



RESEARCH ARTICLE/ÉTUDE ORIGINALE

Privacy and Canadian Political Parties: The Effects of the Data-Driven Campaign on Elector Engagement

Sara Bannerman^{1*} , Julia Kalinina¹, Elizabeth Dubois² and Nicole Goodman³ 

¹Department of Communication Studies & Media Arts, TSH 302, McMaster University, 1280 Main St. W., Hamilton, ON L8S 4L8, Canada, ²Department of Communication, University of Ottawa, Desmarais Building, 11th Floor, DMS 11-156, 55 Laurier Avenue E., Ottawa, ON K1N 6N5, Canada and ³Department of Political Science, Brock University, 1812 Sir Isaac Brock Way, Plaza 325, St. Catharines, ON L2S 3A1, Canada

*Corresponding author. E-mail: banners@mcmaster.ca

Abstract

This article reports the results of a survey examining Canadians' attitudes about political parties' collection of personal information. Datafied campaigning brings concerns about surveillance, divisiveness, digital redlining and elector autonomy. This article asks whether awareness of parties' data collection practices affects willingness to engage with campaigns. We find (1) that respondents are not fully aware of political parties' data collection practices, (2) that awareness of parties' collection of personal information may reduce electors' willingness to interact with political parties online, (3) that those who are more aware of these practices report higher levels of concern about them and that those who do not think that parties' collection of personal information is important to the democratic process also report higher levels of concern, and (4) that new legal measures to regulate how political parties collect and use personal information are supported by respondents.

Résumé

Cet article présente les résultats d'une enquête sur les attitudes des Canadiens à l'égard de la collecte de renseignements personnels par les partis politiques. La datafication des campagnes politiques suscite des inquiétudes concernant la surveillance, les dissensions, le *redlining* numérique et l'autonomie des électeurs. Cet article cherche à savoir si la connaissance des pratiques de collecte de données des partis a une incidence sur la volonté de participer aux campagnes. Nous constatons que 1) les répondants ne sont pas pleinement conscients des pratiques des partis politiques en matière de collecte de données ; 2) la conscience de la collecte de renseignements personnels par les partis peut réduire la volonté des électeurs d'interagir avec les partis politiques en ligne ; 3) ceux qui sont plus conscients

de ces pratiques signalent des niveaux plus élevés d'inquiétude à leur sujet ; ceux qui ne pensent pas que la collecte de renseignements personnels par les partis est importante pour le processus démocratique signalent également des niveaux plus élevés de préoccupation ; et 4) les répondants sont favorables à de nouvelles mesures juridiques visant à réglementer la façon dont les partis politiques recueillent et utilisent les renseignements personnels.

Keywords: privacy; political parties; political engagement; elections

Mots-clés : vie privée; partis politiques; engagement politique; élections

Introduction

In March 2018, the *Guardian* and the *New York Times* revealed that a private company, Cambridge Analytica, had obtained the personal data of more than 87 million Facebook users and was using this data to provide political campaign services around the world. Personal information had been harvested and used to profile and infer personal details about tens of millions of Facebook users. This data was then used to send Facebook users targeted political messages in attempts to influence voting behaviour. These revelations were shocking due to the scale and detail of the personal data involved and the political uses to which it had apparently been put.

While the Cambridge Analytica revelations brought the potential political uses of personal information into the public eye, scholars had been researching and reflecting on these practices for years. Colin Bennett has focused on Canadian political parties' collection of personal information since at least 2012; Philippe Dubois, Thierry Giasson, Alex Marland, Eric Montigny, Steve Patten and Tamara Small have examined the use of data and social media in election campaigning in Canada since around 2017; and Ryan Calo, Kate Dommett, Philip Howard, Daniel Kreiss and Samuel Woolley have published studies of data-driven campaigns, bots and uses of technology in political communication internationally.

The Cambridge Analytica revelations led many to delete their Facebook accounts. In this article, we ask whether collection of personal information by political parties might lead electors to disengage not from social media platforms but from communications with political parties and their campaigns.

Western countries' regulation of political parties' collection and use of electors' personal information lie on a spectrum. At one end is the United States, where political parties are, as in Canada, not bound by privacy laws and where elections are more "data-driven" than anywhere else in the world (Bennett and Oduro-Marfo, 2019; Bennett and Bayley, 2012: 10). At the other end are the United Kingdom and most European countries, where privacy laws do apply to political parties. Canada and Australia fall somewhere in the middle (Bennett and Oduro-Marfo, 2019; Bennett and Bayley, 2012: 9). In Canada, only British Columbia and Quebec have, to date, enacted privacy legislation that applies to political parties (see Judge and Pal, 2021).

Building on our past work (Bannerman *et al.*, 2019), we conducted a survey examining Canadians' attitudes about political parties' collection of personal

information. Although online participation by electors and political parties raises opportunities for democratic engagement, datified campaigning also brings concerns about surveillance, divisiveness, digital redlining and elector autonomy. Our article asks whether awareness of parties' data collection practices affects willingness to engage with campaigns.

We set up this question by outlining what is known about parties' data collection practices in Canada and internationally. Next, we review the literature on political parties' collection of personal information and its effects on electors' willingness to engage with campaigns. Then we detail our methods and present our analysis. In our analysis, we first further set up our question on the effects of awareness on engagement by asking how aware respondents are about federal political parties collecting and retaining their personal information. We followed the question of whether awareness of parties' data collection practices affects willingness to engage with campaigns by examining electors' specific concerns with political parties collecting and storing personal information, the characteristics that correlate with high levels of concern over political parties' information collection practices, and attitudes about the applicability of privacy law and consent requirements to political parties.

We find (1) that respondents are not fully aware of political parties' data collection practices, (2) that awareness of parties' collection of personal information may reduce electors' willingness to interact with political parties online, (3) that those who are more aware of these practices report higher levels of concern about them and that those who do not think that parties' collection of personal information is important to the democratic process also report higher levels of concern, and (4) that new legal measures to regulate how political parties collect and use personal information are supported by respondents. We think that the application of privacy law to political parties is warranted in order to protect electors' trust in the democratic process in Canada.

Current Regulation of Canadian Political Parties' Access to Electors' Personal Information

Several laws constrain Canadian political parties' collection and use of personal information, including laws regarding telemarketing, the Canada Elections Act (S.C. 2000, c. 9; see also Judge and Pal, 2021) and federal commercial privacy laws that apply in a limited way to political parties to the extent that they engage in commercial activity, such as merchandise sales (Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5). The Elections Modernization Act (S.C. 2018, c. 31) now requires federal political parties to maintain and publish privacy policies online. The Canada Elections Act requires Elections Canada to maintain a register of electors (S.C. 2000, c. 9, s. 44(2)). The register is used to produce lists of electors during elections. These lists, containing electors' names, addresses and a unique identifier, are sent annually to all members of Parliament and, on request, to registered political parties (Canada Elections Act, S.C. 2000, c. 9, s. 45).

In British Columbia, where the Personal Information Protection Act (S.B.C. 2003, c. 63) came into force in 2004, provincial privacy laws apply to political parties' noncommercial uses of personal information. Following the Cambridge

Analytica scandal, British Columbia's information and privacy commissioner investigated the ways that British Columbian political parties collect and use electors' personal information. The commissioner found that "political parties are generally collecting too much information about potential electors, without getting proper consent" (McEvoy, 2019: 4). He found that canvassers collect personal information such as electors' ethnicity, age, profession, Facebook ID, family status, and other information and that canvassers make observations from the doorstep about electors and record them in parties' databases (McEvoy, 2019: 12). With respect to this last practice, the commissioner noted that "it is highly debatable that most individuals would agree to [this] if they were told." He also said it was "highly unlikely . . . that voters are consenting" to the collection of gender, ethnicity and religion (McEvoy, 2019: 16) and expressed doubt about the accuracy of information collected in this way. In 2021, Quebec passed Bill 64 (2021, chapter 25), which applies privacy laws in limited ways to political parties.

