PRIVACY AND THE ELECTORATE

Big Data and the Personalization of Politics

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

Faculty of Common Law, University of Ottawa

Table of Contents

Key Messages

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

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

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

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

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

---

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

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

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

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

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

Executive Summary

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

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

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

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

Context

Political parties collect, use, store, and analyze data about voters, including sensitive, personal information, yet these activities are generally not subject to the privacy legislation overseeing the private and public sectors. This report surveys the main issues surrounding the data held by political parties, including the absence of legislative oversight, the practices of political parties with regard to data about voters in an environment of rapid technological change, and the risks to voter privacy.

a. The *Privacy Act* is the federal privacy statute regulating the public sector. It does not regulate political parties because they are excluded from the definition of "government institution."
b. *PIPEDA* is the federal data protection statute regulating the private sector. It regulates entities engaged in "commercial activities. Political parties' political activities have traditionally been distinguished from commercial activities, which place them outside the ambit of *PIPEDA.*
c. The *Canada Elections Act* does not specifically regulate voter privacy. The Chief Electoral Officer of Canada recommended in 2013 that political parties should be subject to the same privacy protection principles as other Canadian institutions and that Elections Canada should have jurisdiction over privacy breaches. That proposal has not been implemented.
d. There is relatively little transparency regarding the voter data operations, voter database systems, or the interpretation and application of the privacy policies of political parties. As previous scholarship has highlighted, much of the knowledge around their use of data relies on anecdotal evidence. The technology involved in voter data procurement and analysis is in a constant state of flux and evolution. The use of technology permeates Canadian federal elections, but the particular technologies fluctuate from election to election. The latest scholarly literature gives an illuminating account as to the types of technologies that were in use up to the 2015 federal election. Such technologies may already be in the process of being updated or replaced, however, as new options emerge, particularly those developed in the United States. This report includes an account of the technology that is currently available to candidates in the United States, which indicates the technology that may shortly be available to Canadian political parties.
e. Voter data procurement and analysis are part of an increasing number of activities carried out by private sector organizations on behalf of political parties. These organizations mine, aggregate, and analyze data about voters, often using big data technologies that are

growing in sophistication. Little is known about these organizations. For example, it is unknown whether their operations are strictly Canadian or whether data about Canadian voters is also stored in the United States. Their activities may or may not be subject to *PIPEDA*, depending on whether their operations are qualified as political rather than commercial.

f. Voter information is also obtained through traditional means of voter contact operations, such as canvassers knocking on doors, observing voter signs, and recording donations. These traditional sources for voter information are now consolidated in parties' voter database systems, aggregated with other information, and potentially analyzed by third-party intermediaries.
g. The levels of interaction and cooperation between political parties at the federal, provincial, and municipal scales remain elusive. The literature primarily discusses political parties at the federal level..
h. Inappropriate use and mishandling of voter data has resulted in several privacy breaches. The Privacy Commissioner (as well as certain provincial privacy commissioners) and the Chief Elector Officer lack jurisdiction to protect individuals whose personal information has been misused.

Implications

The current state of knowledge identifies that: a) political parties hold large amount of data about individuals; b) this data includes personal information; c) there is a regulatory gap with respect to privacy legislation because neither the federal *Privacy Act* nor *PIPEDA* apply to the activities of political parties; d) there is a regulatory gap with respect to election law as no institution is tasked with overseeing the data activities of political parties; and e) voluntary self-regulation appears inadequate to protect personal information.

The first major implication of this knowledge is that there is significant risk of misuse or improper disclosure of sensitive, personal information. The second is that the legal and regulatory framework needs to be updated to take into account the new reality of political parties' extensive collection, storage, and use of voter personal information and the incorporation of more sophisticated technologies and big data analytics.

Results

- The legislative framework currently in place has been identified as inadequate to protect voter personal information and privacy in response to evolving political practices and new technologies.
- There is a lacuna in the legislation with respect to personal information obtained by political parties. Political activities do not fall under *PIPEDA*, because they are likely excluded from the definition of "commercial activities" in the legislation. Political parties are explicitly excluded from the definition of "government institutions" in the *Privacy Act* and are thus not subject to that legislation either.

- Numerous private sector entities collect, analyze, and sell voter data to political parties. It is unclear how the legislative framework applies to them or what privacy rules they apply to their own activities.
- Disclosure of the inner workings of voter management databases is strictly voluntary and has therefore been very limited, despite some high-profile journalistic accounts. Relatively little is known about the amount of data that parties have collected about voters, and how that data is safeguarded.
- Privacy breaches with voters' personal information have occurred but fall outside the jurisdiction of the federal Office of the Privacy Commissioner and Elections Canada.
- The sophistication of the technologies involved in aggregating data about voters is advancing rapidly. Social media, data analytic companies, and mobile device applications are but a few of the different platforms for voter data procurement.
- The algorithms by which data is analysed and by which inferences about voter behaviour are predicted are not well understood, nor is there detailed information about how accurate the predictions generated by the algorithms are with regard to how individuals will vote.
- The use of the most recent mobile applications for campaigns and geolocation tools, which include users' address books and location coordinates, magnify the kind and degree of voter information available to parties, and exacerbate the possibility and severity of voter data leaks.
- The knowledge on voter data is largely anecdotal. Though scholars such as Colin Bennett and journalists such as Susan Delacourt have amassed enough information to raise awareness of this issue, they have encouraged others to investigate with further research.
- A growing literature in the form of blogs and online news articles is attempting to keep voters current on the issue and provide advice to help protect voter privacy.[4] Put differently, voters are being urged to protect their own privacy in the absence of regulatory control.

State of Knowledge

To complete this Knowledge Synthesis Report, we surveyed the scholarly literature, journalistic accounts of current practices, the legal framework (including legislation and the practices of regulators), blogs, and the available information provided by political parties and private companies related to data and privacy. We identified two main challenges affecting the current state of knowledge as a whole: lack of access to information about the activities of political parties and the private sector companies that they work with; and proliferating technologies.

Regulatory Environment

Privacy concerns arise given the centrality of data to the activities of political parties, but also because those activities are generally not subject to federal privacy legislation regarding the

[4] Dave Maass, "Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election" *Electronic Frontier Foundation* (29 February 2016), https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election.

collection, storage, and use of voter data. The two main pieces of federal legislation with respect to privacy are the *Privacy Act*[5] and *PIPEDA*. [6] The *CEA*,[7]which regulates political parties and other political entities, provides parties with a right to obtain basic information about voters, but does not specifically regulate voter privacy. Finally, political parties are explicitly exempt from the *Telecommunications Act*[8] and are not subject to the *Access to Information Act*[9] by virtue of their exclusion from the list of government institutions subject to the Act in Schedule 1.

The only province to have enacted privacy protections that could apply specifically to voters is British Columbia. As such, the *British Columbia Personal Information Protection Act*[10] (hereinafter *BC PIPA*) and the *British Columbia Election Act*[11] are briefly consulted. The legislation of other provinces does not include specific voter privacy provisions, thereby likely creating a similar regulatory gap to that existing federally.

PIPEDA

PIPEDA lists ten fair information principles:[12] Accountability[13]; Identifying Purposes[14]; Consent[15]; Limiting Collection[16]; Limiting Use, Disclosure, and Retention[17]; Accuracy[18]; Safeguards[19]; Openness[20]; Individual Access[21]; Challenging Compliance[22]. The complete list with a concise description of each fair information principle can be found in Appendix F.

