with CIMS, enhancing mapping and maximizing canvassing efficiency (Bennett & McDonald, 2020). In 2011, the New Democratic Party (NDP) launched Populist—an improvement of their previous system called NDP Vote. A year later, in 2012, the Liberals launched Liberalist, a modified version of the NPG VAN’s Votebuilder software, a competitor of Nationbuilder (Bennett & Bayley, 2018). Each party also has canvassing applications for mobile devices, integrated with their VRM databases: the Conservatives use CIMS to Go, the NDP use Dandelion, and the Liberals use MiniVAN. These canvassing applications direct volunteers to the houses of supporters or potential supporters (in some cases, skipping over houses of non-supporters), and allow volunteers to collect data at a voter’s door, and track door-knocking statistics in real time.

When VRM databases were initially launched in Canada, they were the backbone of data-driven campaigns; however recent trends in data collection have somewhat shifted the landscape. In 2012, federal parties shifted away from manually collecting voter data and solely relying on in-house VRM databases to partnering with social media companies to track voters online. Data-driven tools like Nationbuilder help federal parties match social media profiles (like Facebook IDs) to voter profiles in VRM databases (Rubinstein, 2014). For example, each time a voter engages with content from a party or an associated organization on Facebook, Nationbuilder scores the voter with a credit or point and provides the party with their Facebook ID—which the party can

then scrape data from to add to their voter profiles (Participant B, personal communication, February 15, 2022). Importantly, partnering with social media companies like Facebook to collect data is a lot more cost effective for parties than manually collecting data. Conservative strategist K. Boessenkool said that, “when I took over the Facebook side of our voter ID in the middle of 2015 campaign, AI generated from Facebook about 65,000 Voter IDs at a cost of about between \$0.75 to \$1.25 per ID. And at that point, CIMS was costing us between \$7.50 and \$12.50. So literally 10 times more for the same amount of ID” (personal communication, February 11, 2022).

2.2.2. Use and Disclosure of Voter Data

Once data is collected, all federal parties categorize voters with scoring systems into levels of support such as supporters, non-supporters, and undecided voters. Voters can then be targeted with demographic-specific messaging, see Appendix D (Figure D.1.) for an example of the scale used by CIMS (Bennett & Bayley, 2018). Although these scores are used to drive “get-out-the-vote” strategies, less is known about how parties determine issue preferences and generate personalized messages and advertisements through microtargeting (Bennett & Gordon, 2021). Data analytics companies such as Cambridge Analytica have worked on US campaigns to categorize voters into one of six predetermined psychographic profiles that, in their view, efficiently target voters with personalized ads and scripted messages, particularly in swing ridings (Concordia, 2016). A study by Matz et al. (2017) showed how targeting commercial marketing advertisements for a product to viewers based on psychological traits (for example, high extroversion or low extroversion) resulted in a 40% increase in engagement and a 50% increase in product purchase. It is unclear if federal parties are using psychographic profiling techniques but Liberalist was modelled from the same analytics tools used in Barack Obama’s 2008 and 2012 campaigns, which predicted individual voter behaviours from analytics tables with unprecedented accuracy (Deley & Szwarc, 2018).

Algorithmic learning and profiling—computer programs that absorb new information to make choices about voters to categorize them by support or sometimes predict political issue preferences—is also used by political parties (Matwankar & Shinde, 2016; Participant D, personal communication, March 17, 2022). This raises concerns because algorithms do not always make ethical or accurate choices,

sometimes biasing voters depending on known or assumed demographic data (Babic et al., 2021). Similar to the sophistication of microtargeting practices, in the absence of regulatory oversight, the sophistication of federal party algorithms in Canada is also unknown. In 2020, the European Commission began to identify a regulatory framework to ensure the use of algorithmic applications are designed and used ethically and responsibly—which could be adapted to hold federal parties accountable to similar standards, see Table 2.1 (European Commission, 2020). The European Commission also recommended the introduction of a certification mechanism—requiring the owner of an algorithm to register it to receive a certification—as a way of promoting algorithmic transparency. Certification mechanisms can ensure systems used to make automated decisions are designed, built, and tested to comply with set standards (Gryz & Rojszczak, 2021). In 2019, the Danish government introduced a framework to ensure digital responsibility that includes a criteria for companies to train fair and non-biased algorithms (Dataethics, 2019). When algorithms are non-compliant, they could be subject to significant regulatory enforcement. In March 2021, the US Federal Trade Commission introduced an algorithmic disgorgement penalty where algorithmic systems in the private sector (e.g. artificial intelligence or machine-learning) found to be deceptive are required to be destroyed (Kaye, 2022). A disgorgement penalty is a good example of the types of enforcement mechanisms that could be used to ensure all algorithms used by federal parties adhere to standards in the future.

Table 2.1. Selected Regulatory Standards for Artificial Intelligence (European Commission, 2020)

#	Types of Standards	Description
1	Training Data	Requirements to ensure the data sets that algorithms are trained on are sufficiently broad; requirements to ensure the data sets are sufficiently representative of gender, ethnicity, and other possible identifiers that could be grounds of discrimination; requirements to ensure the privacy of personal data is protected while algorithms are in use.
2	Data and Record Keeping	Requirements to ensure accurate and detailed records on the data sets used to train algorithms are kept; requirements to ensure documentation on the training and programming methodologies are kept; requirements to ensure documentation on the processes and techniques used to validate, train, and build algorithms are kept.

3	Information to be Provided	Requirements to ensure clear information on the limitations and capabilities of algorithms are kept, in particular information on an algorithm's expected level of accuracy. Requirements to ensure citizens are informed they interact with algorithms, where it is not immediately clear.
4	Robustness and Accuracy	Requirements to ensure algorithms are robust, accurate, and that outcomes are reproducible. Requirements to ensure algorithms can address errors or inconsistencies.
5	Human Oversight	Requirements to ensure all algorithms are previously reviewed and validated by a human (or if the algorithm becomes immediately effective, that human oversight is ensured afterwards); requirements to ensure humans can monitor the algorithm while in operation and intervene to deactivate in real time.

Since social media platforms are required to maintain advertisement registries that archive all political ads in Canada, not all social media platforms offer advertising to political parties.⁸ Federal parties have adapted by primarily using Facebook to target voter segments, in large part because of its accessibility and affordability⁹ (Bennett & Gordon, 2021). Facebook offers targeting with three methods. First, federal parties can target lists of users generated from a number of criteria such as postal code, age, or other interests and passions. Second, parties can target custom lists of users that support a party, given to Facebook by parties or candidates. Third, parties can target “lookalike audiences” or a computer generated lists of users who have similar interests and demographics as candidate supporters. Leading up to both the 2019 and 2021 federal elections, the Liberals targeted voters with significantly more advertisements than other parties. Over the three months before election day in 2021, the Liberals had 14,800 iterations of Facebook ads compared to the Conservatives with 1,400 and the NDP with 1,250 (Delacourt, 2021; Heath-Rawlings, 2021).

Not all microtargeting is precise. Although federal parties microtarget voters by effectively segmenting audiences, advertisement variations do not seem to be as sophisticated as those used by political parties in the US, primarily due to financial constraints. In other words, while variations of advertisements precisely target voters based on location, demographics, and message, very little evidence supports that

⁸ Ahead of the 2019 federal election, Google decided it would not be able to meet the requirement to host a political advertising library and took away its political advertising service in Canada (Gordon & Bennett, 2021).

⁹ Although most parties use Facebook, the NDP rotated into content creation on TikTok to reach and engage voters for the 2021 election, which is not currently defined as political advertising.

messages are designed to demobilize voters or that they are significantly nuanced to reach specific individual voter concerns (Bennett & Gordon, 2021; Participant B, February 15, 2022; Participant C, February 23, 2022). However, absent transparency and a more comprehensive understanding of how federal parties target voters with personalized advertisements, questions about consent are raised, particularly with regard to whether voters know how federal parties use their data to target them (Bennett & Gordon, 2021).

Little is also known about how and when federal parties disclose their data use to third parties. In Australia, researchers express concern about privacy exemptions that allow political parties to sell voter data to third parties for commercial gain (Cohen, 2021). In Canada, federal parties that share lists with social media platforms to create custom audience raises similar concerns about how federal parties may give sensitive and identifiable voter data to third parties without consent (C. Bennett, personal communication, March 1, 2022).

2.3. Balancing Democratic Engagement with Privacy Infringements and Voter Manipulation

Although the collection, use, and disclosure of personal data by federal parties can be regulated, many see this data collection as permissible because it can increase democratic participation and help inform the electorate (Dommett, 2019). Esselment suggests that permanently collecting and using data over the campaign cycle may bring parties authentically closer to voters' needs and real concerns (2017). Other researchers suggest microtargeting by federal parties can mobilize voters (Burkell & Ragan, 2019). A Statistics Canada survey after the 2019 federal election found 34.6% of eligible voters did not vote because they reported being "not interested in politics" (Elections Canada, 2020). Interview participants stressed that the collection, use, and disclosure of voter data by federal parties plays an important role in elections (K. Dommett, personal communication, March 3, 2022; Y. Dufresne, personal communication, February 23, 2022; Participant B, personal communication, February 15, 2022; Participant C, personal communication, February 23, 2022; K. Boessenkool, personal communication, February 11, 2022). However, if parties are optimal at campaigning and are efficient about where they invest resources to capture votes, some voter segments will never be engaged (C. Bennett, personal communication, March 1, 2022; Y. Dufresne, personal

communication, February 23, 2022). Overall, the extent that data-driven tools are (or can be) used to increase indicators of democratic participation such as voter turnout is unclear. Although turnout slightly increased between 2015 and 2019, rates for federal elections in Canada have generally fluctuated between 60-70% since 1993 (International IDEA, 2022). Data-driven campaigning is often pitched by data analytics companies and data brokers as the lynchpin to winning an election; however, one Conservative-affiliated interview participant suggested, since technologies and elections move quickly, it is challenging for parties to find data analytics companies that are not overpromising their capabilities and can deliver results at the polls (Bennett & Lyon, 2019; Participant C, personal communication, February 23, 2022). Baldwin-Phillipi (2007) suggests there are “myths” about data-driven campaigning, and news coverage often overcalculates what data-driven campaigns are able to achieve on the ground. Strategies are often more effective at mobilizing donors and established supporters than influencing voters (Baldwin-Phillipi, 2017). Ultimately, since elections are highly competitive, proprietary knowledge about the inner workings of data-driven campaigning in Canada is shrouded in secrecy.

Without adequate regulatory oversight to provide transparency and clarity, some researchers are concerned about the consequences of data-driven campaigning on voter privacy and the democratic integrity of elections. The OIPC’s 2019 investigative report—currently the best insight into the voter data collection, use, and disclosure practices of political parties in Canada—exemplified several key ways provincial parties infringe on voter privacy in Canada (McEvoy, 2019). While canvassing door-to-door, the OIPC found that all party representatives sometimes recorded observations about a voter’s ethnicity, religion, gender, and language. The voter was not informed about this data collection, raising significant questions about consent. One participant suggested that making inferences about voters who may belong to marginalized groups moves party data collection beyond privacy rights to a potentially more structured harm (F. McKelvey, personal communication, March 1, 2022). The OIPC also found that all parties made profiles of voters and scored them by their level of support, enabling parties to make predictions about their voting intentions without their consent, in contravention of BC PIPA. Additionally, the OIPC found that all parties turned over voter data to social media companies (e.g. disclosing lists of supporters to make use of

Facebook’s “Lookalike” audience tool). By extension, without transparency, federal parties are assumed to be infringing on voter privacy in the same ways.

A survey conducted for the Centre of Digital Rights found 85% of Canadians were unaware that federal parties are exempted from privacy laws and 87% of Canadians believed privacy laws should extend to federal parties (Campaign Research, 2019). The Office of the Privacy Commissioner of Canada (OPC) continues to receive complaints about invasions of voter privacy and, “has repeatedly called for political parties to be subject to legislation that creates obligations based on internationally recognized privacy principles and provide for an independent third party authority to verify compliance... to better protect both privacy and democratic rights” (Office of the Privacy Commissioner of Canada, 2021). The use of voter data is susceptible to misuses that have consequences for the legitimacy of electoral outcomes (Judge & Pal, 2021). Bennett further argues that the erosion of trust in the campaign process, resulting from voters being unsure of why they are seeing certain targeted advertisements, is a larger problem as a consequence of microtargeting (personal communication, March 1, 2022). Although the goal of parties during an election is to persuade voters, some researchers and advocacy groups suggest data-driven campaign practices like psychographic profiling and microtargeting go beyond reasonable persuasion efforts. Burkell and Ragan (2019) suggest unregulated data-driven campaigning practices that rely on filter bubbles and echo chambers as a result of platform algorithm designs are inherently polarizing and manipulative, undermining voters’ psychological ability to cast their ballots autonomously. As the authors argue, “manipulated messages can be designed to activate implicit attitudes and biases, with effects that are likely to be subtle, and operating at an unconscious level” (p.2). A study by Bailenson et al. (2008) found participants provided greater support to mock candidates when a candidate’s face was digitally altered only very slightly to resemble the participant’s face, another possible tool for deception that challenges the integrity of the electoral process but remains beyond regulatory oversight. If regulations set standards for the ways federal parties collect, use, and disclose data, then the issue of how parties microtarget to narrow voter segments—creating the problem of filter bubbles, echo chambers, deceitful messaging, and polarization—can start to be addressed; however, despite targeted complaints, sporadic litigation, news headlines, and social media campaigns, the combination of low political

will and strong resistance from federal parties has prevented further regulation (C. Bennett, personal communication, March 1, 2022).