At the federal level, political parties have developed privacy policies (as required under the Elections Modernization Act), albeit policies vary considerably (Office of the Privacy Commissioner of Canada, 2019). The Office of the Privacy Commissioner of Canada (2019) found that all major federal parties had failed to provide sufficient evidence that the consent obtained by parties to collect and use personal information was valid and informed. Most parties collect publicly available information, including social media names and contacts. Although each of the parties' policies has provisions for individuals to update or correct personal information, it is unclear how an individual would do this, since no party mentions how—or if—individuals can access their information upon request (Office of the Privacy Commissioner of Canada, 2019; Howard and Kreiss, 2009: 19).

Data-driven campaigns in Canada

Parties vary in the extent to which they use data-driven campaigning, but all major parties in Canada maintain large campaign databases in which they combine Elections Canada information with other sources, including voter contact data, and use it for direct mailing and strategy formation, especially in marginal seats (Bennett and McDonald, 2019; Bennett and Oduro-Marfo, 2019; Bennett and Bayley, 2012: 16; Howard and Kreiss, 2009: 17–19; McEvoy, 2019: 14; Munroe and Munroe, 2018; Judge and Pal, 2021). Each main political party in Canada has developed its own customized database, used to generate call sheets and walk sheets for canvassers, often filtering such sheets strategically to target supporters (Munroe and Munroe, 2018; Judge and Pal, 2021; Patten, 2017). Data can be used to target traditional or online advertisements, decide where and who to canvass, track what issue is important to whom, set targets, measure success, quantify individual campaigners' performance, and make inferences and predictions about electors (for example, data on individuals' personality traits could be used to infer political ideology [Bergeron and Galipeau, 2021]). The extent to which these features are used varies by party and by campaign (Munroe and Munroe, 2018; Montigny *et al.*, 2019; Giasson *et al.*, 2019; McKelvey and Piebiak, 2019).

Because there is no authority to audit or investigate the databases, evidence on what is included in them tends to be anecdotal and speculative (Bennett and

Bayley, 2012: 16; Howard and Kreiss, 2009; Information Commissioner's Office, 2018a). We know that parties use the poll-by-poll results released after an election, cross-referencing this data with the list of electors and addresses provided by Elections Canada (Bennett and Bayley, 2012: 15–19). This provides a starting point for building more complete databases on electors' attitudes, affiliations and intentions. Increasingly, parties collect personal information about electors from social media, political marketing agencies or data brokers (McEvoy, 2019; Bennett and McDonald, 2019). Data is less commercially available, less complete and potentially more expensive in Canada than in the United States, affecting the cost-benefit ratio of data-driven campaigning (McKelvey and Piebiak, 2019).

Door-to-door and telephone canvassing are important sources of data. Canvassing is viewed by some parties not as an opportunity for dialogue or a way to convince electors to vote for their candidates but as a site of data collection (Munroe and Munroe, 2018). Some parties' canvassers use a smartphone app to collect information about constituents, such as whether they are a supporter, their ethnicity, and whether they have young children; others use paper, later entering data into the database (Munroe and Munroe, 2018). Our study focused in part on interactions between party personnel and electors because electors may not be aware that data is being collected through such interactions or what its potential uses are. We wondered whether awareness of data collection might change the nature of electors' interactions with political parties—a key site of democratic engagement.

Given the decreased dialogue and increased emphasis on data collection in electoral canvassing, privacy and surveillance have moved to the core of political communications, where techniques of consumer surveillance have begun to take hold (Bennett and Lyon, 2019). It is taken as established that opaque surveillance practices are problematic for democracy and that privacy is essential to political participation (Bennett and Oduro-Marfo, 2019). Data-driven campaigns can drive divisiveness when different messages are targeted to different groups, and they can harm the “marketplace of ideas” when messages are conveyed in relative secrecy to some groups and not to others, preventing messages from being confronted by other messages and views. Targeted election advertisements could undermine voter autonomy through narrowing information that voters receive. The use of manipulative psychographic profiling could undermine both privacy and autonomy (Burkell and Regan 2019; Dobber et al., 2019). Data-driven campaigning could leave parties in power beholden to specific groups rather than to broader publics, even redlining or ignoring and excluding groups from political communications (Bennett and Lyon, 2019; Cohen, 2021: 604–5). Data-driven campaigning can creep into the “permanent campaign” of governing when it is adopted by parties in power and government itself (Marland et al., 2017; Bodó et al., 2017: 4). The relative availability and affordability of data to large versus small parties, central versus local party organizations, or political parties versus advocacy groups, shifts electoral power dynamics (Bennett and Lyon, 2019; McKelvey and Piebiak, 2019: 209; Small and Jansen, 2020).

In Canada, data-driven campaigning has unique implications given our first-past-the-post electoral system and weaker partisan affiliation of electors, which can mean that some votes are “up for grabs” and can swing elections (Bennett and McDonald, 2019). Further, “the volatile party system, a declining

engagement with political parties, a culture of electoral pragmatism, and strict limitations on campaign financing all increase the importance of gathering and deploying data on actual and potential voters” (Bennett and McDonald, 2019: 146). Most significant, given our focus, is that data-driven elections could lead to negative attitudes and a decline in political engagement if “voters perceive that their interests are being manipulated by political and technical elites” (Bennett and Lyon, 2019: 4).

Literature Review

Awareness of collection

It has often been stated, but never empirically confirmed, that Canadians are unaware of the extent of political parties’ collection of personal information. Therefore, in this article we extend our past work by asking the following question:

RQ1: Are respondents aware that federal political parties collect their personal information?

A decade before the Cambridge Analytica news broke, Howard and Kreiss remarked that voters “do not always realize that data about them is being collected and used for political purposes, and are surprised when they discover that they have been profiled” (2009: 8). As Bennett and Oduro-Marfo also point out, “relatively little” is known about “how privacy has been compromised by democracy [itself], . . . by the agents that seek to mobilise, engage, and encourage us to vote—or not to vote” (2019: 11). A recent survey by OpenMedia asked about awareness of the Cambridge Analytica scandal but not about awareness of the collection of personal information by political parties. It found that about 61 per cent of those surveyed had followed the issue at least somewhat closely (OpenMedia and Innovative Research Group, 2018).

In Canada, the Office of the Privacy Commissioner of Canada (OPC) conducts a survey of Canadian residents’ perceptions of privacy biannually. While these surveys do not normally address awareness about the collection of personal information by political parties specifically, they consistently show that Canadians’ general awareness and knowledge about privacy rights is growing.

We are not aware of a survey other than our own (Bannerman *et al.*, 2019) that examines current knowledge of federal parties’ personal information collection practices in Canada. While there is beginning to be significant literature on datified campaigning in Canada (Giasson *et al.*, 2019; Munroe and Munroe, 2018; McKelvey and Piebiak, 2018, 2019; Bennett and Lyon, 2019), this literature has rarely explored Canadians’ level of awareness that datified campaigning is taking place. Understanding Canadians’ level of awareness is important for our purposes because attitudes may be influenced by a lack of full awareness.

Trust, privacy and democratic engagement

No study, to our knowledge, examines the effects of awareness of Canadian political parties’ collection of personal information on electors’ willingness to engage or

interact with parties or campaigns. Therefore, we ask in our second research question:

RQ2: Does awareness of political party collection of personal information affect willingness to engage with campaigns?

It stands to reason, and privacy experts often state, that privacy plays an essential role in strengthening democratic engagement (Bennett, 2018a, 2018b, 2015; Bennett and Bayley, 2018; Bennett and Oduro-Marfo, 2019; Gavison, 1980; House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2018a, 2018b; Information Commissioner's Office, 2018b, 2018a). One of the purposes of privacy protection, it is said, is to protect citizens' willingness to engage in political processes without fear of judgment or interference. There is a rich literature that addresses the role played by effective privacy protection in democratic societies, in which privacy advances individual autonomy and self-fulfillment, reinforces political competition, and bolsters participation and engagement, including "voting freely, speaking out, engaging in interest groups, signing petitions, participating in civil society activism and protesting"; privacy also "enhances the freedom to make choices under conditions of genuine reflection and equal respect for the preferences, values and interests of others" (Bennett and Oduro-Marfo, 2019: i and 9). The UK Information Commissioner's Office has argued that parties' digital data processing techniques "can have a significant impact on people's privacy," expectations of privacy, and trust in the democratic system (Information Commissioner's Office, 2018a: 8–9).