PIPEDA defines personal information as "information about an identifiable individual".[23] Political parties, though not explicitly exempted from this legislation, are not required to adhere to *PIPEDA* due to s. 4(1), which states that the legislation only applies to an organization that "collects, uses, or discloses in the course of *commercial activities*…."[24] *PIPEDA* defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."[25] Scholars and privacy advocates[26] have reinforced the

[5] *Privacy Act*, *supra* note 2.
[6] *PIPEDA*, *supra* note 1.
[7] *CEA*, *supra* note 3.
[8] *Telecommunications Act*, S.C. 1993, c. 38 at s. 41.7(1).
[9] *Access to Information Act*, R.S.C., 1985, c. A-1
[10] *Personal Information Protection Act*, S.B.C. 2003, c 63.
[11] *Election Act*, R.S.B.C. 1996, c 106.
[12] *PIPEDA* Fair Information Principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/.
[13] *PIPEDA*, *supra* note 1: Principle 1.
[14] *PIPEDA*, *supra* note 1: Principle 2.
[15] *PIPEDA*, *supra* note 1: Principle 3.
[16] *PIPEDA*, *supra* note 1: Principle 4.
[17] *PIPEDA*, *supra* note 1: Principle 5.
[18] *PIPEDA*, *supra* note 1: Principle 6.
[19] *PIPEDA*, *supra* note 1: Principle 7.
[20] *PIPEDA*, *supra* note 1: Principle 8.
[21] *PIPEDA*, *supra* note 1: Principle 9.
[22] *PIPEDA*, *supra* note 1: Principle 10.
[23] *PIPEDA*, *supra* note 1 at s. 2(1).
[24] *PIPEDA*, *supra* note 1 at s. 4(1) (emphasis added).
[25] *PIPEDA*, *supra* note 1 at s. 2(1).

fact that political parties do not engage in "commercial activities" because their activities and purposes are predominantly[27] political. Private sector data intermediaries involved in the collection, sharing, and selling of personal information about voters to political parties may also be outside the scope of *PIPEDA* if their activities are classified as political rather than commercial, although this conclusion has not been tested yet in the courts. The *Digital Privacy Act* 2015,[28] which amended certain provisions of *PIPEDA*, was silent on political parties and the data intermediaries involved in the process of obtaining and analysing voters' personal information.

Political parties have adopted their own internal privacy policies in light of the absence of legislative oversight. Political parties typically define "personal information" in their privacy policies consistently with the statutory definition in *PIPEDA*, but it is unclear how they interpret and apply it.

The *Privacy Act*

The definition of personal information provided in *PIPEDA* can be juxtaposed with the more comprehensive definition offered under the *Privacy Act*. The *Privacy Act* defines personal information as "information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

> (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,
> (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
> (c) any identifying number, symbol or other particular assigned to the individual,
> (d) the address, fingerprints or blood type of the individual…
> (f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence…
> (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual…"[29]

---

[26] Colin J. Bennett, Robin M. Bayley, Philip N. Howard, Daniel Kreiss, Susan Delacourt.
[27] In 2012, Bennett & Bayley highlighted that the merchandise sold on political parties' websites would theoretically qualify as commercial activity. However, being that this was a very small and insignificant part of their overall operations, the criterion of commercial activity is not triggered. Colin J. Bennett and Robin M. Bayley, "Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis," (16 March 2012), Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/ at 25.
[28] *Digital Privacy Act*, S.C. 2015, c. 32.
[29] *Privacy Act*, *supra* note 2 at s. 3.

The *Privacy Act*'s list, however, makes no reference to political information. Pursuant to s. 3, political parties are not regulated by the Act because they do not fall under the definition of "government institution."[30] An exhaustive list of government bodies that are regulated by the legislation is provided in Schedule 1 of the Act. Political parties are not included.

The *Canada Elections Act*

The process of voter data procurement begins with the *CEA*. Pursuant to s. 44(1), the Chief Electoral Officer is assigned the task of maintaining a National Register of Electors. Adopting the same definition for "personal information" in s. 2(1) of the *CEA*[31] as the one used in s. 3 of the *Privacy Act*, the Register contains the surname, given name, sex, date of birth, and civic and mailing addresses of each elector on the register.[32] The accuracy of the information is ensured via sharing agreements between federal and provincial bodies.[33] The Register is used by Elections Canada to administer elections[34] and is distributed to Members of Parliament (MPs) and registered political parties.[35]

Electors can choose to opt out of the Register.[36] Although information regarding sex and date of birth are not shared with political parties by Elections Canada,[37] some scholars have expressed uncertainty as to what other types of information are potentially shared.[38] Candidates and MPs may use the list of electors to communicate with voters, including for the purposes of soliciting contributions and recruiting party members.[39]The *CEA* provides some protection for electors' personal information. The *CEA* does not significantly restrict the use of personal information by political parties, however, if used for purposes related to elections. It states that:

> No person shall… (f) knowingly use personal information that is recorded in a list for a purpose other than (i) to enable registered parties, eligible parties, members or candidates to communicate with electors in accordance with section 110, or (ii) a federal election or referendum.[40]

The 2014 amendments to the *CEA* in the *Fair Elections Act* (*FEA)*[41] have implications for privacy. The *FEA* granted easier access to political parties to information about who has voted in an election, in the form of so-called "bingo cards."[42]

---

[30] *Privacy Act*, *supra* note 2 at s. 3.
[31] *CEA*, *supra* note 3 at s. 2(1).
[32] Elections Canada, "Description of the National Register of Electors," http://www.elections.ca/content.aspx?section=vot&dir=reg/des&document=index&lang=e.
[33] *CEA*, *supra* note 3 at s. 55(2).
[34] *CEA*, *supra* note 3 at ss. 93, 104.1, 105, 107, and 109.
[35] *CEA*, *supra* note 3 at s. 45.
[36] Elections Canada, "Description of the National Register of Electors," *supra* note 32.
[37] Elections Canada, "2015 Guidelines for Use of the Lists of Electors," http://www.elections.ca/content.aspx?section=pol&document=part3&dir=pol/loe&lang=e.
[38] Bennett & Bayley, *supra* note 27 at 13-14.
[39] *CEA*, *supra* note 3 at ss. 110 and 111.
[40] *CEA*, *supra* note 3 at s. 111(f).
[41] *Fair Elections Act*, S.C. 2014, c 12, s. 52.

The British Columbia *PIPA*

British Columbia has been a leading province on privacy protection for voters. British Columbia includes political parties under the B.C. *PIPA*, where an organization includes "a person, an unincorporated association, a trade union, a trust or a not for profit organization."[43] This definition means the legislation could reasonably be interpreted as applying to non-commercial activities and, hence, political activities, unlike *PIPEDA*, the federal legislation.[44]Bennett and Bayley argue that although "the law is untested…it can be argued that the political parties are also acting as non-profit organizations under B.C. *PIPA* and would be subject to the various requirements of the B.C. legislation with regards to their personal information practices within British Columbia."[45] However, it should be noted that under s. 3(2), the B.C. *PIPA* does not apply to "the collection, use or disclosure by a member or officer of the Legislature or Legislative Assembly of personal information that relates to the exercise of the functions of that member or officer." As such, the former B.C. Information and Privacy Commissioner, stating lack of jurisdiction as his reason, refused to investigate a complaint that the constituency office of a federal MP had improperly disclosed personal information.[46] Bennett and Bayley therefore conclude that "the distinction between information collected by elected officials, and that collected by federal and/or provincial political parties will sometimes be difficult to define, and will presumably raise interesting questions of jurisdiction for information and privacy commissioners".[47]

The *B.C. Election Act*

British Columbia recently amended their *Election Act* so political parties will be informed as to who voted in the last provincial election (but not how they voted).[48] The B.C. Privacy Commissioner declared the amendment regrettable and cautioned the public that the office lacked jurisdiction to enforce privacy protections on political parties.[49]

Voter Databases and Voter Management Systems

Political parties *capture, store, and use* voter personal information. Voter data is procured, analysed, used to predict voter behaviour, and then deployed to influence voters through techniques such as micro-targeting.