Chapter 3.

The Current Patchwork of Data Protection Regulations for Federal Parties

This Chapter considers the current regulatory environment that impacts, in some way, how federal parties are able to campaign with voter data and data-driven tools. Broadly, Federal parties are regulated under the context of the *Canadian Charter of Rights and Freedoms* (the Charter). In the past, the Charter was used to challenge political financing regulations that were applied to federal parties. Although other high courts, such as in Australia and the US, have ruled that regulating political financing restricts freedom of speech; however, the Canadian high courts have not historically taken the same perspective—setting a precedent in 2004 by ruling the regulations were not a violation of the Charter¹⁰ (Falguera, Jones, & Ohman, 2014). As a result, federal parties in Canada are constrained by fundraising and spending limits. Tom Pitfield suggests, as a result of legislated spending caps, all federal parties aim for vote efficiency—forced “to deploy limited resources as efficiently as possible to the places where they’ll have the greatest impact” (Maher, 2021). Overall, federal parties are regulated by the *Canada Elections Act* (CEA), but are directly exempted from anti-spam legislation (Canada’s Anti-Spam Legislation and the Telecommunications Act) and the current patchwork of privacy legislation. Parties and Members of Parliament (MPs) also self-regulate, with some regulations impacting how MPs can collect and use voter data.

3.1. Canada Elections Act

The Canada Elections Act (CEA) regulates the federal electoral process in its entirety over the campaign cycle (including regulatory oversight for the election period processes, political financing, campaign advertising, and electoral districts, to name a few). A non-partisan, parliamentary agency, Elections Canada, is responsible for overseeing the CEA. The CEA is administered by the Chief Electoral Officer (CEO), who

¹⁰ In 2004, the Supreme Court of Canada ruled “the overriding aim of fair elections demands that all views shall be heard in an election campaign, and subsequently the use of financial resources should be limited to avoid unequal opportunities for the political competitors” (International IDEA, 2014).

reports directly to the House of Commons. The CEA entitles federal parties to receive basic information about each voter from the National Register of Electors—which contains the full name, gender, date of birth, civic and mailing address of each voter, and has become the building block for data-driven campaigning. The accuracy of the information in the National Register of Electors is maintained by the CEO and enhanced by sharing agreements between various federal and provincial bodies responsible for establishing lists of electors (Judge & Pal, 2021). Voters are able to request access to information that Elections Canada holds on them, update their data, and opt-out of the register entirely. Since Elections Canada is regulated by the *Privacy Act*, the Privacy Commissioner can audit how voter data is protected at any time.

The CEA has undergone a number of amendments. For example, the Conservatives and Liberals historically relied on corporate donations for political financing, disadvantaging smaller parties as competitors.¹¹ However, several amendments to the CEA in 2003 and 2006 introduced contribution limits and quarterly allowances (Feasby, 2010). As a result of the Facebook-Cambridge Analytica Scandal and concerns about data vulnerabilities for voters, in 2018, the *Elections Modernization Act* amended the CEA, requiring federal parties to create a privacy policy, submit it to Elections Canada, and publish it on their party websites—this amendment is discussed in more detail in section 3.4 on self-regulation (Government of Canada, 2022). The *Elections Modernization Act* also required social media companies to set up advertisement registries for political ads, which has indirectly impacted where federal parties can use voter data; leading up to the 2019 election, Google decided not to offer its political advertising service because it was unable to meet the requirement of setting up a registry (Bennett & Gordon, 2021). Beyond an obligation to have a privacy policy, federal parties are not regulated directly by any data protection laws under the CEA.

3.2. Anti-Spam Legislation

Federal parties are exempted from anti-spam legislation in Canada that, in some ways, could regulate the use and maintenance of voter data. First, federal parties are

¹¹ The Sponsorship Scandal, exposing that public money granted to corporations by the Liberal incumbent government was donated back to the party by those same corporations, instigated reform that introduced political financing regulations.

exempted from Canada's Anti-Spam Legislation (CASL). As a result, federal parties or candidates are able to use voter data to text or emails voters, asking for their opinions on various issues or for donations. Since parties are not regulated by CASL, voters are required to reach out directly to parties if they want to be removed from a mailing list, but parties are not obligated to comply (Government of Canada, 2020). Second, federal parties are also exempted from the Telecommunications Act, allowing them to use voter data by making calls to voters who are registered on the National Do Not Call List as long as they identify themselves (Government of Canada, 2019).

3.3. Privacy Legislation Regime

In Canada, privacy is mostly protected by the federal government, leveraging the *Canadian Charter of Rights and Freedoms* as a foundational tool.¹² The *Privacy Act*, which regulates the collection, use, and disclosure of personal information by public or government bodies, was introduced in 1980. Later introduced in 2000, the *Personal Information Protection and Electronics Documents Act* (PIPEDA) regulates the collection, use, and disclosure of personal information by the private sector as well as electronic documents and evidence. Since 2000, PIPEDA has also undergone several amendments. For example, in 2015, the *Digital Privacy Act* amended PIPEDA to introduce mandatory data breach notification requirements. However, as technologies quickly develop or emerge, advancing new threats to personal data privacy, specific rules added to regulate social networks, smartphone apps, and other online activities have lagged.

Currently, federal parties are considered a hybrid between a private organization and government organization, exempting them from PIPEDA and the Privacy Act. As a result, there are virtually no restrictions on their collection and use of voter data. This regulatory gap has enabled federal parties to advance complex VRM databases and canvassing applications, partner with big data analytics companies, and engage in political marketing at increasing rates (Bennett & McDonald, 2020). However, as one interview participant suggested, although federal parties may be directly exempted from

¹² Although mostly a federal responsibility, some provinces—such as Alberta, British Columbia, and Quebec—have statutes that regulate data privacy in the private sector and can take precedence in some cases.

the patchwork of privacy legislation in Canada, they are still indirectly constrained by it (Participant B, personal communication, February 15). Since PIPEDA regulates private organizations, any time federal parties purchase external data from data brokers or other sources, data sellers are prohibited from selling identifiable personal information if the data was collected for other purposes (e.g. to receive a magazine subscription). Consequently, unlike in the US where Republicans can, for example, buy the National Rifle Association donor's list and link the contributors directly to the party's voter profiles, "the secondary market for data acquisition in Canada is relatively limited" (Participant C, personal communication, February 23, 2022). In November 2020, the *Digital Charter Implementation Act* (formerly Bill C-11) was introduced to the House of Commons to significantly overhaul PIPEDA, but the legislation died when the writs were drawn up for the 2021 federal election. Bill C-11 proposed significant changes, including: expanded privacy rights for individuals (e.g. the right to erasure); modernized consent requirements; and, hefty administrative monetary penalties for any contravention (Stacey et al., 2020). However, federal parties continued to receive an exemption.

3.4. Self-Regulation

Absent legislated data protection requirements, federal parties engage in self-regulation. The Board of Internal Economy (BOIE)—a parliamentary committee of MPs—sets some rules for Member allowances that impact how MPs can collect data when they engage with their constituents (House of Commons, 2021). For example, if a MP sends out a piece of mail with a survey to ask their constituents about their views on political issues, the cost of that mail campaign can be covered by the parliamentary budget (within that MP's advertising budget limits). However, if the same mail campaign had a question asking constituents if the MP can count on their vote, delineating that question as clearly partisan, the BOIE requires MPs to use their party budget rather than the parliamentary budget (Participant B, personal communication, February 15, 2022). This stipulation can be constraining for parties with smaller party budgets.

Although the *Elections Modernization Act* obligates federal parties to create privacy policies, the contents of those policies are also self-regulated. As a result, the policies vary widely between parties. For example, the Green Party is the only party to explicitly state they do not engage in microtargeting practices (Green Party of Canada, 2022). As another example, although every party presents a definition for personal

information in their privacy policies, the NDP is the only federal party that defines personal information as “demographic information” in addition to name, address, e-mail address, telephone number, and financial information (New Democratic Party of Canada, 2022). Ultimately, researchers criticize the current privacy policies under the self-regulatory model for being insufficient. All parties’ policies are silent on whether voter data is collected from third-party aggregators and none explicitly mention the use of VRM databases (Judge & Pal, n.d.). Further, none of the policies clarify how federal parties may be sharing their collected voter data with third-parties like social media companies (C. Bennett, personal communication, March 1, 2022).

Chapter 4.

Methods

This research uses a literature review, jurisdictional scan, and qualitative data collected from interviews. The literature review draws on secondary sources, including academic articles, newspaper articles, government publications, research think tank publications, and podcast interviews; it also draws on primary sources such as government acts and the privacy policies of federal parties. The literature was searched using keywords such as “data-driven campaigning,” “vote efficiency,” “voter privacy,” “political marketing,” and “democratic engagement.” The jurisdictional scan identified three Anglosphere countries as appropriate comparators, which have different approaches of political party data regulation: Australia, the UK, and the US. Each case study: (1) provided an overview for the current state of data-driven campaigning; and (2) described the regulatory approach used to safeguard voter data. Ultimately, the bulk of the primary data collected was obtained through expert interviews.¹³ Selected for their expertise on data-driven campaigning in Canada, participants were recruited using publicly available contact information, or were referred by other participants. In total, 10 participants were interviewed—6 researchers, 3 federal party campaign officials, one lawyer, and one digital rights advocate. All federal party campaign officials had previous experience working for the Conservatives—officials from the Liberals and the NDP were contacted in the recruitment stage of research but did not opt to be interviewed. All participants were asked questions that related to: (1) how federal political parties in Canada use voter data over the campaign cycle; (2) assessing trade-offs between the status quo and further regulating federal parties; and (3) identifying policy options that may act to protect voter data, as needed. An interview guide was used to record initial notes, and automated speech-to-text technology was used to record audio and transcribe all the qualitative data gathered from interviews.

¹³ This research received ethics approval on December 17, 2021.

Chapter 5.

Jurisdictional Scan: Data-Driven Campaign Operations in the Anglosphere

This research began broadly scanning Western industrialized democracies that shared similar political-system features with Canada to determine the best comparators, finding data-driven campaign practices widespread. Ultimately, three Anglosphere countries were chosen: Australia, the UK, and the US. Canada, Australia, and the UK are Westminster-style systems; and, Canada, the UK, and the US are first-past-the-post systems. Interview participants identified all countries, frequently positioning the UK and the US as comparators. The regulatory environments in each country offer unique approaches to current data protection and, where regulation is absent, the future possibility of protection.

5.1. Australia

5.1.1. Data-Driven Campaigning in Australia

All political parties in Australia rely on the collection, use, and disclosure of voter data to execute data-driven campaigns; however, not all parties are using data-driven tools to the same extent (Kefford, 2021). Both major parties—the Labour Party and Liberal Party—have comprehensive VRM databases “which build on electoral roll data obtained from the Australian Electoral Commission and log all interactions a constituent has with an electorate office” (Paterson & Witzleb, 2019, p 162). Additionally, it is increasingly common for parties to purchase commercially available data (e.g. subscriber lists) to build out voter profiles and map out party strategy. However, not all parties have the expertise to make use of datasets (Kefford, 2021). Evidence suggests that the Labour Party, Green Party, and Liberal Party have all hired political consultants and used US-owned data-driven campaign platforms such as Nationbuilder to match Facebook profiles with voter profiles (Kaye & Paul, 2019). Software like Nationbuilder allows political parties in Australia to “leverage a suite of commoditized microtargeting tools offered by digital platforms such as Google and Facebook, built on the enormous data reserves held by those companies” (Cohen, 2021). Similar to Canada, all political

parties engage in political marketing and send personalized messages, targeting voters based on their geographical locations online in real time.