While we are not aware of a study empirically examining a link between awareness and engagement, Kefford (2021) has examined Australians' attitudes toward parties' data collection at the point of engagement, finding that 47 per cent of respondents were "uncomfortable" or "very uncomfortable" with parties collecting information on "who you said you would vote for" in person or over the phone (Kefford, 2021: 148). Fewer were "uncomfortable" or "very uncomfortable" with the collection, in person or over the phone, of "the issues you said you are especially concerned about" and "what you said your views were on the prime minister" in their databases (20% and 30% respectively) (Kefford, 2021: 149).

Trust in political institutions and actors is an essential aspect of political culture that serves as a precursor to democratic engagement (Almond and Verba, 1963; Easton, 1965). Trusting citizens are much more likely to cast a ballot than are distrusting electors (Hooghe, 2018). Studies of trust have helped explain lower participation in extraparliamentary elections (Cox, 2003) and have highlighted the importance of trust in parliament and political representatives (Grönlund and Setälä, 2007). Likewise, there is a positive relationship between trust and institutionalized forms of participation organized by elites such as political parties (Hooghe and Marien, 2013). Such activities could include party membership, working with a party or organization, and contacting government officials (Hooghe and Marien, 2013). Overall, the more trusting citizens are, the more likely they are to participate at election time and to leverage other opportunities in the political system.

The importance of trust is juxtaposed with Canadians' increasingly less favourable attitudes toward the political system and declining levels of trust in political institutions (including parties) (Cross, 2004; O'Neill, 2003; Pammett and Leduc, 2003). If parties' data collection practices further erode Canadians' trust in political parties, political engagement could be affected, weakening the social fabric of society and lowering legitimacy in the political system (Putnam, 2000; Easton, 1965).

Some fear that the unauthorized use of personal information may undermine the legitimacy of political and electoral processes (Bennett, 2018b; Bennett and Bayley, 2018; Delacourt, 2013; Hankey *et al.*, 2018; House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2018a; Information Commissioner's Office, 2018b, 2018a). The UK Information Commissioner's Office (2018a) has warned that parties' data practices could negatively impact citizen's privacy and political trust. (Worryingly, 6 per cent of election candidates responding to an Elections Canada survey said they "did not take any measures to protect personal information" [Elections Canada and Ekos Research, 2019: 51].) A significant privacy breach, and media coverage thereof, could have far-reaching implications beyond any one political party, potentially affecting engagement with the broader political system. As Bennett and Bayley (2012) argue, such an incident could hasten trends in falling democratic engagement. Our study is the first of which we are aware to test the empirical link between awareness of parties' data collection practices and engagement with political parties.

Specific concerns and predictors of higher levels of concern

Research has yet to examine Canadians' specific concerns about political parties' collection or use of personal information. To address this gap, we propose a third research question:

RQ3: What are Canadians' concerns regarding political parties' collection and storage of personal information? What characteristics point to higher levels of concern?

Several studies have examined general levels of concern about political parties' collection of personal information, or privacy more broadly; however, much of this has been conducted by polling companies. Work by the Knight Foundation and Gallup show concerns about targeted political ads (McCarthy, *n.d.*), while a study by Ryerson's Social Media Lab suggests that a majority of Canadians (65%) are "uncomfortable" with the use of publicly available social media data by political parties and (54%) political polling (Dubois *et al.*, 2018). An Australian study showed that few respondents were "not concerned" about political parties acquiring personal data from banks or other financial institutions, "companies you buy things from" or social media companies (Kefford, 2021: 150–51). No study of which we are aware has asked participants about a broad range of concerns regarding use of their personal information by parties.

How does awareness of parties' data collection relate to levels of concern? We hypothesize that awareness of parties' data collection practices raises respondents' levels of concern about parties' collection of personal information:

H.a: Those who were aware (before we confirmed or revealed) that political parties collect a lot of personal data will be more concerned with that data collection.

Understanding the relationship between awareness of collection and concern is important because policy makers and privacy experts, as mentioned above, often theorize that as awareness rises, so might levels of concern, presenting a potential threat to democratic trust and engagement. Our work adds to evidence of an empirical link.

At least one past study has associated higher levels of awareness with higher levels of concern about data collection in an electoral context: a 2018 survey by OpenMedia found that 61 per cent of Canadians surveyed were at least “somewhat closely aware” of the Cambridge Analytica scandal and that 65 per cent were either very or somewhat concerned “about the possibility of private companies collecting personal information about Canadians and using it in an attempt to influence the election.” The survey found that the more aware respondents were of the news stories about Cambridge Analytica, the more concerned they were (OpenMedia and Innovative Research Group, 2018: 7). It remains to be examined whether higher levels of awareness of collection by *political parties* correlates with higher levels of concern. (We acknowledge that higher levels of awareness of data collection do not necessarily correlate with behaviours relating to data disclosure or privacy choices [Turow et al., 2015; Williams and Nurse, 2016]).

We are also interested in whether belief in the importance of parties’ collection of personal information to democracy affects level of concern. No previous literature has examined this relationship. We hypothesize that:

H.b: Those who believe political parties collecting personal data is important for democracy will be less concerned with that data collection.

The relationship between the belief that collection is important to democracy and level of concern is important because of how often “importance to democracy” serves to justify collection and lack of privacy regulation. Some scholars have argued that to be able to fulfill their democratic function of mobilizing electors and encouraging participation, political parties need to access personal information (Bennett and Bayley, 2012: 3–4). Parties and politicians contend that their needs for personal information are special (Bennett and Bayley, 2012: 3–4) and that exempting political parties and representatives from privacy law supports freedom of political communication and enhances electoral and political processes (Williams, 2000; Cohen 2021). They have argued that privacy laws intended for the private sector are inappropriate for parties as “associations of volunteers” (Fenrick, 2018) and that privacy law could stand in the way of parties’ ability to develop and assess popular support for policy positions, of parties’ understanding of electors’ political opinions or philosophical beliefs, and of data-intensive campaigning (Cohen, 2021: 590). Some argue that privacy penalties, if applied to political parties, could have a chilling effect on political processes (Fenrick, 2018).

However, the legitimacy of parties’ exemption from privacy law has been questioned by those who argue that political parties should be subject to privacy law (Cohen, 2021; Fenrick, 2018; Williams, 2000). While the belief that the collection

of personal information is important to democracy might be associated with less concern about data collection, it could also be associated with greater concern and associated calls for regulation and oversight to ensure that collection is done properly with appropriate oversight, given its importance.

Attitudes about the applicability of privacy law to political parties

Finally, we ask in our fourth research question:

RQ4: Do Canadians believe that political parties should be subject to privacy and data collection and retention laws?

At least two past surveys have polled Canadians' attitudes toward whether political parties should be subject to privacy laws (Curry, 2019; Office of the Privacy Commissioner of Canada, 2009). A recent survey conducted by the Centre for Digital Rights showed that 91 per cent of respondents in Canada were unaware (or unsure) about whether Canadian privacy law applies to political parties (Curry, 2019). When respondents were informed that federal privacy law did not currently apply to political parties, 88 per cent said that it should (Curry, 2019). This result is similar to a 2009 survey by the OPC that found that an overwhelming majority of Canadians (92%) felt that political parties and politicians should be subject to privacy laws (Office of the Privacy Commissioner of Canada, 2009). An Australian study showed that a smaller percentage (66%) of respondents disagreed or strongly disagreed that "political parties should be exempt from privacy legislation" (Kefford, 2021: 146). Here, our study tests what has been suggested by previous work. No past study, to our knowledge, has broken down the *types* of information that Canadians believe political parties should collect.

Methods

As outlined above, this article answers the following research questions:

RQ1. Are respondents aware that federal political parties collect their personal information?