Political parties augment the basic data available to them through electoral legislation to create sophisticated voter profiles. This information is stored in voter management systems or

---

[42] Laura Payton, "Privacy Concerns Raised by Marc Mayrand Over Election Changes," *CBC* (6 March 2014, http://www.cbc.ca/news/politics/privacy-concerns-raised-by-marc-mayrand-over-election-changes-1.2563048.
[43] *BC PIPA*, *supra* note 10 at s. 1.
[44] Bennett & Bayley, *supra* note 27 at 26-27.
[45] Bennett & Bayley, *supra* note 27 at 26-27.
[46] Bennett & Bayley, *supra* note 27 at 27.
[47] Bennett & Bayley, *supra* note 27 at 27.
[48] *BC Election Act*, *supra* note 11 at s. 51(2).
[49] Office of the Information and Privacy Commissioner for British Columbia, "Statement from B.C. Information and Privacy Commissioner regarding proposed amendments to Bill 20 (Election Amendment Act)," Press Release (14 May 2015), https://www.oipc.bc.ca/news-releases/1792.

databases. Information on the workings of the voter management systems of political parties is largely anecdotal.[50] Membership lists have been kept by political parties for some time. Voter management databases, which include not only declared supporters but also voters who could be persuaded to be supporters, are a relatively new phenomenon.[51] The voter management systems contain information voluntarily submitted to the parties (e.g. through donations and contact with canvassers), but also information parties have acquired about individual voters from other sources, including data intermediaries. In the absence of regulatory oversight from any levels of government, it is increasingly difficult to assess the type and the amount of personally identifiable information that the databases contain.[52] Any information about the databases released by the political parties themselves has been entirely voluntary.[53]

The private sector produces sophisticated technology for the collection and analysis of voter information.[54] Most of the technologies involved in the capture, storage, and analysis of voter information originate in the United States. Canadian political parties borrow heavily from the software used in the United States. The Liberal Party of Canada uses similar software to that of the Democratic Party and the Conservative Party of Canada uses similar software to that of the Republican Party.

The first Canadian political party to use a sophisticated database was the Conservative Party of Canada. Built in 2004, their database is called the Constituent Information Management System (CIMS).[55] Basing the technology on the Voter Vault software of the Republican Party,[56] each voter in the database is assigned a score of -15 to +15.[57] The score is used to allow campaigns to effectively target undecided voters,[58] thereby producing more efficient campaign tools, such as walk lists, phone lists, email lists, and lawn sign allocations.[59] These "scores allow the campaign to focus their persuasion efforts on those voters most likely to be undecided".[60] The party's

[50] Bennett & Bayley, *supra* note 27 at 16.
[51] Colin J. Bennett, "The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies" (5 August 2013), 18:8 *First Monday*, http://firstmonday.org/ojs/index.php/fm/article/view/4789/3730. at 4.
[52] Bennett & Bayley, *supra* note 27 at 16.
[53] Philip N. Howard and Daniel Kreiss, "Political Parties and Voter Privacy: Australia, Canada, the United Kingdom and United States in Comparative Perspective" (2010) 15:12 *First Monday*, http://firstmonday.org/article/view/2975/2627 at 19.
[54] Bennett & Bayley, *supra* note 27 at 10-11.
[55] Conservative Party of Canada database, "Constituent Information Management System," https://apps.conservative.ca/login?rdr=https%3A%2F%2Fsupport.conservative.ca.
[56] Colin J. Bennett, "Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications," (2015)13:3/4 *Surveillance Society*, http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/voter_surv at 372-373.
[57] Bennett, "Trends in Voter Surveillance," *supra* note 56 at 373.
[58] Susan Delacourt, *Shopping For Votes: How Politicians Choose Us and We Choose Them*, Douglas & McIntyre (May 2016) at 246; Bennett, "Trends in Voter Surveillance," *supra* note 56 at 375. This example of a voter scorecard, however, is "dated and static", according to Bennett. As scoring systems are supplemented with far more information, scoring methods become more sophisticated as a result.
[59] Delacourt, *Shopping For Votes*, *supra* note 58 at 246-247 and 254-255; Bennett, "Trends in Voter Surveillance," *supra* note 56 at 373.
[60] Bennett, "Trends in Voter Surveillance," *supra* note 56 at 375.

efforts led to the creation of another voter management system in 2013 called C-Vote.[61] This initiative, however, did not survive and was discontinued by the Conservative Party, costing them millions of dollars.[62] Their most recent venture was to add a smartphone application to their database called "CIMS-to-go" (or C2G).[63]

Another piece of anecdotal evidence comes from an ex-Conservative politician who referred to the party's CIMS database during their 2004 campaign as an "unethical invasion of Canadians' privacy":[64]

> When I went to bang on doors in a neighborhood, my team dug into CIMS, and printed out a walk list for the poll. It told me who lived in each house on each street, along with any known information on what party they support. Every name was followed by a bar code. After talking to each person, I assessed their political leaning and marked it on my sheet. Back at the campaign office, teams of people keyed in the data while using bar code readers to match it up with voters' names.[65]

The Liberal Party of Canada, using a very similar platform as the Democratic Party's Voter Activation Network (VAN), built their own voter databases management system called the Liberalist.[66] It has the capacity to organize membership levels, list donors, sign requests and recognize supporters. It assists local campaign teams, events and volunteers. Additionally, it helps the party contact voters by telephone, email, canvassing or direct mail. The database can map out areas of support and opposition across ridings, track local and national issues, and facilitate grassroots campaigns. It accomplishes much of this by using Obama's neighbour-to-neighbour model, developing micro-targeted and demographic-specific messaging.[67] The Voter Activation Network's "MiniVAN"[68] app for the iPhone and iPad allows Liberal canvassers to transfer information from the central database.[69]

Of all the political parties' websites, the Liberalist is the most transparent about its operations, granting volunteers one of three levels of access: Basic, Intermediate, and Advanced.[70] It is

---

[61] Bennett, "Trends in Voter Surveillance," *supra* note 56 at 373.
[62] Bennett, "Trends in Voter Surveillance," *supra* note 56 at 373.
[63] "CIMS-To-Go" (C2G), https://c2g.conservative.ca/; Delacourt, *Shopping For Votes*, *supra* note 58 at 307.
[64] The Canadian Press, "Tory database draws ire of privacy experts," *CTV News* (18 October 2007), http://www.ctv.ca/CTVNews/QPeriod/20071018/tory_privacy_071018/.
[65] Bennett & Bayley, *supra* note 27 at 17.
[66] Liberal Party of Canada database, "Liberalist," http://liberalist.liberal.ca/; Delacourt, *Shopping For Votes*, *supra* note 58 at 286.
[67] Bennett & Bayley, *supra* note 27 at 16. This is the description provided by Bennett and Bayley. According to the Liberalist's website, however, it states: "Liberalist is our voter identification and relationship management system. Jointly developed by the Liberal Party of Canada and Voter Activation Network (VAN), Liberalist will allow our party to meet the demands of a 21st Century campaign and greatly increase our national voter tracking and messaging capabilities. Liberalist is based closely upon VAN's immensely successful VoteBuilder application, used by both Barack Obama and the Democratic National Committee to identify and track voters throughout the United States." See Liberalist, "What is Liberalist," http://liberalist.liberal.ca/what-is/.
[68] Colin Bennett, "So You Just Want Politicians to Leave You Alone? Good Luck With That," *iPolitics* (24 August 2015), http://ipolitics.ca/2015/08/24/so-you-just-want-politicians-to-leave-you-alone-good-luck-with-that/.
[69] "Liberalist," *supra* note 66.
[70] Bennett & Bayley, *supra* note 27 at 17.

further divided into two groups: MyVoters, offering the complete Elections Canada list of voters in each riding; and SharedContacts, offering information on individuals that may have had contact with the Liberal campaign in a specific district:[71]

a) "My Voters, also called the voter file, contains the complete Elections Canada list of all registered voters in your riding. The voter file is used to create lists of voters and to track information about voters."[72]
b) "Shared Contacts contains those who have had contact with the Liberal campaign in your district (or your committee) and anyone you or your campaign adds to this section. You also have search capability for limited profiles of contacts of the Liberal Party of Canada across the country through Quick Look Up. Individuals do not have to be a registered voters, nor do they have to be a resident of your riding to be added as your electoral district's (committee's) contact. Shared Contacts is used to house information about your volunteers, activists, supporters, staff and anyone who wants you to communicate with them. Under Shared Contacts, you build your contact list, reach out to your volunteers/donors, and manage your campaign's activities."[73]

The website also offers guidance on creating and managing lists, canvassing by door and telephone, robo-calling, emailing, managing events and volunteers, and formulating strategies for get-out-the-vote campaigns.[74]

The New Democratic Party currently uses a system called Populus,[75] cancelling their old system called NDP Vote.[76] Little is publicly known about this voter management system.