5.1.2. Regulatory Environment for Parties in Australia

Political parties in Australia are largely exempt from regulation (Kaye & Paul, 2019). Political parties, political representatives, vendors paid by parties to carry out political activities, and political party volunteers in Australia are all exempted to some degree from data privacy legislation, such as the *Australian Privacy Act* (Office of the Australian Information Commissioner, 2022). Similar to Canada and in dialogue with the *Australian Privacy Act*, the *Do Not Call Register Act* (2006) and the *Spam Act* (2003) both include carve-outs for political parties, exempting them from the prohibition on unsolicited calls and messages (Paterson & Witzleb, 2019). Exempted from Australia's spam legislation, during the 2019 federal campaign, the populist United Australia Party sent an unknown number of unsolicited text messages to voters stirring public concern over Australia's privacy laws; United Australia Party Senate candidate Clive Palmer defended the unsolicited text message campaign as "entirely legal under the *Privacy Act*" (Sweeney & Doran, 2019). Mass unsolicited text message campaigns coupled with the weak data storage practices of political parties prompted various public figures and researchers to repeal legislative exemptions for political parties but the Labour Party and the Liberal Party have resisted, "citing concerns about the impact on freedom of political communications, and consequently, the democratic process" (Cohen, 2021, p. 586). In addition to collecting data for free from voters through various canvassing efforts—and, as voting is compulsory in Australia, from the electoral roll containing the full names and addresses of all 16 million voters—parties are able to purchase external data from data-brokers if businesses who sell data meet consent and turnover conditions. Political parties are not regulated by political financing regulations such as contribution or spending limits and have the highest threshold for legally anonymous donations (which can facilitate foreign interference in elections) compared to the UK, US, and Canada—which, in 2014, was USD\$9350 compared to USD\$20 in Canada (Falguera, Jones, & Ohman, 2014); however, some political financing regulations exist at a state level.

Without transparency requirements for political parties under the *Australian Privacy Act*, data processing practices remain largely secret (Paterson and Witzleb, 2019). In 2008, the Australian Law Reform Commission (ALRC) recommended the

exemption for political parties be lifted as long as doing so does not “infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege,” but the Australia Privacy Act remained unchanged (p. 54). Similar to Canada, some academics argue that political party exemptions from the *Australian Privacy Act* both infringe on the privacy of Australians and threaten core democratic values (Cohen, 2021). Echoing the ALRC’s recommendation, in 2000, a survey found that 66% of Australians agreed that political parties should be covered by privacy legislation; later, in 2018, another survey on Australian attitudes to data privacy found that “76% of people objected to the collection of data about political or social views to share with political parties” (Kefford, 2021, pp. 147). As with the Privacy Commissioner in Canada, the Australian Information Commissioner continues to view the exemption as needed re-examination in the context of a changing digital environment (Kaye & Paul, 2019). A consultation launched by the Australian Government to review the *Australian Privacy Act* and possibly remove the political party privacy exemption closed on January 10, 2022 (Attorney-General’s Department, 2022); this review was launched alongside a consultation for the *Online Privacy Bill*—which closed on December 6, 2022—proposing to introduce a code of practice for social media and other online platforms in an attempt to enhance privacy protection online (Attorney-General’s Department, 2021). As of April 2022, privacy commissioners in Canada have similarly expressed public support to cover federal parties with privacy legislation, but Bill C-11 (the Digital Charter Implementation Act) that was introduced by the Liberals in November 2020—which proposed to significantly overhaul PIPEDA—maintained the regulatory exemption for parties.

5.2. United Kingdom

5.2.1. Data-Driven Campaigning in the UK

All political parties are increasingly engaged in data-driven campaigning practices to reach voters in the UK, despite having to comply with more stringent privacy protection laws than in Canada, Australia, or the US. Political parties in the UK operate VRM databases similar to parties in the US and Canada, using the same proprietary software (Bennett, 2016). Hankey, Morrison, and Naik (2018) suggest the history of data-driven campaigning in the UK comprises “a combination of polling, value-led

marketing and developments in voter databases” (p. 11). Political parties build VRM databases by supplementing basic information from the electoral roll with census data, commercially available data, and polling data; further, they are increasingly targeting voters based on segments (Anstead, 2017). Political parties in the UK are able to purchase data from data brokers, who collect commercial data, if the information is not sensitive, such as financial records from credit unions.

However, all national parties collect, use, and disclose voter data to varying degrees. Interviewing industry experts from various parties after the 2015 UK General Election, Anstead suggested, “smaller parties have limited capabilities, often simply using Microsoft (MS) Excel spreadsheets;” whereas, “larger UK political parties are developing databases capable of matching multiple years of the electoral register, making for more accurate analysis” (2017, p. 302). The Labour Party and the Conservative Party—the two parties with the largest supporter base, influence and income—spend more on data-driven campaigning than their competitors (Macintyre, Wright, & Hankey, 2018). Since 2015, political parties have significantly increased their investments into data-driven campaign practices. In 2011, political parties spent 0.3% of their total advertising budgets on advertising services through online platforms (such as Facebook, Instagram, Google, YouTube, Snapchat or Twitter) versus 42.8% of their budgets in 2017 (Electoral Commission, 2021). Despite an increasing reliance on data-driven tools, political parties are required to collect, use, and disclose data within the confines of data protection, marketing, and political financing regulations.

5.2.2. Regulatory Environment for Parties in the UK

Political parties in the UK are regulated by the *UK General Data Protection Regulation* (UK GDPR), the *Data Protection Act 2018* (DPA) and the *Privacy and Electronic Communications Regulations 2003* (PECR). As an adjacent piece of legislation, the DPA contains extra provisions for the application of the UK GDPR. For example, the DPA adds stronger legal protections for when political parties process sensitive voter data (Government of the United Kingdom, 2022). Layered on top, the PECR provides additional regulations for how voters can be contacted by an electronic method (e.g. text message) to promote a political view or otherwise influence them (Information Commissioner’s Office, 2022). Political parties that send electronic

newsletters or use cookies to track voter activity are required to comply with both the PECR and the UK GDPR.

The UK GDPR—effectively the equivalent of the European Union’s GDPR—was adopted after Brexit and is now retained as domestic law, regulating political parties the same way (CRI Group, 2021). The legislation outlines six legal reasons (outlined in Article 6 GDPR) that allow political parties to process voter data; most legal reasons for parties are either defined as public interest—an activity that promotes or supports democratic engagement—or defined as consent or legitimate interests—a political party uses voter data in ways a voter would expect (Yaffe, 2019). If investigated, parties are required to prove that their collection, use, and disclosure of voter data was lawful and legitimate. Since the UK GDPR was introduced, some UK parties have had to delete large amounts of data, initially gathered for purposes voters were not informed about (K. Dommett, personal communication, March 3, 2022). Regardless of the legal reasons, unless voters give explicit consent, political parties are mostly prohibited from collecting and using sensitive voter data, such as information revealing a voter’s: racial or ethnic background, religious beliefs, philosophical beliefs, trade union membership, genetics, biometrics (when used for identification), health, sex life or orientation (European Commission, 2022). Political parties are granted an exemption under the UK GDPR to process data on political opinions,¹⁴ as long as the appropriate safeguards are established. Consent is required to be free (voluntarily offered by a voter as a real choice), informed (a voter needs to know the identity of the data controller, how the data will be processed, and what the data will be processed for), and unambiguous (a voter needs to offer consent through either a declaration, an opt-in, or an affirmative action). Regardless of whether collected information is classified as sensitive or not, the UK GDPR allows voters to object to data collection, withdraw their consent, or retract their data, which may weaken voter profiles and profiling models, making microtargeting less effective. Further, the UK GDPR constrains the ability for political parties to profile by considering “much of the profiling and micro-targeting carried out by political parties and campaign groups...to be...‘solely automated decision-making,’”—a use of data the UK

¹⁴ The GDPR does not provide a definition for “political opinions.” However, “any type of clear, unambiguous statement, support or, as the case may be, rejection of a political party or of an ideological organization, any subscription to a politically oriented magazine, or participation in offline and online petitions, meetings or demonstrations most likely amount to political opinion” (GDPRhub, 2022).

GDPR restricts (Information Commissioner's Office, 2022). Additionally, political parties are responsible for keeping their collected data up-to-date and are obligated to track who in their organizations have access to voter lists and voter data, as well as, to prevent wide access (European Commission, 2018).

Although the UK GDPR and European GDPR are considered gold standards in the world on data protection regulations by many researchers, there still appear to be some gaps. Some privacy experts suggest political parties continue to collect data linked to sensitive subjects like religion, which remains a legal gray area (Scott, 2020). Despite regulatory efforts taken to safeguard voter data in the UK, many political parties and big data analytics companies employed by parties have breached data protection laws (Information Commissioner's Office, 2018). In 2020, an Information Commissioner's Office audit "found only a limited level of assurance that processes and procedures were in place and delivering the necessary data protection compliance" with "considerable areas for improvement in both transparency and lawfulness" and provided various recommendations to bring the data collection and use practices of political parties in compliance with data protection laws (pp. 4-6).

Similar to Canada, the UK has political financing regulations on campaign spending (caps on party spending, candidate spending, third-party spending); however, contributions to parties are not limited (Falguera, Jones, Ohman, 2014). Since political parties are also required to report campaign financial expenditures to the Elections Commission, clear data shows that political parties purchased digital platforms, advertising and data companies, consultants, and strategists in the 2015 and 2017 General Elections; however, more transparency is needed to determine what data-driven benefits were gained (Hankey, Morrison, & Naik, 2018). It is unclear how much political financing regulations constrain political parties from being able to afford large-scale data-driven campaign operations.

5.3. United States

5.3.1. Data-Driven Campaigning in the US

Adopted from the commercial sector, data-driven campaign practices perform at the largest scale, globally, in the US and are fundamental to campaigning. Historically,

political parties and voters have been “tolerant of a variety of practices to monitor and profile the electorate, and use the techniques of direct marketing to poll, canvass, and get-out-the-vote” (Bennett, 2016, p. 262). Republicans and Democrats both work with data brokers and other vendors to create sophisticated VRM databases, “collecting information from many sources to create detailed profiles of voters with thousands of data points and build models that predict people’s stances on issues or candidates” (Culliford, 2020). Similar to Canada, voter data is collected freely from voter registration, donor lists, website cookies, and inferences from canvassing, to name a few. Voter data is also purchased from commercial vendors. Since data protection legislation exempts commercial third-party data, political parties are able to purchase an extensive amount of information such as real estate property records, magazine subscriber lists, and gun purchasing records. Party registration data and past voting behaviour is also tracked in the US—this includes when a person votes and how often a person votes but not who a person votes for (Rubinstein, 2014). Data collection is centralized through digital tools (e.g. algorithms) that clean and layer voter data for the purposes of identifying support and microtargeting voters. After parties have a foundation of voter profiles, they score voters on their level of party support (e.g. John Doe scores 70% likely to vote for a Democratic candidate) and run predictive modelling to determine a voter’s opinions on political issues. Further, parties target voters with personalized advertising based on psychographic profiling. In the 2016 presidential election, psychographic profiling was reportedly used by the Republican Party to suppress three groups of Hillary Clinton voters (e.g. idealistic white liberals, young women, and African Americans) from casting a ballot (Green & Issenberg, 2016). Sold to political parties all over the world, technologies in the US that collect and use voter data have become increasingly sophisticated. VRM databases are integrated across a variety of other digital tools that support campaign activities such as canvassing apps. Many vendors in the US are available for hire to achieve data-driven campaign strategies. Data-driven campaigns are largely executed, managed, and enabled by private consulting firms that work with a growing industry of data intermediaries (e.g. data brokers) and private firms from politically adjacent industries (e.g. Facebook or Twitter).

Since Republicans and Democrats are not constrained by donor contribution or party/candidate spending caps, they are able to spend significant amounts per voter over the campaign cycle. One interview participant suggested that in the US,

“presidential campaigns are running \$3-4 billion campaigns, it's \$8 per voter—and that's just for one office—plus the Senate gubernatorial house always going to ballot races...in the 2022 cycle, we may see budgets of \$10-15 per eligible voter” (Participant B, personal communication, Feb 15, 2022). Further, the participant suggested, big budgets and little regulations enable new parties to pay \$5000 to a data-analytics company and be set-up to start data-driven campaigning within 24 hours (Participant B, personal communication, Feb 15, 2022). With significant gaps in privacy protection legislation and no political financing regulations, Democrats and Republics have the flexibility to afford running permanent data-driven campaigns at a scale not seen in other Western industrialized democracies.

5.3.2. Regulatory Environment for Parties in the US

The US context is characterized by the absence of regulatory legislation, a protection of democratic engagement under the First Amendment, and opt-in voter registration databases at the state-level. Weak data protection legislation encourages the unfettered collection and use of voter data by political parties, with formal privacy statutes taking the form of “sets of rules directed towards specific sectors, such as health, banking, and consumer credit. The result is a complicated patchwork of federal and state laws with significant gaps” (Bennett, 2012). Further, the Supreme Court has protected political speech in a couple of ways. Ostensibly to preserve and uphold democracy, political speech is protected under the First Amendment (free speech)—particularly concerning the right of voters to support politicians or political candidates. As an extension of political speech under the first amendment, political contributions and spending has also been ruled as a form of speech since “people who intend to express their views may want to spend money to be heard by others, and they may speak up collectively to promote their political views without restriction” (Falguera, Jones, & Ohman, 2014, p. 257). The absence of political financing regulations allows parties to fundraise and spend an exponential amount of money on comprehensive data-driven campaigning operations.