RQ2. Does awareness of political party collection of personal information affect willingness to engage with campaigns?

RQ3. What are Canadians' concerns regarding political parties' collection and storage of personal information? What characteristics point to higher levels of concern? We hypothesize that:

H.a: Those who were aware (before we confirmed or revealed) that political parties collect a lot of personal data will be more concerned with that data collection.

H.b: Those who believe political parties collecting personal data is important for democracy will be less concerned with that data collection.

RQ4. Do Canadians believe that political parties should be subject to privacy and data collection and retention laws? Which types of information should be subject to consent requirements?

Data collection

Building on our previous work (Bannerman et al., 2019), we conducted a survey of 1,000 Canadians in August 2020 through online panel provider AskingCanadians. The survey was conducted in English and French with quotas set for age, gender and province based on Statistics Canada percentages for the population, in order to ensure a sample as representative as possible was obtained. Nevertheless, certain populations were underrepresented, including individuals identifying as “other” gender identities, individuals residing in the territories, and older adults. The use of quotas also renders the sample nonrandom, resulting in larger standard errors than would be the case for simple random samples of the same size.

Respondents were asked if they identified as being a Canadian citizen and were screened based on their commitment to provide honest answers.¹ This was included to encourage respondents’ honesty and attention to the survey. Studies have shown such an approach can reduce the social desirability of responses in online surveys (Vésteinsdóttir et al., 2019).

Measures

The study used the following measures:

Awareness

To measure respondents’ awareness of political parties’ collection of personal information, we first gave respondents a list of 14 types of information that political parties could collect (for example, name, phone number, income, political views). We asked them to respond yes or no to the following statement for each item: “I believe that Canadian federal political parties collect my ___ for use in electoral campaigning.” These 14 questions were used to respond to RQ1. We computed a scale variable by summing the responses for all 14 items, which we used to respond to RQ2 and to H.a, the first hypothesis related to RQ3. We also operationalized awareness through a series of likelihood of engagement questions described next.

Likelihood of engagement

To assess how respondents felt about engaging with political party personnel before and after knowing about their data collection practices, we first asked respondents: “If a federal election were in progress now, how likely would you be to speak with campaign personnel in person or by phone?” We also asked: “If a federal election were in progress now, how likely would you be to interact with political parties or politicians on social media (for example, by liking or commenting on their content, (re)posting their content, or signing on to petitions?)” Having established this baseline, we told participants later in the survey: “Canadian political parties might indeed collect personal information such as your name, contact information, religion, gender, ethnicity, and political views.” We then repeated both likelihood

questions, adding: “Knowing that parties might collect such information.” Response options for all four questions were: “very unlikely,” “somewhat unlikely,” “somewhat likely,” “very likely” and “don’t know/prefer not to say” (treated as missing). Binary versions were computed into likely/unlikely. These measures were used to respond to RQ2. We asked more general questions first before introducing the topic of parties’ collection of data, so as not to prime participants who did not know about parties’ collection of voter data and who might be discouraged by learning about such practices. Asking more general questions before specific ones is also a best practice in survey construction to ensure the responses to more general questions are not affected (McFarland, 1981).

Concern

We measured concern about political parties collecting personal information using a 5-point Likert scale matrix that included 17 items, with response options ranging from “not at all concerned” to “extremely concerned.” We computed a scale variable for concern based on mean values for all 17 items. Cronbach’s alpha is .956, indicating sufficient internal consistency. This variable is the dependent variable in RQ3 and related hypotheses.

Importance for democracy

We asked respondents: “How important is it, to the democratic process, for political parties to collect personal information about Canadian voters?” Response options ranged from “not at all important” to “extremely important” on a 7-point scale. This variable is an independent variable in H.b, the second hypothesis related to RQ3.

Collection

We measured if people believe political parties should be allowed to collect and retain a variety of types of information, using 14 items with the response options “yes,” “yes, but only with my explicit consent,” “no, never,” and “don’t know/prefer not to say.” This measure is used in RQ4.

Privacy laws

We measured whether people believe political parties should be subject to privacy laws with the questionnaire item: “Canadian federal privacy laws generally DO NOT apply to political parties. Do you think that federal privacy laws SHOULD apply to political parties?” Response options were: “I think federal privacy laws SHOULD apply to political parties in Canada,” “I think federal privacy laws SHOULD NOT apply to political parties in Canada” and “don’t know/prefer not to say.” This measure is used to respond to RQ4.

We include control variables for age group, gender, and identification as a visible minority for both hypotheses related to RQ3. [Table 1](#) displays a summary of variables and their characteristics.

Analytical approach

To respond to RQs 1 and 4, we rely primarily on descriptive statistics to illustrate trends. To respond to RQ2 we use McNemar’s test to investigate differences in

Table 1. Variable Characteristics

Variable	Coding	M(SD)	%	N
<i>Awareness scale</i>	Scale (0–14)	6.13(3.58)		1,000
<i>Likelihood—in person or by phone</i>				
- before	Nominal (likely = 1)		34.1	954
- after			35.8	960
<i>Likelihood—social media</i>				
- before	Nominal (likely = 1)		32.7	963
- after			27.7	957
<i>Concern scale</i>	Composite score (max. 5.00)	3.69(0.98)		977
<i>Importance for democracy</i>	Likert scale (0–7)	3.55(1.65)		939
<i>Collection</i>	Ordinal (1 = yes; 2 = yes, but only with my explicit consent; 3 = no, never; 4 = don't know/prefer not to say)	see Figure 4		1,000
<i>Privacy laws</i>	Nominal (should = 1)		84.7	1,000
Controls				
<i>Age</i>	Ordinal (1 = under 18; 2 = 18–24; 3 = 25–34; 4 = 35–34; 5 = 45–54; 6 = 55–64; 7 = 65–69; 8 = 70+)	4.8(1.81)		1,000
<i>Gender</i>	Nominal (1 = not male) (2 = male)		51	999
<i>Visible minority</i>	Nominal (1 = visible minority)		19	1,000

likelihood of engagement with political party representatives before and after a stimulus about data collection by political parties. We also ran a Spearman's rank correlation to supplement these results. We use an exploratory pretest-posttest design, ideal for hypothesis generation, to initially see if there are relationships among variables. The goal of this study is to establish justification for future and more resource-intensive studies based higher in the evidence hierarchy, permitting stronger claims, such as an experimental approach (Leigh, 2009). RQ3 and related hypotheses were addressed using descriptive statistics and a multiple linear regression model.

Analysis

RQ1: *Are respondents aware that federal political parties collect their personal information?*

We found, in response to RQ1, that respondents were aware of some information collected by political parties.² As [Figure 1](#) shows, most respondents (more than 60%) expressed awareness that political parties may collect electors' names, address, phone number, age and gender. However, most were not aware of the wide variety of the types of information that political parties collect. Fewer were aware that parties may collect information about "whether I have voted in elections" (51%) and email addresses (47%). Fewer still showed awareness that parties may collect information about political views (30%), ethnicity (27%), income (23%), online activities (21%), occupation (20%), social media ID (19%) or religion (17%). These results were, overall, consistent with our past research on the same topic (Bannerman et al., 2019). These results build on survey research by OpenMedia that suggested a general awareness among most survey respondents (about 60%) that data

Q. 12 I believe that Canadian federal political parties might collect my () for use in electoral campaigning

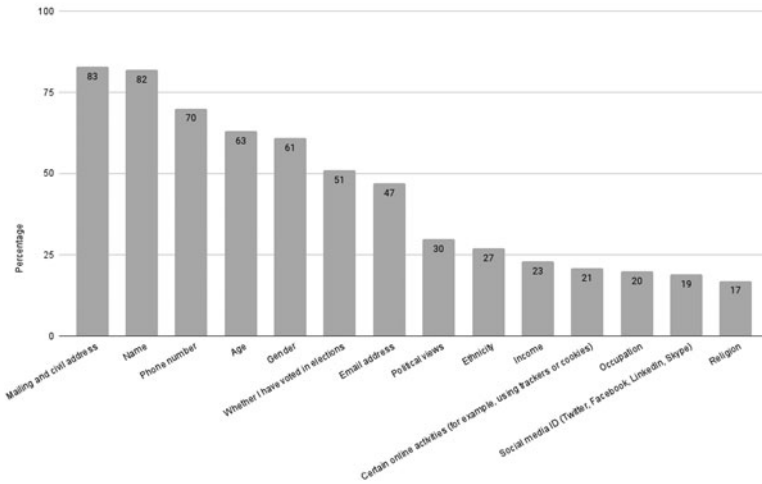


Figure 1. Proportion of respondents who believe political parties collect various types of information.

collection occurs. Our research finds that there is limited awareness of the potential breadth of the types of personal information collected (OpenMedia and Innovative Research Group, 2018).