The overall impact of voter database cannot be confirmed,[77] yet most scholarly and journalistic accounts agree they are a critical ingredient in political success. A recent study reveals a marked growth in the number of technical positions in the employ of political parties.[78] This illustrates that over the past few election cycles, all political parties have upped the ante with respect to their data strategy.[79] In the United States, data plays such a central role that parties have threatened to ban candidates from accessing the party's national database if they do not join in the endorsement of the Presidential candidate.[80] Such accounts, in addition to the increasing

[71] Bennett & Bayley, *supra* note 27 at 17.
[72] "Liberalist," *supra* note 66.
[73] "Liberalist," *supra* note 66.
[74] Bennett & Bayley, *supra* note 27 at 17.
[75] New Democratic Party of Canada database, "Populus," https://populus.ndp.ca/foreAction/login/auth.
[76] Delacourt, *Shopping For Votes*, *supra* note 58 at 307. Colin Bennett, "They're Spying On You: How Party Databases Put Your Privacy at Risk," *iPolitics* (2015), https://ipolitics.ca/2015/09/01/theyre-spying-on-you-how-party-databases-put-your-privacy-at-risk/.
[77] Colin Bennett, "How Campaign 'Micro-Targeting' Works — And Why It Probably Doesn't," *iPolitics* (2015), http://ipolitics.ca/2015/09/09/how-campaign-micro-targeting-works-and-why-it-probably-doesnt/.
[78] Daniel Kreiss and Christopher Jasinski, "The Tech Industry Meets Presidential Politics: Explaining the Democratic Party's Technological Advantage in Electoral Campaigning, 2004–2012," (2016) *Political Communication* 1-19, http://www.tandfonline.com/doi/abs/10.1080/10584609.2015.1121941.
[79] Kreiss & Jasinski, *supra* note 78.
[80] Boris Heersink, "Reince Priebus Vowed to Punish Republicans Who Don't Support Trump: It's an Empty Threat," *The Washington Post* (20 September 2016), https://www.washingtonpost.com/news/monkey-cage/wp/2016/09/20/reince-priebus-vowed-to-punish-republicans-who-dont-support-trump-its-an-empty-threat/.

number of data intermediaries per election cycle and the advancement in technological sophistication of their data analytic strategies, add to the general conclusion that voter databases are essential to the operations of political parties.

Data Procurement

The process of voter data procurement began with individualized information made available by government bodies such as Elections Canada and Statistics Canada.[81] Pursuant to s. 44(1) of the *Canada Elections Act*, for instance, political parties are privy to information of electors, but strictly for elections purposes. Although sex and date of birth were not disclosed, it is unclear what other information is concealed from political parties. Adding to that, voter information can be collected from various sources, including traditional (low technology) means such as canvassing through telephone calls or on doorsteps, donor records, and by mere observation of addresses where election signs are posted.[82] Newer technologies have augmented these sources through the collection of voter information by mobile applications, social media, geolocation, and data intermediaries. As an example, supporters are able to donate directly from their smartphones, using mobile email or SMS.[83] Newer applications enable personal information to be collected not only about the user but also about a user's friends and family, through access to contact lists on mobile devices and social media.

Data Analysis and Data Intermediaries

The current state of politics is fostering a bourgeoning industry that systematically collects, stores, and analyzes voter data. With its proliferating level of sophistication, labels such as "voter surveillance,"[84] and political marketing[85] are emerging to acutely describe these practices. Since the 1990s, scholars have cautioned the public about government and private organizations' use of these data aggregators and the technology that supports them. Recent technological advances exacerbate these concerns.

Parties merge the voter information detailed above with information from public and private sources. For example, parties strive to collect geographically precise information for their database. The first source of such data is Statistics Canada, which provides parties with non-identifiable information. But database aggregation is not entirely performed by the political parties themselves. Marketing companies from the online consumer context are also involved. For example, Environics Analytics uses a system called "Prizm," which enables parties to "break down a population in a critical riding into a large number of types."[86] It was used by the Conservatives in 2006 in tandem with their own internal polling data.[87]

---

[81] Delacourt, *Shopping For Votes*, *supra* note 58 at 254.
[82] Bennett & Bayley, *supra* note 27 at 16.
[83] "Blue State Digital," https://tools.bluestatedigital.com/pages/quick-donate.
[84] Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008) at 119; Bennett, "Trends in Voter Surveillance," *supra* note 56 at 370-372.
[85] Delacourt, *Shopping For Votes*, *supra* note 58
[86] Bennett & Bayley, *supra* note 27 at 18; Howard & Kreiss, *supra* note 53 at 17-18. Since the time of this article's publication, the name of the system appears to have changed to "Prizm5". See Environics Analytics, Segmentation Systems at: http://www.environicsanalytics.ca/prizm5.
[87] Bennett & Bayley, *supra* note 27 at 18.

"Data intermediaries" is used as an umbrella term for companies that engage in collecting, analysing, and/or storing voter data, and includes "data brokers." While some companies market themselves specifically to candidates at the local level,[88] other are national. Some have been linked to numerous campaigns on an international scale,[89] implicating them in current US Presidential campaigns[90] as well as in the Brexit referendum.[91] Certain companies are deliberately partisan, and provide services to groups affiliated with one political side of the spectrum.[92]

The companies engaged in the acquisition and analysis of voter data are predominantly American. Not much has been revealed as to the permeation of their operations into the Canadian voter market, but scholars suspect they are being used by Canadian political parties. It is therefore prudent to explore the American landscape as a harbinger of what may soon affect the Canadian political marketing environment.

Much of the data intermediaries' strategy is to shroud their practices in secrecy to prevent competitive duplication. Basic information is available on the data intermediaries' websites while other information has been obtained by privacy advocates anecdotally. Detailed accounts of any potential privacy-intrusive practices are not yet available.

Although some data intermediary companies offer political intelligence as an explicit part of their services, most advertise their services more generally as consumer insight companies that offer marketing services that are not specific to political parties, candidates, or campaigns. Knowledge of their involvement is therefore often provided by their reference in scholarship or news articles.

Some notable practices include smartphone applications, which could be downloaded by canvassers to give them access to a list of neighbours that had also downloaded the app, interactive maps, the ability to share news, photos, and videos, as well as real-time reporting that details how each conversation went.[93] Targeted online advertising software provide full digital media services.[94] Services also accommodate campaigns with sophisticated market segmentation strategies that align online and offline behaviour.[95]

---

[88] "Nationbuilder," www.nationbuilder.com.
[89] "uCampaign," https://ucampaignapp.com.
[90] uCampaign developed apps for both the Donald J. Trump ("America First," https://www.donaldjtrump.com/app.) and Senator Ted Cruz (Cruz Crews; https://www.tedcruz.org/news/ted-cruzs-official-cruz-crew-campaign-app-tops-2016-field/.).
[91] David Z. Morris, "With Trump's Campaign App, There's No Wall Protecting Your Contact Data," *Fortune* (28 August 2016), http://fortune.com/2016/08/28/trump-campaign-app-data-security/.
[92] "Data Trust," http://thedatatrust.com., "TargetPoint Consulting," http://www.targetpointconsulting.com., "Cambridge Analytica," https://cambridgeanalytica.org., and "i360," http://www.i-360.com, an initiative by the Koch brothers, are companies that actively work in concert with the Republican National Committee for voter data management.
[93] "Organizing for America App for the i-Phone,"a product used by the Obama 2012 campaign. Though it is no longer in service, it was once available online at http://my.barackobama.com/page/content/iphone2010/.
[94] "Google's Political Campaign Toolkit," http://www.google.com/ads/politicaltoolkit/.
[95] A product called Segment Metrix 2.0 from Comscore, http://www.comscore.com/Products_Services/Product_Index/Segment_Metrix_2.0.