In 2002, the *Help America Vote Act* (HAVA) required states to keep a centralized voter registration database in which privacy concerns were meant to be “fully and carefully addressed in designing the system” on a self-regulated basis (Brennan Center for Justice, n.d.). HAVA likely provided the groundwork for political parties to set up their

own VRM databases (Bennett, 2016). However, information for every voter is not kept in the VRM databases in the US. To remedy voter suppression as a result of historical racial prejudices, voters in the US are able to “opt-in” and “opt-out” of VRM databases at a state level, instead of being automatically registered like in Canada (MIT Election Data and Science Lab, 2022). In some states, voter registration lists are available to anyone from the public. For example, in the state of Alaska, a voter list is provided to anyone by request, containing the names, addresses, and party affiliations of registered voters (National Conference of State Legislators, 2022). It is possible that anyone with an intention to discriminate against another person’s gender, ethnicity, or religion could infer an identity from the list of names and know where that person lives.

Krotoszynski Jr. (2019) suggests structural reforms or regulations that prohibit the collection, use, and disclosure of voter data by political parties in the US are needed. On the one hand, structural reform could use big data to adapt gerrymandering by making ridings more competitive. Once partisan support is identified, instead of rigging the electoral boundaries of ridings so the riding is more Republican or more Democratic, electoral boundaries can be drawn so the riding better represents mixed partisan support. On the other hand, regulations could be set to safeguard the collection, use, and storage of voter data. Recently, several bills have been introduced in US Congress with some bipartisan support, including the *Consumer Online Privacy Rights Act*, *Consumer Data Privacy Act*, *Filter Bubble Transparency Act*, and *Do Not Track Act*, to name a few. However, bills sponsored by Democrats make up most of federal privacy legislation, and have not been able to secure bipartisan support (Fazlioglu, 2019). Krotoszynski Jr. suggests that, “given the Supreme Court’s holding that the gathering and mining of data constitutes ‘speech’, any legislative efforts to rein in such practices will have to survive strict judicial scrutiny” (2019, pp. 198). Further regulation may be considered a First Amendment challenge.

Chapter 6.

Interview Findings

Ten semi-structured interviews were conducted with researchers (n=5), Conservative campaign officials (n=3), one lawyer, and one data protection advocate (Appendix B). These interviews were critical to this research and attempted to engage a variety of participants as diverse stakeholders. The qualitative data was used to support and supplement published work captured by the literature review, providing important insights into the current state of data-driven campaigning in Canada, the trade-offs between the status quo and data protection regulation, and possible regulatory approaches. This section discusses four primary themes that emerged from the interviews.

6.1. Data-Driven Campaign Practices Lack Transparency

We're told that data and digital campaigns makes such a huge difference these days. And it actually does make the difference between who's in the government and the opposition. And yet, the practices are shrouded in so much mystery. If it's so important, so critical, to the point that determining which party forms the government, then isn't establishing more transparency and understanding and debate, the conversation in Canada about what is appropriate and what is not.

– Colin Bennett, Academic

There was a concern back in the spring of 2018, could Facebook-Cambridge Analytica debacle happened here? Is it happening? And the truth is, no one knew—not even the regulators.

– Bill Hearn, Regulatory Lawyer

The interviews highlighted how little researchers, lawyers, and digital rights advocates know about the intricacies and sophistication of data-driven campaign operations in Canada. Conservative campaign officials described their data collection, use, and disclosure methods to varying degrees; all officials described VRM databases and digital advertising as supplementary to traditional canvassing methods, but no official provided clear details about how computational tools and algorithms are used by parties. Non-party affiliated interview participants suggested the lack of transparency is problematic for various reasons. First, without open knowledge of how federal parties

collect, use, and disclose voter data, journalists, researchers, and policymakers are not able to assess the validity of potential concerns. Second, without transparency, it is difficult for journalists, researchers, and policymakers to hold federal parties accountable if data is used in ways that may infringe on privacy or compromise democratic integrity. Interview participants suggested the lack of transparency was a result of privacy legislation exemptions and no regulatory oversight for the way federal parties campaign with data.

6.2. No Political Will to Include in Federal Parties in Data Protection Legislation

My experience has been the political parties fighting tooth and nail to have a nonpartisan independent expert just look at what they're doing...if what they're doing isn't nefarious, what's the problem?

– Bill Hearn, Regulatory Lawyer

In general, it seems clear at this point that the way parties collect data is a privacy issue and the fact that it continues to not be regulated under PIPEDA or the reforms to PIPEDA is—at this point—an inexcusable omission, that seems, as far as I can tell, solely motivated by partisan ambition.

– Fenwick McKelvey, Academic

Interview participants felt there was little political will for any federal party or Member of Parliament to bring legislation forward in the House of Commons that would extend data protection legislation to cover themselves. With some variation, all Conservative campaign officials were generally opposed to regulation. Over the last few years, legal complaints have been filed on behalf of individual complainants to the Competition Bureau of Canada, Canadian Radio-television and Telecommunications Commission, Elections Canada (CRTC), OPC, and OIPC. All major federal parties, regardless of partisanship, hired big law firms to fight the submissions and maintain their status quo exemptions. Many interview participants offered policy options with the pretext that they would be difficult to make happen.

6.3. Participants Differed on How to Approach Data Protection Regulation

Basically if I was going back to square one, and looking at where I would start from a policy perspective and revelatory perspective, it would be a long and rather heated conversation with folks on the big tech side of it rather than the parties themselves.

– Participant B, Conservative Campaign Official

It's not just the data practices, it's the algorithms that go with that data. And once you've trained the algorithms, it's almost like the data isn't quite as important as it used to be. Because I can sort of infer that with a fraction of the data that I used to have. It used to be the tyranny of the data (collecting practices and profiling). Now, it's almost the tyranny of the algorithms more than the practices.

– Participant D, Data Protection Advocate

My personal view is that PIPEDA is the right vehicle and through PIPEDA there could be some kind of code of practice, developed by PIPEDA or the son of PIPEDA, whatever it's called C-11 that's supposed to be coming down the pike.”

– Colin Bennett, Academic

Interview participants' responses differed on whether federal parties should be regulated by data protection. Some participants did not believe data protection regulation was possible, or they believed there was not enough good evidence at this point to demonstrate why data protection regulation was needed. One party campaign official was concerned that if the government built and exercised control over federal parties, it could be extraordinarily dangerous to federal parties prevented from reaching and engaging voters in the long run. Other participants saw absolutely no reason why federal parties continue to receive privacy law exemptions, definitively believing their data practices should be regulated.

Interview participants who thought further regulation was necessary had diverse suggestions for how to approach regulation. Some interview participants believed restricting the ways federal parties could use social media platforms to campaign by regulating big tech companies would be more beneficial than directly regulating the ways federal parties collect, use, and disclose voter data. Other interview participants argued applying data protection legislation to federal parties would level the playing field—with no single federal party having a competitive advantage and all parties better off. Mostly, overhauling PIPEDA and removing the federal party exemption was suggested as the

appropriate policy vehicle for regulation. Several interview participants thought the Commissioner of Canada Elections did not have the expertise to efficiently provide guidance and enforce data protection regulation; however, one party campaign official suggested they would rather see the Commissioner of Canada Elections regulate federal parties than have a one-size-fits-all privacy legislation extended to cover them. One academic participant suggested two regulatory approaches not commonly discussed as remedies in the literature. First, they suggested that increasing the per vote subsidy could inadvertently act as a privacy remedy by removing some pressure on federal parties to collect, use, and disclose voter data to fundraise.¹⁵ Second, as an expansion of the National Register of Electors, they suggested that Elections Canada could become a clearinghouse for voter data with all parties having access to and using the same information, restricted from collecting or using their own.

Many interview participants emphasized that federal parties use data differently than private organizations to engage voters in the democratic process—further suggesting that not all data uses by federal parties are inherently nefarious. Most participants who advocated to cover federal parties with privacy legislation were not necessarily arguing to strip away the ability of federal parties to collect and use voter data; instead, they argued, further regulation could provide clarity through rules that set limits and reasonable expectations, striking a balance between engaging voters, protecting voter privacy, and protecting the democratic legitimacy of elections. Although a few interview participants viewed federal parties as essentially operating like private organizations, they advanced a code of practice as a way to cover parties with data protection legislation in a way that recognized parties as unique—providing more flexibility for data-driven campaigning in some cases.

6.4. Data Operations are Relatively Small and Less Sophisticated as Compared to the US

“We try and do as sophisticated of things as we can but we’re constrained because we don’t have issue information on a very sizable portion of the Canadian electorate. We know a little bit about a lot of people but not enough to have the type of effective interactions that would really be necessary to do this at scale.”

¹⁵ The per-vote subsidy was phased out in 2015, which has put pressure on federal parties to fundraise large sums of money from voters. In 2018, it was estimated that reinstating the per-vote subsidy would cost \$44M per year (The Canadian Press, 2018).

– Participant B, Conservative Campaign Official

“The party data operations in Canada are tiny by global comparisons, even by Canadian comparisons. Canada Post has a billion times more information about its customers. For political party (during election campaign) spending is regulated so you're talking about a \$27 or \$30 million spending cap, which has to cover everything. So the data portion of that might be \$1 million—depending on how the party counts data, what the strategy is. And between elections, the parties are running on about \$10-12 million a year of an operating budget for national election readiness activities—of which data is a part of that. Kellogg's in Canada will spend more than 10 times that a year on data; and, the banks would spend like 100 times that. So we're talking about relatively small data operations.”

– Participant C, Conservative Campaign Official

Conservative campaign officials emphasized that federal parties in Canada are indirectly constrained by other regulatory legislations around campaigns, resulting in smaller and less sophisticated data operations than operations in the US. By limiting how much parties can fundraise and spend, political financing regulations prevent federal parties from being able to extensively partner with data analytics companies and data brokers. Further, unlike parties in the US, federal parties in Canada are constrained by what information they can outright purchase from data brokers, since the sale of personal data held by private organizations in the first place is regulated by PIPEDA, and usually needs to be de-identified before being sold. Given these indirect constraints on federal parties, to supplement a select number of data analytics and data broker partnerships, a substantial amount of time is required for volunteers to incrementally collect and input data where they can over the campaign cycle. However, a few other participants suggested that despite potential constraints, all major parties have worked closely with American political parties and companies to build and model their own databases, canvassing applications, and big data analytics tools.

Chapter 7.

Policy Options

Interview participants advanced several policy options intended to safeguard voter data. Based on these interviews, and other research compiled for this analysis, this section outlines four policy options that regulate how federal parties campaign with voter data and data-driven tools. In other words, alongside the collection, use, and disclosure of voter data, each policy option considers the need for algorithm standards and certification mechanisms. All options vary fundamentally in approach, with the exception of overhauling PIPEDA and amending the *Canada Election Act*, which are similar but regulate federal parties under different regulatory bodies.

7.1. Overhaul PIPEDA and Extend to Federal Parties

Frequently identified by interview participants, option 1 proposes to overhaul PIPEDA to align it with the data protection principles of the European Union’s General Data Protection Regulation (GDPR) and extend its regulatory scope to federal parties (see Table 7.1 for a list of all GDPR data protection principles). Option 1 also proposes to apply a code of practice to acknowledge circumstances where the lawful collection, use, and disclosure of data may be unique as compared to private organizations—determined as an agreement between federal parties and the Office of the Privacy Commissioner of Canada (OPC). Similarly, although the GDPR generally restricts political opinions from being collected, it provides political parties with more flexibility than other private organizations—allowing parties to process data on political opinions for electoral activities as long as safeguards are established.¹⁶ Rolled into the GDPR data protection principles, voters would have certain rights over their data, including: the right to be informed, the right of access, the right of rectification, the right of erasure, the right to restrict processing, the right of data portability, the right to object, and rights in relation to automated decision making and profiling. For example, the GDPR data

¹⁶ Recital 56 of the GDPR grants political parties some flexibility to process data: “Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people’s political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established” (GDPR.EU, 2022).

protection principles would set standards for federal parties that restrict them from collecting sensitive personal information on voters,¹⁷ require them to prove the legal reasons for collecting and using voter data (e.g. parties are expected to use voter data in ways voters would expect), prohibit the use of automated software used for profiling, and allow voters the right to opt-out of data collection and use. Federal parties would have to receive a voter’s informed consent before any inferred data can be collected while canvassing. The OPC would be responsible for investigating the voter data collection and uses of federal parties and could issue fines of between \$10-25 million or 3-5% of an organization’s gross global annual revenue, as suggested by C-11 (Stacey et al., 2020). This option would also prevent federal parties from allowing wide access to voter lists and VRM databases, requiring them to provide selective access based on a registered list of party affiliates.