RQ2: *Does awareness of political party collection of personal information affect willingness to engage with campaigns?*

To answer RQ2, we tested individuals’ likelihood of engaging with political parties by phone or in person, and by social media, “if a federal election were in progress now” and then again after we revealed (or confirmed) that political parties might collect personal data. Tables 2 and 3 depict responses before and after the reveal for phone or in person and via social media, respectively.

With respect to engagement in person or by phone, before the reveal, 34 per cent of respondents were likely to engage with campaigns while 66 per cent were not. After the reveal, 36 per cent were likely to engage while 64 per cent were not. In total, 54 people went from being likely to engage by phone or in person to being unlikely once they were informed that parties can collect personal data, and 73 people went from being unlikely to engage to being likely to engage once they were informed that parties can collect personal data. Using McNemar’s test revealed that these small differences are not statistically significant.

Table 2. Likelihood to Engage in Person or by Phone, before and after Reveal (n = 932)

		After reveal (in person or by phone)		
		Unlikely	Likely	Total
Before reveal (in person or by phone)	Unlikely	543	73	616
	Likely	54	262	316
	Total	597	335	932

Table 3. Likelihood to Engage via Social Media, before and after Reveal ($n = 948$)

	After reveal (via social media)			Total
		Unlikely	Likely	
Before reveal (via social media)	Unlikely	607	33	640
	Likely	77	231	308
	Total	684	264	948

Our findings related to engagement on social media were, however, statistically significant. On social media, before the reveal, 32 per cent of respondents were likely to engage with campaigns while 68 per cent were not. After the reveal, 28 per cent were likely to engage while 72 per cent were not. In total, 77 people went from being likely to engage via social media to being unlikely once they were informed that parties can collect personal data. Meanwhile, 33 people went from unlikely to being likely to engage once they were informed that parties can collect personal data. While still relatively small, this difference is statistically significant ($p < .001$).

In short, awareness of political parties' collection of personal data seems to have a different impact on individuals' likelihood of engaging with political parties depending on whether they are engaging by phone or in person or via social media. When it was revealed or confirmed that political parties do collect personal information, respondents' likelihood of engaging in person or by phone did not change. However, they became less likely to engage via social media. While the reported results are based on two McNemar's tests using dichotomous versions of our variables, Wilcoxon tests on ordinal versions of our variables also support this conclusion.

We also checked the relationships between the number of types of personal information people believe political parties collect and likelihood of engagement by phone or in person and likelihood of engagement on social media. We used Spearman's rank order correlation, and the only significant correlation was with social media after the reveal; this relationship was very weak and positive ($r = .083$, $p = .011$).

The main finding from this analysis is that people feel differently about engaging with campaign personnel by social media compared with engaging by phone or in person. When it was revealed or confirmed that political parties may collect a broad range of personal information, respondents became less likely to engage via social media.

RQ3: What are Canadians' concerns regarding political parties' collection and storage of personal information? What characteristics point to higher levels of concern?

Next, we asked respondents about the types of concerns they have with political parties collecting and storing their personal information (RQ3). We then examined what predicts concern and hypothesized that:

H.a: Those who were aware (before we confirmed or revealed) that political parties collect a lot of personal data will be more concerned with that data collection.

H.b: Those who believe political parties collecting personal data is important for democracy will be less concerned with that data collection.

Given that we know variables such as age, gender, and whether an individual is a member of a visible minority group can impact levels of concern, we controlled for these variables.

We developed a scale for concern based on mean responses to 17 different Likert scale items (see Question 15 in Appendix C and D). This question was close-ended, and possible areas for concern were provided for respondents, possibly giving them ideas they may not have otherwise considered. That said, respondents chose to select responses that they identified with and that they felt captured their concerns.

Before discussing our regression analysis, it is useful to review responses to those questions. Figure 2 shows levels of concern for each question individually. Among the top-ranked concerns were those involving data security and breaches, including unauthorized access to personal information. Parties sharing or selling personal information with third parties (62% were “extremely concerned”) was most respondents’ primary concern with parties’ data practices, followed by “hackers accessing the party database” (59% were “extremely concerned”). Parties having outdated information and parties predicting voting behaviour were least concerning for respondents. Even those items people were least concerned with showed high levels

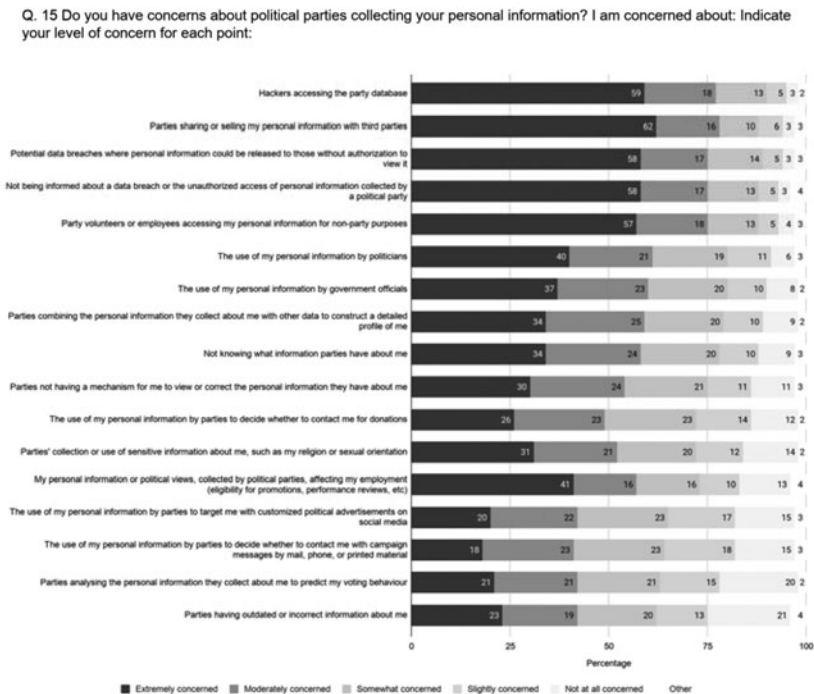


Figure 2. Concerns about political parties collecting personal information

Q.16 How important is it, to the democratic process, for political parties to collect personal information about Canadian voters?

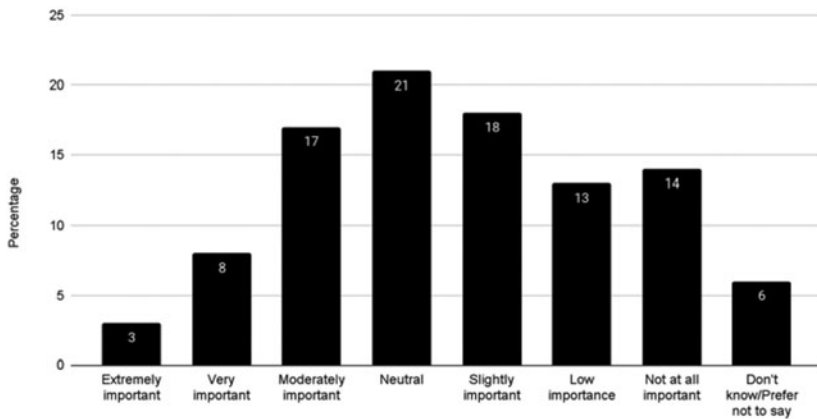


Figure 3. Importance of collection of personal information to the democratic process.

of concern, with over 75 per cent of respondents saying they were at least “slightly concerned” about all 17 items.