The potential intrusiveness is further highlighted by companies that can track phones to determine voter preference.[96]

> In order to register, you will be asked to provide certain identifying information, including your phone number. In order to maximize your experience with our website and America First and to provide its features and services, we may periodically access your contact list and/or address book on your mobile device. You hereby give your express consent to access your contact list and/or address book.[97]

Individual information can be procured from a phone's internet browser that uses an advertising network. The internet advertising is enabled by an auction triggered when an individual opens an app or looks at a browser page. The information sent to potential advertisers can include an identifying code as well as the individual's precise location (latitude and longitude).[98]

> While the America First application is in use, we may keep track of your device's geographic location so that we can connect you to other America First users based on your particular geographic location.[99]

One such company boasts their trove of information amounts to a "10 terabyte database – enough to fill more than 2,100 DVDs – that contains as many as 5,000 biographical details about the 240 million Americans of voting age," with sophisticated algorithms capable of predicting personality traits.[100]

> We use various technologies to collect information, and this may include sending cookies to your computer or mobile device. Cookies are small data files stored on your hard drive or in device memory that helps us to improve our Sites and your experience, see which areas and features of our Sites are popular and count visits. We may also collect information using web beacons (also known as "tracking pixels" or "clear GIFs"). Web beacons are electronic images that may be used in our Sites or emails and help deliver cookies, count visits, understand usage and campaign effectiveness and determine whether an email has been opened and acted upon. For more information about cookies, and how to disable them, please see "Your Choices" below.[101]

The newer apps are a hybrid between a social network and a game, where users can collect points, donate money to campaigns, and broadcast their support for candidates through social media.[102] This builds on earlier concepts that aimed to create a gaming experience for voters.[103]

---

[96] "Dstillery," http://dstillery.com.
[97] "America First" Privacy Policy, https://www.donaldjtrump.com/pages/app-privacy.
[98] The information regarding the functions of this company are given anecdotally in Kashmir Hill, "How this company tracked 16,000 Iowa caucus-goers via their phones," *Fusion* (12 February 2016), http://fusion.net/story/268108/dstillery-clever-tracking-trick/.
[99] "America First" Privacy Policy, *supra* note 97.
[100] Maass, *supra* note 4. This is a description of Cambridge Analytica's services, https://cambridgeanalytica.org.
[101] "Hillary For America" Privacy Policy, https://www.hillaryclinton.com/page/privacy-policy/.
[102] Caitlin Dickson. "Trump launches America First app, a competitive social network," *Yahoo!Tech* (26 August 2016), http://www.yahoo.com/tech/trump-campaign-launches-america-first-000000643.html.

Users are also asked to login using their email, phone number, or Facebook account, where the latter grants the candidate's campaign access to personal information available on Facebook as well as a list of their friends and family (who do not have the opportunity to consent).[104]

> The Sites may offer social sharing features and other integrated tools (such as the Facebook "Like" button), which let you share actions you take on our Sites with other media, and vice versa. The use of such features enables the sharing of information with your friends or the public, depending on the settings you establish with the entity that provides the social sharing feature. For more information about the purpose and scope of data collection and processing in connection with social sharing features, please visit the privacy policies of the entities that provide these features.[105]

Some of the more seasoned companies promote their ability to merge publicly available data with their own privately stored data.[106] Such companies have been in operation for decades.[107] Their services, however, have evolved to include scoring systems integrated to consider "voter registration, participation in past elections, political giving, property and neighbourhood information, periodic surveys, door-to-door contacts and other field work".[108]

> We may allow third parties to use cookies, web beacons, or other technologies or otherwise collect information about you in order to provide analytics and advertising services, including serving ads on the Sites or on other sites based on your visits to the Sites and other sites across the Internet and across various mobile applications. These entities may collect or receive information about your use of the Sites and other websites and mobile applications, including your IP address, browser, device information, pages viewed, time spent on pages, links clicked and conversion information. This information may be used by HFA and others to, among other things, analyze and track data, determine the popularity of certain content, deliver advertising and content targeted to your interests and better understand your online activity.[109]

---

[103] "Blue State Digital," www.5ivepoints.com. This website does not appear to be in operation; see Bennett, "Trends in Voter Surveillance," *supra* note 56 at 378-379.
[104] Michael Biesecker and Julie Bykowicz, "Cruz app data collection helps campaign read minds of voters," *The Associated Press* (11 February 2016), http://bigstory.ap.org/article/2db0fc93cf664a63909e26e708e91c67/cruz-app-data-collection-helps-campaign-read-minds-voters.
[105] "Hillary For America" Privacy Policy, *supra* note 101.
[106] "Catalist," http://www.catalist.us/about/., "Aristotle", http://aristotle.com, "Response Unlimited," http://www.responseunlimited.com.
[107] Maass, *supra* note 4.
[108] In describing "Acxiom Corporation", http://www.acxiom.com. See David Z. Morris, "With Trump's Campaign App, There's No Wall Protecting Your Contact Data," *Bloomberg Politics* (28 August 2016), https://www.bloomberg.com/politics/articles/2016-05-31/republicans-fight-to-regain-voter-data-parity-with-democrats.
[109] "Hillary For America" Privacy Policy, *supra* note 101.

Services that call themselves a "platform for social action" allow users to develop email lists in order to target fundraising and advocacy efforts.[110] Other socially-oriented apps enable their clients to "match their Facebook friends to the voter file as they take part in everyday campaign activities like voter identification and persuasion, grassroots fundraising, crowd building, volunteer recruitment, and get-out-the vote activities."[111]

Some companies employ geo-positioning software to trace the precise routes of canvassers and volunteers, eventually merging the information procured on the ground with the party databases.[112]

Data Use

The literature suggests that political parties, as well as private companies that potentially possess their own databases, create individualized portfolios (or digital dossiers) that assist with the reading and prediction of voter behaviour. Although the accuracy of the digital dossiers is unknown, parties use them in a variety of ways, including the creation of integrated voter management platforms,[113] and micro-targeting to influence voters. Micro-targeting "uses whatever individual-level information is available and combines it with demographic, geographic and marketing data about those individuals to build statistical models to better understand the attitudes and behaviours of others."[114] Parties also increasingly gather information from social media[115] and use it to shape their activities.

It is unclear to what extent information is shared between federal, provincial, and municipal campaigns or political parties. Bennett found that federally mined voter data was sold to local campaigns,[116] though this has not been verified. Provincial parties sometimes voluntarily subscribe to federal party databases.[117] The Liberal Party of Ontario switched from their old database to the federally used Liberalist.[118]

Political parties' use of databases, voter management systems, and data intermediaries raises several privacy concerns, especially with regard to how the data is collected, how it is *used*, how extensively it is *shared* within political parties, and who has *access* to it. With unconfirmed reports acting as the sole source of information, the impact on voter privacy remains uncertain.

---

[110] "Actionsprout," www.actionsprout.com.
[111] "NGP VAN," https://www.ngpvan.com/.
[112] Describing "Footwork App," www.gofootwork.com; see Bennett, "Trends in Voter Surveillance," *supra* note 56 at 378. This website is no longer active and their Twitter account was last updated in 2013 (https://twitter.com/etpio).
[113] Bennett, "Trends in Voter Surveillance," *supra* note 56 372-373.
[114] Bennett, "Trends in Voter Surveillance," *supra* note 56 at 376. See also Sasha Issenberg. "Obama's White Whale: How the campaign's top-secret project Narwhal could change this race, and many to come," *Slate* (15 February 2012), http://www.slate.com/articles/news_and_politics/victory_lab/2012/02/project_narwhal_how_a_top_secret_obama_campaign_program_could_change_the_2012_race_.html.
[115] Bennett, "Trends in Voter Surveillance," *supra* note 56 at 377.
[116] Bennett, "Trends in Voter Surveillance," *supra* note 56 at 370-372.
[117] Adrian Morrow, "Ontario Liberals to target ethnic voters with demographic database software," *The Globe and Mail (*14 April 2014), http://www.theglobeandmail.com/news/politics/database-helps-liberals-woo-ethnic-vote/article17953049/.
[118] Morrow, *supra* note 117.