Table 7.1. GDPR Data Protection Principles

#	Principle	Description
1	Lawfulness, fairness and transparency	Processing is lawful, fair, and transparent to the data subject
2	Purpose limitation	Data is processed for legitimate purposes specified explicitly to the voter when collected
3	Data minimization	Only as much data is collected and processed as absolutely necessary for the lawful purposes specified
4	Accuracy	Stored personal data is accurate and up to date
5	Storage limitation	Personally identifying data is only stored for as long as necessary for the specified purpose
6	Integrity and confidentiality	Processing is done in a way that ensures appropriate security, integrity, and confidentiality (e.g. by using encryption)
7	Accountability	Data controller is responsible for demonstrating compliance with all of the GDPR data protection principles outlined

¹⁷ The GDPR defines sensitive personal information as information revealing a voter’s racial or ethnic background, political opinions, religious beliefs, philosophical beliefs, trade union membership, genetics, biometrics (when used for identification), health, sex life or orientation (European Commission, 2022).

7.2. Amend CEA: Apply GDPR Data Protection Principles to Federal Parties

Since Elections Canada specializes in election administration, a second option would be to regulate the collection, use, and disclosure of voter data by federal parties by amending the CEA (Judge & Pal, 2021). The GDPR data protection principles outlined in option 1 would be applied at all times (not only over a defined election period); similarly, federal parties would have to gain informed consent for all data collection—including inferred data (e.g. canvassing inferences)—and voters would have the same data privacy rights listed in option 1 (e.g. the right to erasure). The Commissioner of Canada Elections (CCE) would be responsible for investigating federal parties and issuing fines if federal parties fail to comply. Option 2 varies from option 1 because the CCE’s regulatory expertise pertains broadly to the operations of campaigning, elections, and referendums rather than personal privacy and data protection. This option was the second most frequently identified by interview participants.

7.3. Amend CEA: Regulate Platform Accountability and Provide Voluntary Code of Practice

In interviews, campaign officials were generally opposed to policy options that directly regulated their data practices under broad, catch-all privacy legislation (K. Boessenkool, personal communication, February 11, 2022; Participant B, personal communication, March 15; Participant C, personal communication, February 23, 2022); alternatively, one interview participant suggested, regulating the algorithms of social media platforms is likely a better approach to protect data privacy and ensure the democratic integrity of elections (Participant B, personal communication, March 15). Option 3 proposes an amendment of the CEA to include stronger platform accountability beyond the current political advertisement library—and its limitations (Burkell & Ragan, 2019; Participant A, personal communication, March 16; Participant B, personal communication, March 15). To better regulate political advertising and microtargeting, online platforms would be required to disclose: (1) who is sponsoring political advertisements; (2) how ads are microtargeted. Federal parties would not be restricted from scraping voter data from online platforms but online platforms would be required to notify voters if federal parties collect their information. The amendment also proposes to

define a set of algorithm standards and to advance a certification mechanism for algorithms used by online platforms when political parties advertise or scrape Facebook ID information. Standards would include requirements for platforms to design algorithms from sufficiently large and diverse data sets, adequately representative of various demographics that could be used as a foundation for discrimination. Standards would also include requirements to ensure records are kept how algorithms are built, trained, and validated. Platforms would be required to keep records on the expected accuracy and limitations of an algorithm. Users would be able to request information about how an algorithm made a predictions about them, if systems were used to make automated decisions. Further, all algorithms would require human oversight. If algorithms are used by platforms in ways out of compliance with the defined standards, platform companies would be required to disgorge them.

Algorithms used by federal parties independently from platforms would be held to adjacent voluntary standards, defined by a voluntary code of practice that federal parties are required to design alongside the Commissioner of Canada Elections (CCE). A voluntary code of practice would outline best practices for the collection, use, and disclosure of voter data that voters can publicly access. For example, a best practice could state that, while canvassing, parties should not record assumptions about a voter's gender, ethnicity, or religion. However, there would be no penalties if federal parties were found to be out of compliance with the voluntary code.

7.4. New Legislation: Establish Singular Elections Canada Voter Database

Currently, Elections Canada provides all parties with the voter list four times per year, giving federal parties the full names and addresses of all eligible voters. However, to even the playing field, more information could be provided to federal parties by Elections Canada, with the most valuable data being email addresses and phone numbers of eligible voters in addition to full names and addresses (Participant B, personal communication, February 15, 2022). Building from a suggestion advanced by an interview participant, option 4 would introduce a separate piece of legislation “to restrict parties from collecting data and to incentivize Election Canada to be a clearinghouse for data so that it levels the playing field for...data analytics” (F. McKelvey, personal communication, March 1, 2022). Under this option, the CCE would

be the designated regulator responsible for investigating federal parties and issuing fines when appropriate. Instead of collecting and using data independently over the campaign cycle, all federal parties would be required to use data from the same data storage database provided by Elections Canada. The Elections Canada database, as a clearinghouse, would build out the National Register of Electors to collect and store semi-granular data; further, it would be responsible for keeping information current throughout the year. All federal parties would be required to pay approximately 5% of their budgets to fund the Elections Canada voter database infrastructure and operation.

Although Elections Canada is currently regulated by the *Privacy Act*, this policy option would provide Elections Canada with an exemption to set-up and maintain the voter database, with some conditions. First, Elections Canada would have to report how the voter data collected and stored is relevant to the political process and/or in the public interest. Second, Elections Canada would not be able to include sensitive personal information—as defined by the GDPR¹⁸—unless a voter gave unambiguous and informed consent. Third, Elections Canada would be required to offer a plain language transparency statement explaining how data on voters gets collect and used. Fourth, Elections Canada would have to offer voters the possibility of opting-out. Parties would not be permitted to allow wide access to the database, with only a certain number of recorded party affiliates able to login.

¹⁸ The GDPR defines sensitive personal information as information revealing a voter’s racial or ethnic background, political opinions, religious beliefs, philosophical beliefs, trade union membership, genetics, biometrics (when used for identification), health, sex life or orientation (European Commission, 2022).

Chapter 8.

Evaluation Criteria & Measures

To evaluate the policy options described in Chapter 6, three societal and governmental objectives are outlined below: effectiveness, compliance issues, and administrative complexity. Each objective is defined as criteria that are scored on a three-point scale with the effectiveness objective—as the key objective—double weighted. For a summary of all the criteria and measures, please see Table 8.2 at the end of Chapter 8.

8.1. Effectiveness

This research highlights the current regulatory gap in data protection legislation that enables federal parties to collect, use, and disclose data as a way of reaching and engaging voters. Interview participants and published literature often presented regulation and democratic engagement as trade-offs. To account for both considerations, the “effectiveness” objective is split into two criteria: “data protection” and “democratic engagement.”

The “data protection” criterion evaluates how thoroughly each policy option safeguards the collection, use, and disclosure of voter data—including through the use of data-driven tools such as profiling algorithms. Judge and Pal’s (2021) guidelines for voter privacy reform will be used to assess each policy option (see Table 7.1 for a summary of guidelines). Considering that concerns over privacy infringement and the democratic integrity of elections are linked, democratic integrity will be safeguarded as a result of privacy protection. For example, guidelines that change the way parties are able to microtarget, provide voters with the right to know how algorithms made decisions about them, require federal parties to gain consent before making inferences about voters, and are broad enough to extend to new technologies as they emerge, are expected to go some way to safeguard the threats to democracy discussed in Chapter 2. Data protection will be scored as “high” if all guidelines are met. Data protection will be scored as “moderate” if between 6 and 10 data principles are met. Data protection will be scored as “weak” if 5 or fewer data principles are met.

Both campaign officials and researchers stress the importance of independent voter data collection, use, and disclosure to reach and engage voters in the democratic process; for candidates and MPs to effectively understand what issues matter to their constituents, some granular data is needed (K. Boessenkool, personal communication, February 11, 2022; Participant B, personal communication, February 15, 2022; Participant C, February 23, 2022; K. Dommett, personal communication, March 3, 2022; Y. Dufresne, personal communication, February 23, 2022). Based on the assumption that some granular data can help parties reach voters and engage the electorate over the campaign cycle, the “democratic engagement” criterion evaluates whether each policy option gives parties the flexibility to collect, use, and disclose data broadly. This criteria also assumes the opportunity to collect, use, and disclose “issue information” and other forms of granular data will be used for good reasons—connecting voters to issues that matter to them and helping parties or candidates understand what really matters to Canadians, thereby enhancing the democratic process. Democratic engagement will be scored as “democracy enhancing” if federal parties have the flexibility to collect, use, and disclose granular data without significant data protection regulations that may constrain democratic engagement (e.g. parties would be able to use private algorithms and in-house VRM databases linked to canvassing apps). Democratic engagement will be scored as “somewhat democracy enhancing” if federal parties have the flexibility to collect, use, and disclose granular data broadly but are obligated to comply with data protection regulations that somewhat constrain their data practices, inhibiting engagement. Democratic engagement will be scored as “not democracy enhancing” if federal parties do not have the flexibility to collect, use, or disclose granular data broadly as a result of data protection regulations that significantly inhibit engagement.

Table 8.1. Guidelines for Voter Privacy Reform (Judge & Pal, 2021)

#	Guideline	Description
1	Mandatory obligations	Protections that apply to parties are mandatory
2	Continuous application of privacy obligations	Protections apply continuously rather than in the election period, to align with the year-long campaign strategies of federal parties
3	Protect individual voters rather than “voter data”	Voter data is <i>not</i> differentiated in legislation as different from broader legal definitions of personal information
4	Technological neutrality and future-focused regulation	Legislation is broad enough to apply to new technologies that will inevitably develop

5	Limit data use to political purposes only and prohibit commercial activities	Federal parties are <i>not</i> permitted to sell or transfer voter data to other entities seeking to use this information for commercial gain
6	Informed consent	Federal parties are required to obtain informed consent for any personal information, including inferences pertaining to individuals.
7	Expand opt-out to cover any personal information held by political parties	Voters are able to opt-out of all data collected, used, and disclosed by federal parties—not just the National Register of Electors
8	Additional voter rights pertaining to big-data analytics	Voters have the right to: know specifics about the information federal parties hold on them; know how their data was obtained; correct data if inaccurate; receive an explanation for how an algorithm made decisions about their voting preferences or persuadability; and, erase data
9	Data sharing	Federal parties are regulated on how they share voter information with third parties, with other parties, and within their parties
10	Cybersecurity protocols	Federal parties are required to implement cybersecurity protocols that protect the storage and transmission of voter data
11	Enforcement	Legislation has strong enforcement, compliance, and oversight measures; regulator has sufficient powers to levy fines and make orders

8.2. Compliance Issues

In some cases, not all federal parties may have the adequate resources to comply with data protection obligations compared to large, established federal parties. The “compliance issues” criterion evaluates whether the policy option makes compliance requirements easy to achieve for all federal parties. Compliance barriers will be scored as “low resources” if the compliance process is clear and simple without federal parties requiring many additional resources to meet requirements. Compliance barriers will be scored as “moderate resources” if the compliance process is clear but requires additional resources from parties to meet requirements. Compliance barriers will be scored as “high resources” if the compliance process inhibits parties from operating effectively and requires additional resources from parties to meet requirements.

8.3. Administrative Complexity

The “administrative complexity” criterion evaluates the expected governmental complexity of integrating each policy option within the existing patchwork of legislation. This criterion considers if existing legislation can be amended or if new legislation needs

to be introduced. Further, this criterion considers if government infrastructure (e.g. an internal database) or new regulatory bodies need to be established (e.g. the organization needs to be expanded or training is required). A score of “low complexity” will be given if the policy option can be implemented easily within the patchwork of legislation, government infrastructure, and regulatory bodies already in place. A score of “medium complexity” will be given if the policy option further complicates the existing patchwork of legislation, and if coordination may be required between government organizations or if either a new regulatory body needs to be established or government infrastructure needs to be established. A score of “high complexity” will be given if the policy option layers to complicate the existing patchwork of legislation, and if both new government infrastructure and regulatory bodies need to be established.

Table 8.2. Criteria and Measures

Objective	Criteria	Measure	Score
Key Objective			
Effectiveness Double weight	(A) Data Protection: Amount of voter privacy guidelines applied as safeguards	All voter privacy guidelines are met	High Protection (6)
		Between 6 and 10 voter privacy guidelines are met	Moderate Protection (4)
		5 or less voter privacy guidelines are met	Weak Protection (2)
	(B) Democratic Engagement: Flexibility of federal parties to broadly to reach and engage the electorate with granular voter data	Parties have the flexibility to collect, use, and disclose granular data broadly, with no significant data protection regulations that impede democratic engagement	Democracy Enhancing (6)
		Parties have some flexibility to collect, use, and disclose granular data broadly but are somewhat constrained by data protection regulations that impede democratic engagement	Somewhat Enhancing (4)
		Parties do not have flexibility to collect, use, and disclose granular data broadly due to data protection regulations that significantly impede democratic engagement	Not Enhancing (2)
Additional Considerations			
Compliance Issues	Barriers to compliance requirements that require additional party resources	Compliance process is simple and clear and does not require many additional party resources to meet	Low Resources (3)
		Compliance process is clear but requires additional party resources to meet	Moderate Resources (2)
		Compliance process is unclear, inhibits parties from operating effectively, and requires additional party resources to meet	High Resources (1)
Administrative Complexity	Complexity of integrating the policy option, considering the existing patchwork of legislation and the administrative ease of implementation	Easy integration within the existing framework, government infrastructure, and regulatory bodies	Low Complexity (3)
		Slightly complex integration where some coordination between government departments may be required and either new government infrastructure or regulatory bodies need to be established	Medium Complexity (2)
		Complex integration where legislation layers on top of the existing framework and new government infrastructure or regulatory bodies need to be established	High Complexity (1)
			/18

Chapter 9.