When all concerns are taken together as a scale, responses are on average “somewhat concerned” but skew toward moderately/extremely concerned ($M = 3.69$, $SD = 0.982$).

We asked respondents how important it is for the democratic process that political parties be able to collect information about the electorate; results are shown in Figure 3.

Only 28 per cent of respondents saw the collection of personal information as extremely, very or moderately important to the democratic process. A large percentage said it was “not at all important,” of “low importance” or “slightly important” (45% in total). A fifth (21%) of respondents said that they were neutral on the question. Just over a tenth of respondents said that collecting personal information was “not at all” important to the democratic process.

Next, we conducted a multiple linear regression model to respond to our hypotheses about information and level of concern; results are shown in Table 4.

Here we see that both our independent variables and all our control variables are significant. However, none of them are particularly strong explanatory variables. Overall, about 9.1 per cent of variance in concern can be explained by the independent and control variables together.

All demographic variables predict concern in the expected way. As age group increases, so does concern. People who self-identify as male are less concerned than those who self-identify as something other than male.³ Self-identifying as being a visible minority is a predictor of higher concern related to parties’ data collection practices.

We find support for our first hypothesis (H.a) that those who were aware (before we confirmed or revealed) that political parties collect a lot of personal data will be

Table 4. Multiple Linear Regression ($N = 924$)

	<i>B</i>	<i>SE</i>
Age	.129***	.017
Gender (not male/male)	-.158*	.062
Visible minority (yes/no)	.255**	.081
Information awareness	.033***	.009
Importance for democracy	-.071***	.019
Constant	3.291***	.149
R^2	.091	

* $p < .05$; ** $p < .01$; *** $p < .001$

more concerned about that collection. As people indicate higher prior awareness of data collection, their concern about its use increases.

We also find support for our second hypothesis (H.b) that those who believe that political parties collecting personal data is important for democracy will be less concerned with that data collection. As people report higher perceived importance for democracy of political parties' data collection, concern decreases.

It should be noted that this is an exploratory investigation. Our research confirms a link between prior awareness and concern, and it provides initial evidence of an inverse link between belief in the importance of collection to democracy and concern. As we suggest below, these links have important policy implications. Future research should seek to understand what other variables might help explain variance in levels of concern.

RQ4: Do Canadians believe that political parties should be subject to privacy and data collection and retention laws? Which types of information should be subject to consent requirements?

When we asked respondents whether they believed that Canadian political parties should be subject to privacy law, a strong majority (85%) answered in the affirmative. Only 4 per cent were opposed to the application of privacy laws to political parties. This finding is consistent with past surveys' findings, discussed in the literature review above.

To further examine which types of personal information should require consent under privacy law, our survey listed 14 different kinds of personal information that political parties in Canada may collect. Figure 4 represents respondents' answers regarding whether they believe parties do collect each kind of information, laid over a bar graph of normative beliefs about whether parties should be allowed to collect these kinds of information.

Most strikingly, respondents felt that explicit consent should be required even for the least controversial types of information: names and addresses. The Canada Elections Act currently explicitly authorizes members of Parliament and political parties to obtain this information without specific consent.

Nearly a fifth of respondents indicated their belief that political parties should never (not even with consent) be allowed to collect electors' names. Over two-thirds stated that political parties should never be allowed to collect social media information and sexual orientation information. Some respondents said that political

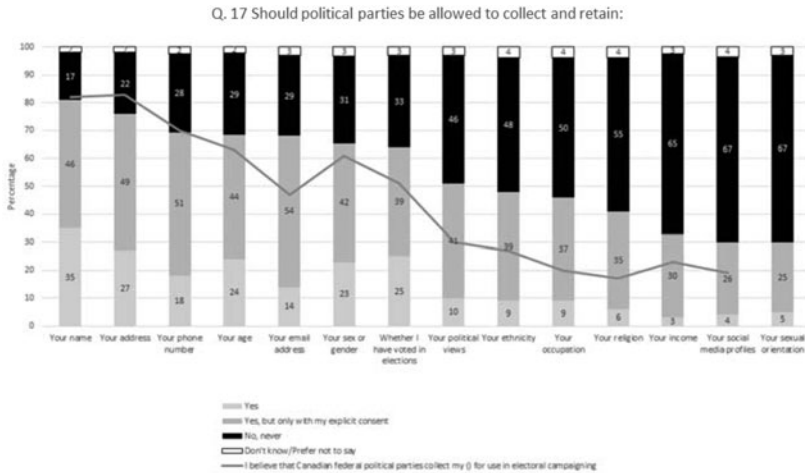


Figure 4. Types of information political parties should be allowed to retain.

parties should never be allowed to collect information about names and addresses (17% and 22%, respectively). Half of respondents or more also felt that parties should never be allowed to collect personal information about occupation (50% of respondents said political parties should never be allowed to collect this type of information), religion (55%), income (65%), sexual orientation (67%) and social media profiles (67%). A large share of respondents said that political parties should never be allowed to collect information about political views (46%) and ethnicity (48%). This suggests that Canadians might like to see a consent requirement applied to a broad range of information collection.

Conclusion

We find (RQ1) that survey respondents are not currently aware of the extent of parties' data collection practices in Canada. While this has often been stated, our survey provides the first empirical evidence of the lack of awareness of the breadth of types of personal information parties may collect. Here, our work builds on an OpenMedia survey investigating levels of awareness that collection occurs.

We find limited evidence (RQ2) that when informed of parties' data collection practices, respondents are significantly less likely to engage with parties on social media. While it is often stated, and stands to reason, that privacy strengthens democratic engagement, we are not aware of a study empirically linking awareness of collection by political parties and engagement. Our exploratory study provides some initial evidence about this relationship using pretest-posttest design, justifying future more resource-intensive studies, such as an experimental approach. If future studies confirm that collection, or awareness thereof, reduces political engagement, the results would be concerning.

Our study (RQ3) adds to some existing evidence of an empirical link between awareness of collection and levels of concern—a link that policy makers and privacy experts have theorized. While awareness of the extent of Canadian parties' data collection is currently low, respondents who are more aware of this collection are more

concerned about it, confirming hypothesis H.a: “Those who were aware (before we confirmed or revealed) that political parties do collect a lot of personal data will be more concerned with that data collection.” These findings raise alarms about what a growing awareness of parties’ collection practices might mean for datified campaigning. As social media and online engagement become a growing part of Canadian political campaigns (Giasson *et al.*, 2019), increasing awareness combined with growing concern could threaten to undermine whatever potential social media offers to lower barriers to political engagement (Small *et al.*, 2014).

No previous study has examined levels of belief in the importance of parties’ collection of personal information to democracy or the relationship between levels of belief in collections’ importance to democracy and levels of concern about such collection. We found that many respondents do not believe that collection is important to democracy and that respondents who believe political parties’ collection of personal information is important for democracy are less concerned about data collection (RQ3, confirming hypothesis H.b: “Those who believe political parties collecting personal data is important for democracy will be less concerned with that data collection”).

Confirming the link between belief in the importance of data collection to democracy and lower levels of concern is important because of how often “importance to democracy” serves to justify collection of personal information by political parties and because of the lack of privacy regulation. We might now theorize that if the value of certain types of collection and use by parties to democracy were demonstrated, it is possible that this could lower concern.

Our study adds to the literature on datified campaigning, which, to date, has been primarily interview-based (Bodó *et al.*, 2017). It provides initial quantitative evidence of (RQ1) relatively low levels of awareness of the extent of parties’ data collection practices, of a link (RQ2) between awareness of collection and decreased willingness to engage with parties on social media, of the types of concerns that respondents have about collection, of skepticism (RQ3) about whether collection is important to democracy, and of an inverse link between belief in collections’ importance to democracy and levels of concern. Most importantly, our research on the link between awareness and concern (RQ2) suggests that (and provides groundwork for future investigation of whether) political parties’ failure to subject themselves to oversight of their data collection and use may, over time, undermine electors’ willingness to engage with parties—particularly online—as awareness grows. Even a small decrease in engagement could have important implications in a first-past-the-post system, where a small number of votes can swing elections (Bennett and McDonald, 2019).