Together these activities could result in the access, collection, and storage of substantial amounts of personal information about voters, including their locations and their contacts.[119] This increases the scope of the privacy risks if there is a security breach.[120]

For example, privacy concerns have been raised with regard to data collection and the relationship between the official role of Members of Parliament and their partisan responsibilities. Significantly, it is generally unclear whether parties distinguish between constituent service records accumulated by Members of Parliament in performance of their official duties and data amassed for political purposes.[121] There is evidence that the Conservative Party, with the Constituent Information Management System (CIMS), makes use of a single database that amalgamates both activities.[122]

The extent of *disclosure* of personal information and access to it is also a potential issue. The most current information in this respect is related to the Conservative Party's CIMS database. Local offices of the Conservative Party pay a $2000 fee to the national party for a database of voters in their respective districts, which includes "geo- and psychographic surveys, polling, and personal contacts."[123] In the Conservative Party website, the privacy statement reads: "The Conservative Party does not actively seek to collect the personal information of Canadians. Nor does it collect any personal information about you without your permission." It proceeds to state, however, that:

> As a national organization with a riding-based membership system, your personal information may also be disclosed to our local riding associations, who may also communicate with you. Additionally, non-personal information may be collected by the Conservative Party through the use of cookies, including third-party cookies. Cookies allow us to track how people are using our site and help us deliver better content to our visitors. We may use this information, in aggregate, to improve our site or to assist in advertising.[124]

Self-Regulation

In the absence of legislative requirements, political parties engage in self-regulation with regard to privacy. The privacy policies of political parties are thus relevant. All of the major federal parties, the Liberal Party of Canada, Conservative Party of Canada, New Democratic Party, and Green Party of Canada, have privacy policies on their websites. These policies, however, do not explicitly reference the use of their respective voter management systems and offer relatively little detail on the type of data that is stored in their databases and the manner in which the data is used. Political parties' privacy policies It is unknown whether the privacy policies pertain solely

[119] Morris, *supra* note 91.
[120] "Donald Trump's Campaign Was Hacked", *Fortune* (19 August 2016), http://fortune.com/video/2016/08/19/donald-trumps-campaign-was-hacked/.
[121] Howard & Kreiss, *supra* note 53 at 17.
[122] Howard & Kreiss, *supra* note 53 at 17.
[123] Howard & Kreiss, *supra* note 53 at 17.
[124] Conservative Party of Canada Privacy Policy, http://www.conservative.ca/privacy-policy/.

to the websites of the political parties, or whether the policies encompass a range of the political parties' services, including the voter management systems.[125]

For example, the Green Party of Canada's privacy policy states:

> *As a registered federal political party, the Green Party of Canada requires your assistance in providing us with your personal information to fulfill certain legal obligations. If you become a member, you must provide certain information, which is added to our internal membership database that by law must be maintained. The information maintained in the database includes:*
>
> - *Member number;*
> - *Member name, address and telephone number;*
> - *Amount of member donation(s);*
> - *Date on which the member registered as a member of the Green Party of Canada, and/or made (a) donation(s);*
> - *Date on which any person ceased to be a member.*[126]

However, the parties' level of compliance with their own internal policies is unclear, as are the potential enforcement mechanisms. The parties' privacy policies accord individuals some rights consistent with fair information principles, modified to account for federal elections requirements such as compliance with record keeping pertaining to campaign financing. For example, federal privacy legislation provides qualified rights to an individual to request that her own personal information be deleted. The Green Party of Canada's policy with respect to deleting information personal information states that:

> We will not, without your consent, use your personal information for any purpose other than as described in this privacy policy, *except where permitted or required by applicable legislation*. For example, under the Canada Elections Act, we are required to provide Elections Canada with our donors' names, addresses and contribution amounts.[127] [emphasis added]
>
> If you wish to have any of your personal information removed from our databases, or if you no longer want us to send any further communications to you, please send an e-mail to membership@greenparty.ca with your request. *Please note, however, that as a federal political party we are required by law to maintain certain information about our members, as noted above. We may be required by law to maintain this information for a period of time after a member has terminated his or her membership.*[128] [emphasis added]

[125] Colin Bennett, "So You Just Want Politicians to Leave You Alone? Good Luck With That," *iPolitics* (2015), http://ipolitics.ca/2015/08/24/so-you-just-want-politicians-to-leave-you-alone-good-luck-with-that/.
[126] Green Party of Canada Privacy Policy, https://www.greenparty.ca/en/privacy.
[127] Liberal Party of Canada Privacy Policy, https://www.liberal.ca/privacy/.
[128] Green Party of Canada Privacy Policy, *supra* note 126.

The parties' website privacy policies are explicit about downstream *uses* of personal information, such as whether voter data may be shared with or sold to data intermediaries. For example, the Green Party's website privacy policy states with respect to use of personal information:

> We use this data, in aggregate form only, to compile statistics and reports for the Green Party of Canada's use, and improve the online experience for all visitors. *We reserve the right to provide general descriptions or portions of this aggregate information to vendors, consultants, partner NGOs or news services.* Such uses of the data in this fashion would typically be to plan site architecture improvements or to measure public interest in our site.[129] [emphasis added]

> As we are a federal party, we may share your information internally within our national organization, including with NDP riding associations.[130]

> The information contained in the database can only be used for official Green Party business such as informational mailings, internal election materials, and other correspondence. *The Green Party of Canada does not sell, rent, or lend our membership lists to anyone.*[131]

The Liberal Party's policy states that voter information can be shared with local ridings and other associations and organizations:

> Given that the Liberal Party is a national organization, personal information may be shared internally, for instance between the Party and its electoral district associations (riding associations). In addition, we may engage third party providers to perform tasks on our behalf such as processing your donation, making phone calls and providing technical services to our website. When information is shared with third parties for these purposes, we include privacy protective clauses in written contracts to help safeguard personal information.[132]

But parties' privacy policies are silent on data *procurement*, such as whether personal information is obtained from third-party aggregators. It is also not clear what data security measures (encryption, prohibiting data transfer to USB keys) political parties are currently using to protect voters' personal information against hacking and other data leaks. With much of the database management labour work delegated to private companies, some authors query: "If they fail to state a policy on selling data, does that mean that they do sell it, that they reserve the right to sell it, or that they neglected to develop a policy on selling it?" and "what exactly does it mean when a party pledges to not surrender data to a 'third party'?"[133]

---

[129] Green Party of Canada Privacy Policy, *supra* note 126.
[130] New Democratic Party of Canada Privacy Policy, http://www.ndp.ca/privacy.
[131] Green Party of Canada Privacy Policy, *supra* note 126.
[132] Liberal Party of Canada Privacy Policy, *supra* note 128.
[133] Howard & Kreiss, *supra* note 53 at 28.

Voter Privacy Breaches

Labeled as a form of surveillance,[134] the level of information obtained by political parties through these practices is unprecedented. A number of instances where voters' personal information was not protected have been reported in the media. While not all of these involve the voter management systems, they do indicate the risks involved when large amounts of voter personal information are collected. These privacy risks are exacerbated by the lack of regulatory oversight, enforcement, and remedies.

The most notorious of such breaches was the robo-calls incident, which prompted a white paper,[135] a roundtable,[136] an unsuccessful legal challenge to overturn disputed electoral results in ridings where they had occurred,[137] and a criminal conviction in the riding of Guelph.[138] The reports prompted calls for increased privacy measures, resorting to very few substantive recommendations that would prevent future incidents. In the disputed elections case, the judge found that:

> Access to a party's central database is carefully controlled. The calls at issue in these proceedings are most likely to have been organized by a person or persons with: i) access to the central information system of a political party that included contact information about non-supporters; ii) the financial resources to contract voice and automated service providers to make such calls; and iii) the authority to make such decisions.[139]

In 2006, Conservative Party MP Cheryl Gallant sent birthday cards to her constituents using data procured from their passport applications.[140] Due to the fact that the Privacy Commissioner did not have jurisdiction to investigate, the Office of the Ethics Commissioner undertook the matter under the Conflict of Interest Code for Members of the House of Commons. Although it was concluded that no breach occurred because no 'private interest' was advanced, the Ethics Commissioner did state the following:

> As legislators, members should be guided by the principles they themselves have established in the various pieces of legislation related to the privacy of information…That is, personal information should only be

[134] Solove, "Understanding Privacy", *supra* note 84 at 119; Colin J. Bennett, "Data Point – What Political Parties Know About You" (2013) 34:2 *Policy Options* 51, http://policyoptions.irpp.org/wp-content/uploads/sites/2/2013/02/data-point.pdf at 51-53.
[135] Chief Electoral Officer of Canada, "Preventing Deceptive Communications with Electors: Recommendations from the Chief Electoral Officer of Canada Following the 41st General Election," (2013) *Library and Archives Canada Cataloguing in Publication*, http://www.elections.ca/res/rep/off/comm/comm_e.pdf.
[136] "Issues Arising from Improper Communications with Electors: Round Table Report," (March 2013) *IRPP*, http://irpp.org/wp-content/uploads/assets/research/strengthening-canadian-democracy/communications-with-electors/roundtable-031513.pdf.
[137] *McEwing v Canada (AG)*, 2013 FC 525.
[138] Diana Mehta, "Ex-Tory staffer Michael Sona's sentence upheld in robocalls case," *The Toronto Star* (9 June 2016), https://www.thestar.com/news/canada/2016/06/09/ex-tory-staffer-michael-sonas-sentence-upheld-in-robocalls-case.html.
[139] *McEwing*, *supra* note 140 at para 183.
[140] Bennett & Bayley, *supra* note 27 at 21.