Evaluation of Policy Options

In this chapter, the policy options identified in Chapter 6 are analyzed using the criteria and measures from Table 8.2. Options were analyzed using a jurisdictional scan, interviews, and literature review. A summary of the evaluation is presented below in Table 9.1, with each policy option receiving a score out of 18. Option 1 received the highest score and Option 4 received the lowest score.

Table 9.1. Summary of Policy Analysis

Objective	Criteria	Overhaul & Regulate Parties: PIPEDA	Regulate Parties: CEA	Platform Regulation & Voluntary Code: CEA	Elections Canada Database
Effectiveness Double weight	(A) Data Protection: Amount of voter privacy guidelines applied as safeguards	High Protection (6)	Moderate Protection (4)	Low Protection (2)	Moderate Protection (4)
	(B) Democratic Engagement: Flexibility of federal parties to broadly to reach and engage the electorate with granular voter data	Moderately Restricted (4)	Moderately Restricted (4)	Not Restricted (6)	Completely Restricted (2)
Compliance Issues	Barriers to compliance requirements that require additional party resources	Moderate Resources (2)	High Resources (1)	Low Resources (3)	Low Resources (3)
Administrative Complexity	Complexity of integrating the policy option, considering the existing patchwork of legislation and the administrative ease of implementation	Low Complexity (3)	Moderate Complexity (2)	Moderate Complexity (2)	High Complexity (1)
		15	11	13	10

9.1. Analysis 1: Overhaul and Regulate Parties – PIPEDA

9.1.1. Effectiveness

Option 1 is expected to meet all the voter privacy guidelines, resulting in **high protection**. Data protections applied to federal parties would be mandatory at all times. Federal parties would also be responsible for acquiring meaningful and unambiguous consent in all their data collection activities, as well as securing data with better storage practices. Data-sharing would be further constrained, dependent on how parties initially disclosed how they would use data with voters upon collection. Federal parties would also not be able to sell or transfer data for commercial use if their data was obtained lawfully for campaigning. Voters would have rights over their data, including the right to opt-out of data collection or erase data held by a federal party. When overhauling PIPEDA, the language in the Act could be drafted broadly to apply to new technologies, algorithm standards, and algorithm certification principles. Voter data would be defined as “personal information” under the PIPEDA—a definition integrated with commercial private sectors. With an increased ability to levy fines, the OPC is expected to be able to provide strong regulatory oversight and enforcement.

By aligning PIPEDA with the GDPR data protection principles, the broad collection, use, and disclosure of granular data by federal parties will be somewhat impeded; as a result, this option scores as **somewhat democracy enhancing**. After the GDPR was introduced in the UK, the Labour Party was required to delete a number of email addresses that were collected for data uses for which voters were not informed (K. Dommett, personal communication, March 3, 2022); the Conservative Party was also required to voluntarily delete data on the ethnic backgrounds of 10 million voters that was collected illegally (Gayle, 2021). Overhauling PIPEDA would not give federal parties as much flexibility with granular data, which may lower their ability to effectively reach and engage voters.

9.1.2. Compliance Issues

In addition to the compliance requirements that parties are already obligated to meet, a large amount of rigorous compliance requirements for the collection, use, and disclosure of voter data would have to be introduced. Some indications from the UK,

where political parties are bound to the UK GDPR, suggest federal parties may face difficulties in implementing the processes and procedures necessary to meet data protection compliance requirements (Information Commissioner’s Office, 2020). Constrained by resources, smaller federal parties would likely find it hardest to meet all compliance requirements, and would be particularly punished given the significant fines associated with this option, of between \$10-25 million or 3-5% of their gross global annual revenue. However, the OPC is likely the best positioned regulatory body with the most privacy expertise to assist political parties with clear compliance requirements (C. Bennet, personal communication, March 1, 2022); as a result, this option is given a **moderate resources** score for compliance issues.

9.1.3. Administrative Complexity

Amending PIPEDA would not layer further legislation on top of the existing patchwork of legislation. No infrastructure or large organizational expansion is expected since federal parties would continue to collect data independently and the OPC would be mostly set up to accommodate extending its current regulatory framework to parties. Considering the OPC is an expert in privacy and security issues—and is already responsible for enforcing privacy and security standards for private organizations (under PIPEDA) and the federal government system (under the *Privacy Act*)—publications, guidance, and support can likely be adapted from previous work. Taken together, this option scores **low complexity**.

9.2. Analysis 2: Regulate Data Practices of Parties – CEA

9.2.1. Effectiveness

Option 2 proposes to apply the GDPR principles to federal parties under an amendment to the CEA rather than PIPEDA. In this case, not all but most of the voter privacy guidelines are expected to be met, resulting in **moderate protection**. Similar to option 1, data protections applied to federal parties would be mandatory at all times. Federal parties would also be responsible for acquiring meaningful and unambiguous consent in all their data collection activities, and for securing data with better storage practices. Data sharing would be further constrained depending on how parties initially sought consent to collect data from voters. Federal parties would also not be able to sell

or transfer data for commercial use if their data was obtained lawfully for campaigning. Voters would have rights over their data, including the right to opt-out of data collection or erase data held by a federal party. The language in the CEA could be drafted broadly to apply to new technologies, algorithm standards, and algorithm certification principles. However, as option 2 is enforced by Elections Canada, the definition of “voter data” may be legally considered as a separate category of data (e.g. data used to determine the support of a voter for a party or candidate) compared to PIPEDA’s definition of “personal information” (e.g. data used for advertising); defining “voter data” as legally separate from “personal information” may present a legal grey area if data collected by parties is deployed for commercial purposes rather than campaign modelling (Judge & Pal, 2021). With the ability to levy fines, the CCE is expected to be able to provide regulatory oversight and enforcement. However, since the CCE is not a privacy expert, the strength of oversight and enforcement is assumed to be moderate.

For the same reasons mentioned in option 1, some party officials suggested that additional data protection regulations applied to federal parties would compromise their flexibility to collect, use, and disclose the granular data required to broadly reach and engage voters (K. Boessenkool, personal communication, February 11, 2022; Participant B, personal communication, February 15, 2022). Although this option allows parties to collect, use, and disclose granular data independently, it would likely only be **somewhat democracy enhancing**.

9.2.2. Compliance Issues

In addition to the compliance requirements that parties are already obligated to meet, a number of rigorous compliance requirements would have to be introduced. Similar to option 1, it is likely that federal parties would be unable to meet some of these additional compliance requirements (particularly small parties with constrained budgets). Further, since “Elections Canada does not have specific expertise with privacy,” the CCE may not be able to provide the adequate guidance and clarity to federal parties in order to help them meet compliance requirements, presenting another challenge (Judge & Pal, 2021; C. Bennett, personal communication, March 1, 2022). As a result, this option would likely require **high resources**.

9.2.3. Administrative Complexity

Further legislation would not be layered on top of the existing patchwork of legislation. Similar to the first policy option, no infrastructure is expected to need to be established since political parties will be able to maintain their own data collection and use. However, considering that the CCE is not an expert on privacy and security, some training for the CCE may be required, which would add complexity. Guidance and publications on data protection best practices would likely need to be created from scratch, which may require some organizational expansion. As a result, **moderate complexity** is expected as the CCE transitions to establishing a regulatory approach.

9.3. Analysis 3: Platform Accountability and Voluntary Code of Practice – CEA

9.3.1. Effectiveness

Since option 3 regulates online platforms instead of political parties, very few of the voter privacy guidelines are expected to be met, resulting in **weak protection**. As the strongest option to regulate algorithmic transparency on online platforms and provide the transparency around microtargeting and political advertising, some guidelines would be partially met. However, not all of Judge and Pal's (2021) guidelines for voter privacy reform are expected to be met because a voluntary code of practice would allow federal parties to remain largely unregulated by mandatory data protection regulations. A voluntary code of practice is advantageous to "increase public trust in parties, encourage the parties to coalesce around common practices, remind parties of their duties to the public, support party members with ethical concerns, and to be consistent with other sectors that have implemented codes of ethics" (Judge & Pal, 2021, p. 35). However, since the data practices of parties are not directly constrained by any mandatory obligations, concerns arise over parties having the political will necessary to self-regulate; parties are expected to continue independently campaigning with data as usual despite the voluntary codes of practice. Accordingly, federal parties would likely continue collecting, using, and disclosing voter data in ways previously identified as problematic. For example, federal parties would still be able to infer issue information data while canvassing without always acquiring meaningful and unambiguous consent; or, parties will be able to use an algorithm on the voter list to pick out certain names that they

assume would celebrate certain holidays and then send those identified voters a celebratory card in the mail. Option 3 does not provide the CCE with enforcement power if federal parties are out of compliance with the voluntary code.

Largely informed by interview participants, in part, option 3 was designed to safeguard voter privacy and the integrity of elections by directly regulating platforms rather than federal parties as a way to preserve the role federal parties play in democratic engagement. A voluntary code of practice maintains flexibility for federal parties to collect, use, and disclose granular data broadly to effectively reach and engage voters; as a result, this option scores **democracy enhancing**.

9.3.2. Compliance Issues

Option 3 requires platforms to comply with regulations and algorithmic standards. However, with no mandatory data protection legislation applied to federal parties, there would be no additional compliance requirements. Therefore, this option scores **low additional resources**.

9.3.3. Administrative Complexity

Although this option would not layer on top of the existing patchwork of legislation, establishing algorithm standards and a certification framework for platforms is expected to be **moderately complex**, possibly requiring Elections Canada to hire additional staff and create guidance documentation from scratch. Further, the CCE may have to receive some training to gain some expertise in privacy and security.

9.4. Analysis 4: Elections Canada Database – New Law

9.4.1. Effectiveness

Restricting federal parties from collecting and storing their own granular data would make Elections Canada responsible for some voter privacy guidelines, removing the burden from federal parties. Elections Canada would be responsible for ensuring the database is secure and gaining informed consent upon data collection to provide federal parties with data points. Voters would be given rights over the data held by Elections

Canada, with the ability to opt-out at anytime. The restrictions on political parties would be mandatory at all times. The data held by Elections Canada would only be permitted for political use purposes. Issues from data sharing between parties or within parties would be mitigated by all federal parties having access to the same data and by Elections Canada restricting access to registered federal parties. However, this option does not apply much regulatory oversight to how federal parties use voter data once accessed from the Elections Canada database. As a result, federal parties are expected to continue using algorithmic learning and profiling as a way of identifying support and persuasion with no standards or certification obligations. With the ability to levy fines, the CCE is expected to be able to provide enforcement, but the strength of enforcement is assumed to be moderate since the CCE is not a privacy expert and will be constrained by managing the database. Taken together, this option offers **moderate protection**.

Further, a separate piece of legislation that prevents federal parties from having the flexibility to independently and broadly collect granular data is likely to impede democratic engagement—particularly since the level of granularity of data that Elections Canada would be able to collect is unclear. Elections Canada would have to establish a team to manage the database, instead of outsourcing data entry to volunteers like federal parties currently do, which would require significant resources. It is unlikely Elections Canada would have sufficient resources (time and capital) to work with data brokers, and they would likely only be able to pull in a limited amount of voter data from other government departments (such as Statistics Canada). It is also unclear if Elections Canada would be able to capture up-to-date issue information (or, how voters feel about certain political issues), which is data that federal parties rely on in order to connect voters to Canadian politics. As a result, this option scores **not democracy enhancing**.

9.4.2. Compliance Issues

Federal parties would be restricted from collecting and storing their own data. As a result, the burden of meeting compliance requirements for the collection of voter data would be mostly removed from political parties and transferred to Elections Canada. To ensure Elections Canada's database is secure and that data collection meets regulatory standards, as a clearinghouse for voter data, the overall operations of Elections Canada may be somewhat impacted. Federal parties would still have to meet some compliance requirements for the use of voter data. For example, federal parties would have to

register affiliates to access the Elections Canada voter database and would have to justify lawful reasons for using the data. However, since federal parties would not have to meet many additional compliance requirements, they are expected to need **low additional resources**.