A vast majority of respondents (RQ4) believe that political parties should be subject to privacy and data collection and retention laws. In fact, most respondents do not believe that Canadian political parties should be allowed to collect personal information—even basic information—without consent. Canadians’ sense of what political parties should be allowed to collect and retain without explicit consent may be at odds with both the law and parties’ practices, particularly with regard to names and addresses, but also with regard to a broad range of personal information that parties may have collected without consent, including age, email addresses, gender, ethnicity, occupation, religion, and social media information—categories that the vast majority of survey respondents felt should “never” be collected and retained or should only be collected and retained with an individual’s “explicit consent.”

There has so far been “a notable reluctance among elected officials and party leaders to take up the issues of data security and privacy in a comprehensive way,” perhaps because both political leaders and data firms have interests in access to elector data and, perhaps, in preventing industry oversight. Most discussions attempt to frame the narrative around security instead of privacy (Howard and Kreiss, 2009), and our respondents’ main concerns (RQ3) reflected this focus on security. It would be interesting to track Canadians’ concerns in order to determine whether concerns about security, data profiling, targeting, or incorrect or outdated information change over time. After all, there are numerous reasons to be concerned about datified campaigning, including problematic implications of surveillance for democracy and democratic engagement, concerns about effects on the “marketplace of ideas” and open exchange of ideas, the adoption of surveillance techniques in the permanent campaign and everyday governance, and the effects of datified campaigning on the centralization or diffusion of power among political parties and groups in Canada.

More research is needed to understand the effects of Canadian political parties’ data practices, as well as the potential impacts of privacy law and regulation, on electors’ trust and willingness to engage in the democratic process, particularly online. A comparative study, for example, might explore electors’ trust and engagement between jurisdictions in which privacy law varies in its applicability to political parties. Future research could leverage interviews, focus groups or additional surveys—including those that might make use of an experimental model in which one group of participants is told how much data parties collect and the other not—to deepen our understanding of the effects of political party data practices, as well as knowledge about those practices, on voting and civic engagement.

Our findings thus far lead us to support calls made by regulatory bodies in Canada and other parts of the world to extend privacy laws to political parties, because parties’ contemporary data practices may pose a risk to Canada’s democratic process. To protect electors’ willingness to interact with parties, we recommend that federal privacy laws be extended to apply to federal political parties. The question of whether the Personal Information Protection and Electronic Documents Act (PIPEDA) or the Privacy Act should be amended to apply to federal parties, or whether legislation that is specific to political parties should be enacted, is a question that should be subject to further research (see Judge and Pal, 2021). In addition to federal extension of privacy laws, we recommend that all provinces (except for British Columbia, which has already enacted such laws) should enact privacy laws that fully regulate provincial political parties’ use of electors’ personal information.

Supplementary Material. To view supplementary material for this article, please visit <https://doi.org/10.1017/S000842392200066X>

Competing interests. The authors declare none.

Notes

- 1 Respondents were asked whether they committed to providing thoughtful and honest answers to the questions in this survey.
- 2 Given that political parties in Canada (other than in British Columbia) are not subject to privacy laws and parties’ exact data practices are not audited, we cannot know in detail the extent to which each political

party in Canada collects each type of information. However, we base the following discussion on the available evidence of parties' practices overall and discuss what is known about political parties' practices in general, rather than as related to any particular political party discussed earlier in this article.

3 Our gender variable response options were male, female, non-binary/third gender, prefer to self-describe (open text box) and prefer not to say. One respondent selected "prefer not to say"; this was treated as missing data. There were no self-describe responses, and there were five responses for non-binary/third gender. We combined female and non-binary/third gender responses, since five observations constituted insufficient data for a single category and since this grouping reflects the theoretical expectation that those traditionally marginalized in society based on gender will differ from those not traditionally marginalized, in terms of their privacy concerns. This is in line with current best practices.

References

- Almond, Gabriel and Sidney Verba. 1963. *The Civic Culture: Political Attitudes and Democracy in Five Nations*. Princeton: Princeton University Press.
- Bannerman, Sara, Nicole Goodman, Julia Kalinina and Jenny Zhan. 2019. "Political Parties and Data Privacy." In *Understanding the Digital Ecosystem: Findings from the 2019 Federal Election*, ed. Elizabeth Dubois and Taylor Owen. Ottawa: Digital Ecosystem Research Challenge. <https://www.digital-ecosystem.ca/report>.
- Bennett, Colin and Smith Oduro-Marfo. 2019. "Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities." Paper commissioned by the UK Office of the Information Commissioner for presentation to the 2019 International Conference of Data Protection and Privacy Commissioners.. University of Victoria, BC. https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf.
- Bennett, Colin J. 2015. "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications." *Surveillance & Society* 13 (3/4): 370–84.
- Bennett, Colin J. 2018a. "Cambridge Analytica and Facebook: A Wake-Up Call." *Privacy Laws and Business International Report*, no. 152. https://www.privacylaws.com/Documents/PLB_INT_SPL/INT152sample.pdf.
- Bennett, Colin J. 2018b. "Data-Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations." *Canadian Journal of Law and Technology* 16 (2): 195–226.
- Bennett, Colin J. and Robin M. Bayley. 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/.
- Bennett, Colin J. and Robin M. Bayley. 2018. "The Influence Industry: Data Analytics in Canadian Elections." Paper for Tactical Technology Collective Personal Data and Political Influence Project. <https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-canada.pdf>.
- Bennett, Colin J. and David Lyon. 2019. "Data-Driven Elections: Implications and Challenges for Democratic Societies." *Internet Policy Review* 8 (4). <https://doi.org/10.14763/2019.4.1433>.
- Bennett, Colin J. and Michael McDonald. 2019. "From the Doorstep to the Database: Political Parties, Campaigns, and Personal Privacy Protection in Canada." In *Big Data, Political Campaigning and the Law*, eds. Normann Witzleb, Moira Paterson and Janice Richardson. New York: Routledge.
- Bergeron, Thomas and Thomas Galipeau. 2021. "The Political Implications of Personality in Canada." *Canadian Journal of Political Science* 54 (2): 292–315.
- Bodó, Balázs, Natali Helberger and Claes H. de Vreese. 2017. "Political Micro-Targeting: A Manchurian Candidate or Just a Dark Horse?" *Internet Policy Review* 6 (4): 1–13.
- Burkell, Jacquelyn and Priscilla M. Regan. 2019. "Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy." *Internet Policy Review* 8 (4): 1–24.
- Cohen, Tegan. 2021. "The Political Exemption: A Justifiable Invasion of Privacy in the Political Sphere?" *University of New South Wales Law Journal* 44 (2): 584–612.
- Cox, Michaelene. 2003. "When Trust Matters: Explaining Differences in Voter Turnout." *JCMS: Journal of Common Market Studies* 41 (4): 757–70.
- Cross, William. 2004. *Political Parties*. Vancouver: UBC Press.
- Curry, Bill. 2019. "Majority of Poll Respondents Express Support for Extending Privacy Laws to Political Parties." *Globe and Mail*, June 13. <https://www.theglobeandmail.com/politics/article-majority-of-poll-respondents-express-support-for-extending-privacy/>.