> used for the purpose for which it is gathered, or for a use consistent with that purpose.[141]

Again in 2006, voter names and addresses were recovered in the office of a Toronto cell of the Tamil Tigers during an RCMP raid.[142] The Prime Minister's Office was also subject to such controversies when Rosh Hashanah cards were sent to his supporters with Jewish sounding names because religious beliefs are considered to be sensitive information.[143] This event, as well, fell outside of the Privacy Commissioner's jurisdiction.[144] In 2011, an email revealing the names, addresses, phone numbers, and emails of six thousand constituents was mistakenly sent to an environmental activist by a Conservative candidate.[145] That same year, an individual's complaint to her MP about receiving Conservative campaign literature prompted a Conservative party spokesman to respond to the complaint by stating that it was party policy to remove a name from distribution lists on request.[146] The Conservative Party was also the victim of hackers, stealing online donor information from the Conservative's website.[147] Again in 2011, during a reform of election laws, the Nova Scotia chief electoral office provided political parties with voters' year of birth.[148] In 2012, two USB keys containing over 2 million voter files from Elections Ontario went missing.[149] Finally, "robo-calling," the act leading to voter suppression, was investigated by Elections Canada and the RCMP.[150]

In 2013, an investigation was conducted by the Information and Privacy Commissioner for BC.[151] It pertained to the Liberal Party's Multicultural Strategic Outreach Plan and intended to "to determine whether there was sharing of personal information between the government and the BC Liberal Party, and if there was, whether this sharing was authorized under provincial privacy law".[152] Although no wrongdoing of the mishandling of personal information was found, the Commissioner did forward recommendations.[153] The recommendation can be found in the Appendix. The BC Commissioner has shown a proactive approach, also investigating the NDP

---

[141] Bennett & Bayley, *supra* note 27 at 21.
[142] Howard & Kreiss, *supra* note 53 at 12-13; Bennett & Bayley, *supra* note 27 at 23. This incident was mentioned in a news release by the Privacy Commissioner. They also found the following: "some voter lists simply vanished during elections and by-elections; Elections Canada collects too much personal information on voters, including on teenagers too young to vote; and Canadians are not fully informed about how their personal information will be used". See Office of the Privacy Commissioner of Canada, "Audit reveals privacy gaps at federal agencies," News Release (12 February 2009), https://www.priv.gc.ca/media/nr-c/2009/nr-c_090212_e.asp.
[143] Howard & Kreiss, *supra* note 53 at 17; Bennett & Bayley, *supra* note 27 at 23.
[144] Bennett & Bayley, *supra* note 27 at 23.
[145] Bennett & Bayley, *supra* note 27 at 23.
[146] Bennett & Bayley, *supra* note 27 at 23-24.
[147] Bennett, "The Politics of Privacy," *supra* note 51 at 13.
[148] Bennett & Bayley, *supra* note 27 at 23.
[149] Bennett, "The Politics of Privacy," *supra* note 51 at 13.
[150] Bennett & Bayley, *supra* note 27 at 24.
[151] Office of the Information and Privacy Commissioner for British Columbia, "Sharing of Personal Information as part of the Draft Multicultural Strategic Outreach Plan: Government of British Columbia and the BC Liberal Party," Investigation Report F13-04 (1 August 2013), https://www.oipc.bc.ca/investigation-reports/1559.
[152] Information and Privacy Commissioner for BC, "Multicultural Strategic Outreach Plan," *supra* note 154 at 4.
[153] Information and Privacy Commissioner for BC, "Multicultural Strategic Outreach Plan," *supra* note 154 at 25.

on allegations that candidates were asked to disclose their social media passwords to party leaders.[154] This investigation, however, did not pertain to voters' personal information.

Legislative Lacuna and Reform

Political parties are not governed by the *Privacy Act* because they are not "government." Political parties are not governed by *PIPEDA* because their activities are political rather than "commercial." Furthermore, legislative exemptions appear to also apply to campaign volunteers and canvassers, who may have had insufficient privacy training. Lastly, data intermediaries may also not be covered by privacy legislation when voter data is submitted to political parties for advertising purposes, even where the data is sold.

Both privacy and elections law experts have noted that there is a significant regulatory gap with respect to the protection of voter's personal information by political parties. Canada's Office of the Privacy Commissioner, the Chief Electoral Officer, and scholars have made recent statements indicating that legislative oversight is needed.

The most prolific scholar on the lack of privacy protection for voters' personal information is Colin Bennett, who has highlighted the issue in a series of articles in iPolitics. In 2012 in a report for the Office of the Privacy Commissioner of Canada, he and Robin Bayley did a comparative study of the federal political parties' protections for personal information, examining how and whether the legal frameworks apply to political parties, which emphasized the legislative gaps and uncertainties in the current regulatory structure.

In a 2013 report, the Chief Electoral Officer of Canada recommended that legislation be amended to grant Elections Canada jurisdiction over privacy breaches. The report states:

> In order to preserve the confidence of Canadians in the political entities with whom they deal, and in order to better protect the privacy of Canadian electors dealing with political entities, it is recommended that the Canada Elections Act be amended to provide a mechanism by which the application of privacy protection principles governing most Canadian institutions and organizations would be extended to political parties.
>
> The Act should also be amended to require that political parties demonstrate due diligence when giving access to their voter databases.[155]

The Chief Electoral Officer held that "there are privacy risks associated with these databases," where political parties "not only handle large amounts of personal information, but also share this information with a small army of volunteers and local campaign workers."[156]

Agreeing with Elections Canada's report, the Office of the Privacy Commissioner of Canada responded:

---

[154] Office of the Information and Privacy Commissioner for British Columbia, "Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's use of social media and passwords to evaluate candidates," https://www.oipc.bc.ca/mediation-summaries/1399.
[155] Chief Electoral Officer of Canada, "Preventing Deceptive Communications," *supra* note 137 at 32.
[156] Chief Electoral Officer of Canada, "Preventing Deceptive Communications," *supra* note 137 at 20.

> We welcome the report from Elections Canada, which highlights the fact that there is currently a gap in coverage under federal privacy legislation and suggests measures to address this gap. We feel this is an issue that warrants public discussion…We are pleased to see a recommendation that political parties should be required to meet these standards.[157]

Approach & Methodology

The project gathered research related to:

- the legal framework governing personal information held by political parties in Canada about voters;
- political parties' practices with respect to data procurement, analysis, and use of voters' personal information, including the use of big data analytics and data intermediaries.

Our research looked to catalogue laws that potentially regulate political parties' collection, use and disclosure of voters' personal information, focusing on privacy laws and election laws. Referring to CanLII, Quicklaw, and Justice Laws website, we consolidated sources of all statutes and regulations in Canada. Further, we conducted a comprehensive search of literature on big data techniques and voter management systems and how they are used by political parties. In so doing, we examined the legal, policy, and ethical issues in the scholarly literature on privacy and big data. Relying on databases such as Lexis, Westlaw, SSRN, HeinOnline, Academic Search, and Google Scholar, we assessed the state of knowledge on big data and politics. In the final stages, we consulted credible news articles to gauge the next level technology that is originating in the 2016 presidential race in the United States. This final step was of critical importance, allowing us to gain a sense of the technologies that will potentially be emerging in the next election cycle.