9.4.3. Administrative Complexity

Introducing a new piece of legislation would layer it on top of the existing patchwork of legislation, inherently creating more complexity to the regulatory environment for federal parties. Designating Elections Canada as a clearinghouse for voter data would add further complexity. Elections Canada would likely have to set up new infrastructure, into which it would need to integrate the current National Register of Electors. Elections Canada would also likely need to hire a team of staff to maintain the database throughout the year. Although Elections Canada is a parliamentary agency, some coordination may be required between federal government departments to collect voter data (e.g. with Statistics Canada). Further, the CCE may have to receive some training to gain some expertise in privacy and security. Data protection guidance and publications would likely need to be created from scratch. Overall, this option would have **high complexity**.

Chapter 10.

Recommendation

The analysis in Chapter 9 and summary in Table 9.1 demonstrate that there are trade-offs between all the options presented. Option 2 is similar to Option 1 but is not considered beneficial over others because of Elections Canada’s limited expertise as a privacy regulator. Option 3 would be the most effective at providing transparency around microtargeting, platform algorithms, and political advertising, but would only effectively regulate federal parties in line with the status quo. Option 4 would be the most effective at leveling the playing field and providing moderate data protection without burdening parties with hefty compliance requirements. This option could be analyzed in further work as many option variations that propose less severe levels of data collection, independent of a centralized Elections Canada database. However, considering how option 4 was designed for this research, it would be very administratively complex and would strongly restrict what kinds of granular data parties could use to engage the electorate.

Consequently, with the highest score, it is recommended that option 1—to overhaul PIPEDA and extend data protection legislation to federal parties with the use of a code of practice—be adopted. Many interview participants suggested that the OPC was best positioned to regulate the collection, use, and disclosure of voter data by federal parties. If the GDPR data protection principles are applied in Canada, the voter privacy guidelines advanced by Judge and Pal (2021) are best met, particularly if applied under the purview of the OPC rather than the CCE. In Judge and Pal’s (2021) analysis of regulated federal parties under PIPEDA or the CEA, the CEA was recommended because PIPEDA was only analyzed as it is currently enacted. Although C-11 was introduced in the House of Commons in November 2020 to significantly overhaul PIPEDA, interview participants expressed that it does not go far enough to adequately safeguard voter privacy or to uphold the democratic integrity of the campaign process in Canada. Another proposal to amend PIPEDA is expected to be introduced following the 2021 election, and a directive to “introduce legislation to advance the Digital Charter” remains on the Minister of Innovation, Science, and Industry’s mandate letter (Office of the Prime Minister, 2021). Either the Liberals would have to draft the next version of C-

11 with the exemption for political parties removed or the NDP or Conservatives would have to lobby for the exemption to be removed—with the draft subsequently amended—before the House of Commons votes to pass it. However, with concerns over political will, removing the exemption for federal parties seems unlikely at this point (see Chapter 12 for the political feasibility of implementing option 1 moving forward).

Chapter 11.

Limitations

Over the course of this research, several limitations were identified that could not be addressed given the scope of the research and the nature of the regulatory gap. First, many VRM databases have grown to become attractive targets for hacking—sometimes from foreign state actors—which poses a real threat to Canadian security (Richardson, Witzleb, & Paterson, 2019). Nor did the scope of this research explicitly cover data storage considerations, which are also relevant and should be considered alongside recommendations on the collection, use, and disclosure of voter data. Third, although all major federal parties were approached by the researcher, only party officials from the Conservatives agreed to participate, leaving perspectives from other major federal parties out of data collection. Fourth, with a lack of transparency around the actual data collection, use, and disclosure practices of federal parties, the research was limited to report what practices were “known”—established by the literature or offered by party campaign officials. Participant D also suggested that presenting an analysis that covered algorithm standards and certifications would make this research current (personal communication, March 17, 2022); however, no literature has been published that examines the use of algorithms by federal parties in depth and no interview participant was forthcoming with information about their party’s use of algorithms. Since technologies develop quickly, it is likely federal parties are using strategies not covered by research to date.

Chapter 12.

Moving Forward: Political Feasibility

Political feasibility is a criterion not considered in the analysis presented in Chapter 8 because there is concern about the political will required to adopt *any* policy option. From a political perspective, Participant C suggested directly regulating parties under the CEA may be a viable option as long as their collection, use, and disclosure of voter data was treated as distinct from catch-all privacy legislation that regulates private organizations (personal communication, February 23, 2022). Broadly, many interview participants suggested further regulation would be difficult.

However, recent developments suggest the issue may be gaining legislative attention. Over the last couple of years, the Centre for Digital Rights has filed several privacy-related legal complaints on behalf of individual complainants with five regulators: the Competition Bureau of Canada, Canadian Radio-television and Telecommunications Commission (CRTC), Office of the Privacy Commissioner of Canada (OPC), Elections Canada, and Office of the Information and Privacy Commissioner for BC (OIPC). The Competition Bureau of Canada, CRTC, OPC, and Elections Canada have since closed their investigations, stating they lack the jurisdiction over federal parties needed to investigate. However, on March 1, Queen’s Council lawyer, David Loukidelis issued an order for the OIPC, stating the collection, use, and disclosure of voter data by federal parties is constitutionally subject to BC PIPA.¹⁹ This order is the first time any regulator has claimed jurisdiction over federal parties. Immediately, federal parties will have an opportunity to apply for judicial review; however, assuming parties do not apply or after a review period ends (assuming the order was granted lawfully), it is expected that Commissioner McEvoy will commence an investigation and federal parties will be required to show regulators how they collect, use, and disclose voter data for the first time (B. Hearn, personal communication, February 15, 2022). Although federal parties would only be regulated by privacy law in the province of British Columbia, there will likely be an extraterritoriality effect to other provinces—some of which were already taking steps to apply data protection regulation to provincial parties before Loukidelis’

¹⁹ BC PIPA is constitutional provincial privacy law, written broadly to state all “political parties” are covered by the OIPC’s authority.

order (e.g. Quebec) (Participant D, personal communication, February 17, 2022). Depending on the OIPC's investigation, a political shift or legal direction may be forthcoming.

References

- Anstead, N. (2017). Data-driven campaigning in the 2015 United Kingdom General Election. *The International Journal of Press/Politics*, 22(3), 294–313.
- Attorney-General's Department. (2021). Online Privacy Bill exposure draft. *Australian Government*. <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>
- Attorney-General's Department. (2022). Privacy Act review – discussion paper. *Australian Government*. <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/>
- Australian Law Reform Commission. (2008). *For your information: Australia privacy law and practice report*. https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol1.pdf
- Bailenson, J. N., Ivengar, S., Yee, N., & Collins, N. A. (2008). Facial similarity between voters and candidates causes influence. *Public Opinion Quarterly*, 72(5), 935–961.
- Baldwin-Philippi, J. (2017). The myths of data-driven campaigning. *Political Communication*, 34(4), 627-633.
- Bennett, C. J. (2012). Canadian federal political parties and personal privacy protection: A comparative analysis. *Office of the Privacy Commissioner of Canada*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/#toc2b
- Bennett, C. J. (2015). Trends in voter surveillance in Western societies: Privacy intrusions and democratic implications. *Surveillance and Society*, 13(3/4), 370-384.
- Bennett, C. J. (2016). Voter databases, micro-targeting, and data protection law: Can political parties campaign in Europe as they do in North America? *International Data Privacy Law*, 6(4), 261-275.
- Bennett, C. J. & Bayley, R. M. (2018). *The influence industry data analytics in Canadian elections*. Tactical Tech. <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-canada.pdf>
- Bennett, C. J., & Gordon, J. (2021). Understanding the 'micro' in political micro-targeting: An analysis of Facebook Digital Advertising in the 2019 Federal Canadian Election. *Canadian Journal of Communication*, 46(3), 431–459.
- Bennett, C. J., & Lyon, D. (2019). Data-driven elections: Implications and challenges for democratic societies. *Internet Policy Review*, 8(4). <https://policyreview.info/data-driven-elections>

- Brennan Centre for Justice. (n.d.). HAVA fact sheet. *NYU School of Law*.
<https://www.brennancenter.org/sites/default/files/legacy/d/HAVA%20Fact%20Sheet.pdf>
- Boutille, A. (2020, Jan 15). Liberals, Conservatives and NDP face competition bureau investigation into how they use Canadians' personal data. *Toronto Star*.
<https://www.thestar.com/politics/federal/2020/01/15/federal-parties-face-competition-probe-over-collection-of-canadians-personal-data.html>
- Campaign Research. (2019). National data privacy study. *Centre for Digital Rights*.
<https://centrefordigitalrights.org/files/document/2020-01-11/156-102825.pdf>
- Cohen, T. (2021). The political exemption: A justifiable invasion of privacy in the political sphere? *UNSW Law Journal*, 44(2), 584-612.
<https://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2021/06/Issue-442-PDF-5-Cohen.pdf>
- Concordia. (2016). *The power of big data and psychographics | 2016 Concordia Annual Summit*. [video]. YouTube. <https://www.youtube.com/watch?v=n8Dd5aVXLcc>
- Culliford, E. (2020). How political campaigns use your data. *Reuters*.
<https://graphics.reuters.com/USA-ELECTION/DATA-VISUAL/yxmvjijgoivr/>
- Dataethics. (2019). Danish companies behind seal for digital responsibility. *Dataethics*.
<https://dataethics.eu/danish-companies-behind-seal-for-digital-responsibility/>
- Delacourt, S. (2021, Sept 23). Liberals used an old trick to turn the election around in the campaign's final days: They knocked on doors. *Toronto Star*. Retrieved from:
<https://www.thestar.com/politics/political-opinion/2021/09/23/liberals-used-an-old-trick-to-turn-the-election-around-in-the-campaigns-final-days-they-knocked-on-doors.html>
- Deley, T. & Szwarc, J. (2018). Block the parties from predicting voters' private traits. *Policy Options*. <https://policyoptions.irpp.org/magazines/june-2018/block-the-parties-from-predicting-voters-private-traits/>
- Dubois, E., & McKelvey, F. (2019). Political bots: Disrupting Canada's democracy. *Canadian Journal of Communication Policy Portal*, 44(2), 27-33.
- Elections Canada. (2020). Turnout and reasons for not voting: October 21, 2019, federal election: Results from the Labour Force Survey supplement. *Elections Canada*.
<https://www.elections.ca/content.aspx?section=res&dir=rec/eval/pes2019/lfs&document=index&lang=e>
- Electoral Commission. (2021). *Report: Digital campaigning: Increasing transparency for voters*. <https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/report-digital-campaigning-increasing-transparency-voters>

- Electoral Matters Committee. (2021). Inquiry into the impact of social media on Victorian elections and Victoria's electoral administration. *Parliament of Victoria*. <https://apo.org.au/sites/default/files/resource-files/2021-09/apo-nid314042.pdf>
- Elections Modernization Act, S.C. 2018, c. 3 (2022). https://laws-lois.justice.gc.ca/eng/annualstatutes/2018_31/page-1.html
- Esselment, A. (2017). Canada's embrace of the permanent campaign. *Policy Options*. <https://policyoptions.irpp.org/fr/magazines/july-2017/canadas-embrace-of-the-permanent-campaign/>
- European Commission. (2018). *Protecting Europeans' personal data in elections*. European Commission. https://ec.europa.eu/info/sites/default/files/soteu2018-factsheet-personal-data-elections_en.pdf?fbclid=IwAR1xKOvoJPcDZBBt8rUSShICcMp-gpvwSzKm9ovGaS6dDDoW_sRZKw_X5Vw#page30
- European Commission. (2020). *On artificial intelligence: A European approach to excellence and trust*. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
- European Commission. (2022). What personal data is considered sensitive? *European Commission*. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- Falguera, E., Jones, S., Ohman, M. (2014). *Funding of political parties and election campaigns: A handbook on political finance*. International IDEA. <https://www.idea.int/sites/default/files/publications/funding-of-political-parties-and-election-campaigns.pdf>
- Fazlioglu, M. (2019). Tracking the politics of US privacy legislation. *International Association of Privacy Professionals*. <https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/>
- Feasby, C. (2010). Contemporary issues in Canadian Political finance regulation. *Policy Quarterly*, 6(3), 14-20. <https://www.yumpu.com/en/document/read/51011306/contemporary-issues-in-canadian-political-institute-for-governance->
- Gayle, D. (2021, Jan 26). Tory party illegally collected data on ethnicity of 10m voters, MPs told. *The Guardian*. <https://www.theguardian.com/technology/2021/jan/26/conservative-party-illegally-collected-data-on-ethnicity-of-10m-voters-mps-told>
- GDPRhub. (2022). Article 9 GDPR. *GDPRhub*. Retrieved from: https://gdprhub.eu/Article_9_GDPR#Political_opinions
- Gerald Butts. [gmbutts]. (2021, Sept 21). Vote efficiency isn't accidental. All three Trudeau Liberal campaigns were among the most efficient in CA history. The unsung team of super geniuses put together and led by @tompitfield at Data