- Delacourt, Susan. 2013. *Shopping for Votes: How Politicians Choose Us and We Choose Them*. Madeira Park: Douglas & McIntyre.
- Dobber, Tom, Damian Trilling, Natali Helberger and Claes de Vreese. 2019. "Spiraling Downward: The Reciprocal Relation between Attitude toward Political Behavioral Targeting and Privacy Concerns." *New Media & Society* 21 (6): 1212–31.
- Dubois, Elizabeth, Anatoliy Gruz, Philip Mai and Jenna Jacobson. 2018. "Social Media and Political Engagement in Canada." Version 1.0. Ryerson University Social Media Lab. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299155.
- Easton, David. 1965. *A Systems Analysis of Political Life*. New York: John Wiley & Sons.
- Elections Canada and Ekos Research. 2019. "Survey of Candidates of the 43rd Federal General Election: Narrative Report." Ottawa: Elections Canada. https://publications.gc.ca/collections/collection_2021/elections/SE3-114-4-2021-eng.pdf.
- Fenrick, Michael. 2018. "Evidence - ETHI (42-1) - No. 123." Standing Committee on Access to Information, Privacy and Ethics. House of Commons of Canada. October 30. <https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-123/evidence>.
- Gavison, Ruth. 1980. "Privacy and the Limits of Law." *The Yale Law Journal* 89 (3): 421–71.
- Giasson, Thierry, Gildas Le Bars and Philippe Dubois. 2019. "Is Social Media Transforming Canadian Electioneering? Hybridity and Online Partisan Strategies in the 2012 Quebec Election." *Canadian Journal of Political Science* 52 (2): 323–41.
- Grönlund, Kimmo and Maija Setälä. 2007. "Political Trust, Satisfaction and Voter Turnout." *Comparative European Politics* 5 (4): 400–22.
- Hankey, Stephanie, Ravi Naik and Julianne Kerr Morrison. 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>.
- Hooghe, Marc. 2018. "Trust and Elections." In *The Oxford Handbook of Political Trust*, ed. Eric M. Uslaner. Oxford: Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780190274801.013.17>.
- Hooghe, Marc and Sofie Marien. 2013. "A Comparative Analysis of the Relation Between Political Trust and Forms of Political Participation in Europe." *European Societies* 15 (1): 131–52.
- House of Commons Standing Committee on Access to Information, Privacy and Ethics. 2018a. "Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process." Report of the Standing Committee on Access to Information, Privacy and Ethics. <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf>.
- House of Commons Standing Committee on Access to Information, Privacy and Ethics. 2018b. "Toward Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act." Report of the Standing Committee on Access to Information, Privacy and Ethics. <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf>.
- Howard, Philip N. and Daniel Kreiss. 2009. "Political Parties & Voter Privacy: Australia, Canada, the United Kingdom, and United States in Comparative Perspective." World Information Access Project Working Paper #2009.1. Seattle: University of Washington. <http://dx.doi.org/10.2139/ssrn.2595120>.
- Information Commissioner's Office. 2018a. "Democracy Disrupted: Personal Information and Political Influence." July 11. <https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf>.
- Information Commissioner's Office. 2018b. "Investigation into the Use of Data Analytics in Political Campaigns." November 6. <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.
- Judge, Elizabeth and Leslie Pal. 2021. "Voter Privacy and Big-Data Elections." *Osgoode Hall Law Journal* 58 (1): 1–55.
- Kefford, Glenn. 2021. *Political Parties and Campaigning in Australia: Data, Digital and Field*. Cham, Switzerland: Springer.
- Leigh, Andrew. 2009. "What Evidence Should Social Policymakers Use?" In *Economic Round-Up* 1: 27–43. Canberra: Commonwealth of Australia.
- Marland, Alex, Thierry Giasson and Anna Lennox Esselment, eds. 2017. *Permanent Campaigning in Canada*. Vancouver: UBC Press.
- McCarthy, Justin. n.d. "In U.S., Most Oppose Micro-Targeting in Online Political Ads." *Knight Foundation* (blog), March 2. <https://knightfoundation.org/articles/in-us-most-oppose-micro-targeting-in-online-political-ads/> (May 6, 2020).

- McEvoy, Michael. 2019. "Full Disclosure: Political Parties, Campaign Data, and Voter Consent." Office of the Information and Privacy Commissioner for British Columbia. Investigation Report P19-01. February 6. oipc.bc.ca/investigation-reports/2278.
- McFarland, Sam G. 1981. "Effects of Question Order on Survey Responses." *Public Opinion Quarterly* 45 (2): 208–15.
- McKelvey, Fenwick and Jill Piebiak. 2018. "Porting the Political Campaign: The NationBuilder Platform and the Global Flows of Political Technology." *New Media & Society* 20 (3): 901–18.
- McKelvey, Fenwick and Jill Piebiak. 2019. "Does the Difference Compute? Data-Driven Campaigning in Canada." In *What's Trending in Canadian Politics? Understanding Transformations in Power, Media, and the Public Sphere*, eds. Erin Crandall, Vincent Raynauld and Mireille Lalancette. Vancouver: UBC Press.
- Montigny, Eric, Philippe Dubois and Thierry Giasson. 2019. "On the Edge of Glory (. . . or Catastrophe): Regulation, Transparency and Party Democracy in Data-Driven Campaigning in Québec." *Internet Policy Review* 8 (4). DOI: 10.14763/2019.4.1441.
- Munroe, Kaija Belfry and H. D. Munroe. 2018. "Constituency Campaigning in the Age of Data." *Canadian Journal of Political Science* 51 (1): 135–54.
- Office of the Privacy Commissioner of Canada. 2009. "Canadians and Privacy: Final Report." https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2009/ekos_2009_01/#sec6_10.
- Office of the Privacy Commissioner of Canada. 2019. "Briefing Note 7777-6-335754: Political Party Privacy Policy Alignment to OPC Guidance. [Released under the Access to Information Act]".
- O'Neill, Brenda. 2003. "Examining Declining Electoral Turnout among Canada's Youth." *Electoral Insight* 5 (2): 15–19.
- OpenMedia and Innovative Research Group. 2018. "Federal Privacy Law: National Online Omnibus Survey." <https://openmedia.org/files/OPM.02-Federal-Privacy-Law-Omnibus-Questions-Report-20180516.pdf>.
- Pammatt, Jon H. and Lawrence LeDuc. 2003. "Explaining The Turnout Decline In Canadian Federal Elections: A New Survey Of Non-Voters." Elections Canada. <https://www.elections.ca/res/rec/part/tud/TurnoutDecline.pdf>.
- Patten, Steve. 2017. "Databases, Microtargeting, and the Permanent Campaign: A Threat to Democracy?" In *Permanent Campaigning in Canada*, ed. Alex Marland, Thierry Giasson and Anna Lennox Esselment. Vancouver: UBC Press.
- Putnam, Robert D. 2000. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon and Schuster.
- Small, Tamara and Harold Jansen. 2020. *Digital Politics in Canada: Promises and Realities*. Toronto: University of Toronto Press.
- Small, Tamara, Harold Jansen, Frédéric Bastien, Thierry Giasson and Royce Koop. 2014. "Online Political Activity in Canada: The Hype and the Facts." *Canadian Parliamentary Review* 37 (4): 9–16.
- Turow, Joseph, Michael Hennessy and Nora Draper. 2015. "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation." A Report from the Annenberg School for Communication, University of Pennsylvania. <http://dx.doi.org/10.2139/ssrn.2820060>.
- Vésteinsdóttir, Vaka, Adam Joinson, Ulf-Dietrich Reips, Hilda Bjork Danielsdottir, Elin Astros Thorarinsdottir and Fanney Thorsdottir. 2019. "Questions on Honest Responding." *Behavior Research Methods* 51 (2): 811–25.
- Williams, Daryl. 2000. "Parliamentary Debates: Privacy Amendment (Private Sector) Bill 2000: Second Reading: Speech." Hansard. Canberra, Australia. <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansard%2F2000-04-12%2F0005%22>.
- Williams, Meredydd and Jason R. C. Nurse. 2016. "Optional Data Disclosure and the Online Privacy Paradox: A UK Perspective." In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 186–197, https://doi.org/10.1007/978-3-319-39381-0_17.

Cite this article: Bannerman, Sara, Julia Kalinina, Elizabeth Dubois and Nicole Goodman. 2022. "Privacy and Canadian Political Parties: The Effects of the Data-Driven Campaign on Elector Engagement." *Canadian Journal of Political Science* 55 (4): 873–896. <https://doi.org/10.1017/S000842392200066X>