- Sciences deserves a lot more credit than they've ever received. #Elxn44 (43 and 42) [Tweet]. <https://twitter.com/gmbutts/status/1440347519284760580>
- Government of Canada. (2019). Rules for unsolicited telecommunications made on behalf of political entities. *Canadian Radio-television and Telecommunications Commission*. <https://crtc.gc.ca/eng/phone/telemarketing/politi.htm>
- Government of Canada. (2020). "Frequently asked questions about Canada's Anti-Spam Legislation." *Canadian Radio-television and Telecommunications Commission*. <https://crtc.gc.ca/eng/com500/faq500.htm>
- Government of the United Kingdom. (2022). Data protection. *GOV.UK*. Retrieved from: <https://www.gov.uk/data-protection>
- Green, J. & Issenberg, S. (2016). Inside the Trump bunker, with days to go. *Bloomberg*. <https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go>
- Green Party of Canada. (2022). "Privacy Policy." *Green Party of Canada*. <https://www.greenparty.ca/en/privacy>
- Gryz, J., & Rojszczak, M. (2021). Black box algorithms and the rights of individuals: No easy solution to the "explainability" problem. *Internet Policy Review*, 10(2). <https://policyreview.info/articles/analysis/black-box-algorithms-and-rights-individuals-no-easy-solution-explainability>
- Hankey, S., Morrison, J. K., Naik, R. (2018). *Data and democracy in the digital Age*. The Constitution Society. <https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf>
- Heath-Rawlings, J. (Host). (2021, Nov 22). Political parties are getting ruthlessly efficient at finding votes. Is it bad for democracy? (N. 418) [Audio podcast episode]. In *The Big Story*. Frequency Podcast Network. <https://thebigstorypodcast.ca/2021/11/22/political-parties-are-getting-ruthlessly-efficient-at-finding-votes-is-it-bad-for-democracy/>
- House of Commons. (2021). *Member's allowances and services*. <https://www.ourcommons.ca/Content/MAS/mas-e.pdf>
- Information Commissioner's Office. (2018). *Investigation into the use of data analytics in political campaigns*. <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>
- Information Commissioner's Office. (2020). *Audits of Data Protection Compliance by UK Political Parties*. <https://ico.org.uk/media/action-weve-taken/2618567/audits-of-data-protection-compliance-by-uk-political-parties-summary-report.pdf>
- Information Commissioner's Office. (2022). Guidance for the use of personal data in political campaigning. *Information Commissioner's Office*. <https://ico.org.uk/for->

[organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/](https://www.idea.int/data-tools/data/voter-turnout)

- International IDEA. (2022). Voter turnout database. *International IDEA*.
<https://www.idea.int/data-tools/data/voter-turnout>
- Judge, E. & Pal, M. (n.d.). *Privacy and the electorate: Big data and the personalization of politics*. University of Ottawa Centre for Law Technology and Society.
https://techlaw.uottawa.ca/sites/techlaw.uottawa.ca/files/judge_pal_privacyandthe_electorate_ksg_report_oct_14_final.pdf
- Judge, E. & Pal, M. (2019). Election cyber security challenges for Canada. *Center for International Governance and Innovation*.
<https://www.cigionline.org/articles/election-cyber-security-challenges-canada/#footnote1><https://www.cigionline.org/articles/election-cyber-security-challenges-canada/#footnote1>
- Judge, E. & Pal, M. (2021). Voter privacy and big data elections. *Osgoode Hall Law Journal*.
<https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=3631&context=ohlj>
- Kaye, K. (2022). How to kill an algorithm. *Protocol*.
<https://www.protocol.com/newsletters/protocol-enterprise/ftc-algorithmic-disgorgement-japan-chips?rebelltitem=1#rebelltitem1>
- Kaye, B. & Paul, K. (2019). After data scandals, Australia faces an election under heavy profiling. *Reuters*. <https://www.reuters.com/article/uk-australia-election-data/after-data-scandals-australia-faces-an-election-under-heavy-profiling-idUKKCN1SB016?edition-redirect=uk>
- Kefford, G. (2021). *Political parties and campaigning in Australia: Data, digital and field*. Springer International Publishing AG.
- Keller, T. R., & Klinger, U. (2019). Social bots in election campaigns: Theoretical, empirical, and methodological implications. *Political Communication*, 36(1), 171-189.
- Krotoszynski Jr, R. J. (2019). Big data and the electoral process in the United States: Constitutional constraint and limited data privacy regulations. In N. Witzleb, M. Paterson, & Richardson, J (Eds.), *Big data, political campaigning, and the law: Democracy and privacy in the age of micro-targeting* (pp. 182-207). Taylor & Francis Group.
- Lees-Marshment, J. (2012). *Routledge handbook of political marketing*. Taylor and Francis 2012.
- Macintyre, A., Wright, G., & Hankey., S. (2018). Data and democracy in the UK. *Tactical Tech*. <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-uk.pdf>

- Maher, S. (2022, Jan 2). The ruthless math of political campaigns: Is big data bad for democracy? *The Walrus*. <https://thewalrus.ca/vote-efficiency-federal-elections/>
- Matwankar, S. H., & Shinde, S. K. (2016). Case study: Political profiling based on Twitter sentiment analysis for big data using data mining algorithms. *International Journal of Engineering Research & Technology*, 5(2), 225-228.
- Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*, 114(48), 12714–12719.
- McDonagh, M. (2019). Freedom of processing of personal data for the purpose of electoral activities after the GDPR. In N. Witzleb, M. Paterson, & Richardson, J (Eds.), *Big data, political campaigning, and the law: Democracy and privacy in the age of micro-targeting* (pp. 115-138). Taylor & Francis Group.
- McEvoy, M. (2019). *Full disclosure: Political parties, campaign data, and voter consent*. Office of the Information and Privacy Commissioner for British Columbia. <https://www.oipc.bc.ca/investigation-reports/2278>
- MIT Election Data and Science Lab. (2022). Voter registration. *Massachusetts Institute of Technology*. <https://electionlab.mit.edu/research/voter-registration>
- National Conference of State Legislators. (2022). Access to and use of registration lists. *National Conference of State Legislators*. <https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx>
- New Democratic Party of Canada. (2022). Privacy policy. *New Democratic Party of Canada*. <https://www.ndp.ca/privacy>
- Office of the Information Commissioner. (2022). Political parties and elections. *Australian Government*. <https://www.oaic.gov.au/privacy/your-privacy-rights/political-parties-and-elections>
- Office of the Information and Privacy Commissioner for British Columbia. (2015). *A guide to BC's Personal Information Protection Act for businesses and organizations*. <https://www.oipc.bc.ca/guidance-documents/1438>
- Office of the Privacy Commissioner of Canada. (2021). OPC responds to privacy complaint against three federal political parties. *Office of the Privacy Commissioner*. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_210513/
- Paterson, M. & Witzleb, N. (2019). Voter privacy in an era of big data: Time to abolish the political exemption in the Australian Privacy Act. In N. Witzleb, M. Paterson, & Richardson, J (Eds.), *Big data, political campaigning, and the law: Democracy and privacy in the age of micro-targeting* (pp. 162-181). Taylor & Francis Group.
- Ralston, N. (2013, Aug 11). Tony Abbott's Twitter followers drops after fake buyers culled. *The Sydney Morning Herald*.

<https://www.smh.com.au/politics/federal/tony-abbotts-twitter-followers-drops-after-fake-buyers-culled-20130811-2rpt2.html>

- Reid, D. (1988). Marketing the political product. *European Journal of Marketing*, 22(9), 34-47.
- Richardson, J., Witzleb, N, & Paterson, M. (2019). Political micro-targeting in an era of big data analytics: An overview of the regulatory issue. In N. Witzleb, M. Paterson, & Richardson, J (Eds.), *Big data, political campaigning, and the law: Democracy and privacy in the age of micro-targeting* (pp. 11-25). Taylor & Francis Group.
- Rubinstein, I. (2018). Voter privacy in the age of big data. *2014 Wisconsin Law Review* 861, 861-936. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447956
- Scott, M. (2020). UK political parties accused of misusing data privacy rules. *Politico*. <https://www.politico.eu/article/labour-conservatives-liberal-democrats-data/>
- Stacey, G., R., Kearney, E., K., Manji-Knight, A., and Stevenson, T. (2020). New privacy law for Canada: Government tables the *Digital Charter Implementation Act, 2020*. *Davies, Ward, Phillips & Vineberg LLP*. <https://www.dwpv.com/en/Insights/Publications/2020/Government-Tables-New-Privacy-Law>
- Sweeney, L. & Doran, M. (2019, Jan 16). Clive Palmer's party uses unsolicited political text messages to announce ban on unsolicited political texts. *ABC News Australia*. <https://www.abc.net.au/news/2019-01-17/clive-palmers-party-uses-unsolicited-political-text-message/10720948>
- The Canadian Press. (2018, Jan 30). Report says reviving political subsidies costs \$44M per year, Liberals shut door. *CTV News*. <https://www.ctvnews.ca/politics/report-says-reviving-political-subsidies-costs-44m-per-year-liberals-shut-door-1.3781846>
- Trudeau, J. (2021). Minister of Innovation, Science, and Industry mandate letter. *Office of the Prime Minister*. <https://pm.gc.ca/en/mandate-letters/2021/12/16/minister-innovation-science-and-industry-mandate-letter>
- Turcotte, A. (2021). *Political marketing alchemy: The state of opinion research*. Springer International Publishing AG.
- Wolford, B. (2020). What is GDPR, the EU's new data protection law? *GDPR.EU*. <https://gdpr.eu/what-is-gdpr/>
- Yaffe, M. (2019). Political parties warned about using personal data in the election campaign by the ICO. *JMW*. <https://www.jmw.co.uk/services-for-business/commercial-litigation-dispute-resolution/blog/political-parties-warned-about-using-personal-data-election-campaign-ico>

Appendix A. Interview Participants

Table A.1. List of Interview Participants

Interview Participant	Interview Date
Academics	
Yannick Dufresne	February 23, 2022
Colin Bennett	March 1, 2022
Fenwick McKelvey	March 1, 2022
Kate Dommett	March 3, 2022
Academic Participant	March 16, 2022
Conservative Campaign Officials	
Ken Boessenkool	February 11, 2022
Conservative Source	February 15, 2022
Conservative Source	February 23, 2022
Lawyers	
Bill Hearn	March 15, 2022
Advocacy Groups	
Data Protection Advocate	March 17, 2022

Appendix B. Sample Interview Questions

1. From how you understand it, what are the key elements of a data-driven campaign?
 - a. To your knowledge, how do federal political parties use voter data during the campaign cycle?
 - b. To your knowledge, where do political parties get or collect voter data from?
2. Do you think that all federal parties have the opportunity to use data pretty much the same way over the campaign cycle?
3. To your knowledge, how is data shared between federal and provincial levels of parties?
4. Do you think that Canadian political parties use voter data differently than federal political parties in other countries?
5. Do you think the collection and use of voter data by federal political parties in Canada is a voter privacy issue or an issue of voter autonomy/voter manipulation?
6. From your perspective, what do you think might be compromised if federal political parties were further regulated on how they are able to collect and use voter data?
 - a. From your perspective, what benefits do you think there are in further regulating how federal political parties collect, use, and store voter data?
7. If any, what policy options do you recommend to safeguard voter data?
8. What principles do you think should guide evaluating different policy options?
9. Do you think there is a current policy window for new safeguards to be adopted?




Appendix C. Sample of Data Collected by Political Parties

Table C.1. Voter Data Collected by Political Parties in BC (McEvoy, 2019)

Collected Personal Information			
Information Related to Identity			
Surname	Given name(s)	Date of birth	Residential address
Mailing address	Email address	Phone number	
Other Information About the Individual			
Sex	Ethnicity	Age	Language(s)
Religion	Income	Education	Familial relations
Family or marital status	Profession	Workplace name	Job title
Profession status (e.g. practicing or non-practicing)	Number of years at residential address	Neighbourhood demographics	Issues of interest to the individual
Political support tier/score	Ease of persuasion tier/score	Do not call or Do not contact notices	LinkedIn ID
Twitter ID	Facebook ID	Skype ID	
Party Participation Data			
Party membership status	Type of membership	Prospective number	Volunteer status
Volunteer availability	Interest in a lawn sign	Donor status (monthly, one time)	Donation amount
Date of donation	Previous election support levels	If the individual subscribes to communications	What communications were sent and when
Internal working group membership			
Financial Information			
Personal cheque or credit card number	Name as shown on credit card	Card expiry	Signature
Election BC Data (Voter List/Voter Participation Data)			
Electoral district	Electoral district code	Voting area code	Previous or current election voter number
Voting card number	Federal riding	Party's share of votes in an individual riding	Voting location
Municipal district	If the individual has voted in the current election	If/when the individual voted in the last election (advanced v. general voting day)	

Appendix D. Example of VRM Database Scale that Measures Levels of Voter Support

Figure D.1. Scale Used to Score Level of Voter Support in CIMS VRM Database (Bennett & Bayley, 2018)

-15 to -5	-4 to -1	0	1 to 4	5 to 15
				
Non Supporter	Accessible Somewhat	Undecided	Accessible Likely	Supporter