Additional Resources

Please refer to references in the bibliography. In addition, please refer to the material included in the appendices:

a) Privacy Policy of the Conservative Party of Canada
b) Privacy Policy of the Green Party of Canada
c) Privacy Policy of the Liberal Party of Canada
d) Privacy Policy of the New Democratic Party of Canada
e) Leak from the Jeb Bush Presidential campaign
f) Recommendations by the Information and Privacy Commissioner for BC

[157] Office of the Privacy Commissioner of Canada, "Statement from the Office of the Privacy Commissioner of Canada Regarding a Report by Elections Canada," Press Release (27 March 2013), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2013/nr-c_130327/.

Further Research

Gaps in the Law

- The current federal privacy legislation applying to the public and private sectors does not cover federal political parties with respect to voters' personal information. The *Canada Elections Act* does not do so either, except with respect to the basic information contained in the Registry of Electors. The Chief Electoral Officer, has identified this gap in the legal framework.
- In the absence of legislative requirements, political parties self-regulate. The scholarly literature has highlighted the flaws in the model of self-regulation currently being employed. Analysis of the effectiveness of the privacy policies of political parties is hindered by lack of evidence with regard to how they are interpreted and enforced by the parties themselves.
- Current scholarship has identified a further gap in the legal framework with regard to the sharing of information across federal, provincial, and municipal levels.
- It is unclear how the existing legislation designed to protect privacy and impose fair information principles applies to private sector entities that work with political parties on data collection, use, and analysis.
- There are similar legal gaps in provincial privacy and electoral legislation, with the notable exception of political information under the *B.C. PIPA*. The scholarship, however, has largely focused on the practices of federal parties' voter management systems and focuses predominantly on federal legislation. Although some mention is made of provincial privacy legislation, specifically B.C. *PIPA*, there has not been a detailed study of provincial election laws. It is unclear whether or not any privacy breaches of provincial parties' voter management systems would be the jurisdiction of the provincial privacy watchdogs.
- Another legal gap is with regard to investigation and enforcement. If privacy rules were to be imposed on political parties, either the Chief Electoral Officer or the Office of the Privacy Commissioner could potentially be granted the statutory authority to investigate privacy breaches and impose penalties.

Gaps in the Scholarship

- The most comprehensive treatments to date are by academic Colin Bennett and journalist Susan Delacourt. The technologies available to political parties and their practices both progress quickly, however, meaning that there are inevitably gaps in the scholarship. Gaps in the scholarship exist with regard to:

- What new technologies are being used, given their constant updating and evolution, especially after the 2015 federal election;
- How parties are using the data at their disposal, given the lack of disclosure of these practices;
- How parties interpret and enforce their own internal privacy policies;
- The role of private sector data companies working with political parties;
- Best practices for self-regulation by parties; and
- Comprehensive studies of possible legal regimes to replace self-regulation, including jurisdiction and enforcement.

Gaps in Knowledge Regarding Technology

- Bennett's last scholarly article on this issue was published in 2014. With the 2015 Canadian federal election hailed as a big victory for big data companies,[158] and given the nature of secrecy surrounding the use of such technologies by political parties, the emergence of technologies between the 2015 Canadian federal elections and the 2016 American presidential election will remain unknown until further research is undertaken.

Knowledge Mobilization

Our knowledge mobilization plan for the remaining term of the Grant will involve engagement with the academic community, across relevant disciplines and the dissemination of results with policy makers and broader public audiences. The results will be shared through a variety of means, including:

- a public-lecture at a speaker series co-sponsored by the Public Law group and Centre for Law, Society, and Technology at the University of Ottawa's Faculty of Law.
- publication of the Report and distribution to relevant stakeholders, users, and academic experts
- partnership with a policy journal with a wide-online readership for dissemination of the key recommendations;
- drafting FAQs based on the report for distribution to civil society groups;
- integration of the topic into our law classes on technology law, privacy law and electoral law; and
- dissemination through social media such as a blog posting on the Centre for Law, Society and Technology website and through personal and Faculty of Law twitter accounts.

Conclusion

New technologies are rapidly shifting the practices of political parties around the collection, use, storage, and analysis of data composed of the personal information of Canadians. The federal

[158] Susan Delacourt, "How the Big Red Machine Became the Big Data Machine," *The Toronto Star* (21 May 2016), https://www.thestar.com/news/insight/2016/05/21/how-the-big-red-machine-became-the-big-data-machine.html.

legal framework has not kept up with the expectations of Canadians that their privacy will be protected by all private and public sector actors, including political parties. The literature has identified significant risks in the model of voluntary self-regulation, though lack of knowledge about these policies hinders a full analysis. There are gaps in the existing scholarship with regard to what new technologies are being used, the exact practices of parties, the approaches of other democracies, and the alternative legal regimes and enforcement mechanisms that might reduce the risks of privacy breaches. Significant research remains to be done to develop alternative legal regimes and enforcement mechanisms in light of fair information principles and the best practices for the regulation of political parties. There is also significant work to be done to assess the broader implications for democracy of big data politics.

References and Bibliography

Cases

McEwing v Canada (AG), 2013 FC 525.

Legislation

Access to Information Act, R.S.C., 1985, c. A-1.

Digital Privacy Act, S.C. 2015, c. 32.

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

Election Act, R.S.B.C 1996, c. 106.

Personal Information Protection Act, S.B.C 2003 c. 63

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

Privacy Act, R.S.C. 1985, c P-21.

Telecommunications Act, S.C. 1993, c. 38.

Literature

Bennett, Colin J., "Data Point – What Political Parties Know About You," (2013) 34:2 *Policy Options*, 51, http://policyoptions.irpp.org/wp-content/uploads/sites/2/2013/02/data-point.pdf.

----. "How Campaign 'Micro-Targeting' Works — and Why It Probably Doesn't," *iPolitics* (2015), http://ipolitics.ca/2015/09/09/how-campaign-micro-targeting-works-and-why-it-probably-doesnt/.

----. "So You Just Want Politicians to Leave You Alone? Good Luck With That," *iPolitics* (24 August 2015), http://ipolitics.ca/2015/08/24/so-you-just-want-politicians-to-leave-you-alone-good-luck-with-that/.

----. "The Politics of Privacy and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies," (5 August 2013) 18:8 *First Monday*, http://firstmonday.org/ojs/index.php/fm/article/view/4789/3730. 1.

----. "They're spying on you: how party databases put your privacy at risk," *iPolitics* (2015), https://ipolitics.ca/2015/09/01/theyre-spying-on-you-how-party-databases-put-your-privacy-at-risk/.

----. “Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications,” (2015)13:3/4 *Surveillance Society*, http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/voter_surv 370.

Bennett Colin J., and Robin M Bayley, “Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis,” (16 March 2012) Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/.

Biesecker, Michael and Julie Bykowicz, “Cruz app data collection helps campaign read minds of voters,” *The Associated Press* (11 February 2016), http://bigstory.ap.org/article/2db0fc93cf664a63909e26e708e91c67/cruz-app-data-collection-helps-campaign-read-minds-voters.

Bourgeois, Donald J, *Election Law in Canada* (Lexis-Nexis, 2015).

Brennan, Allison, “Microtargeting: How campaigns know you better than you know yourself,” *CNN* (5 November 2012), http://edition.cnn.com/2012/11/05/politics/votersmicrotargeting.

The Canadian Press, “Tory database draws ire of privacy experts,” *CTV News* (18 October 2007), http://www.ctv.ca/CTVNews/QPeriod/20071018/tory_privacy_071018/.

Chief Electoral Officer of Canada, “Preventing Deceptive Communications with Electors: Recommendations from the Chief Electoral Officer of Canada Following the 41st General Election,” (2013) *Library and Archives Canada Cataloguing in Publication*, http://www.elections.ca/res/rep/off/comm/comm_e.pdf.

Cosgrove, Ken, “It’s More Than Robo-Calls,” (2013) 34:2 *Policy Options* 54, http://policyoptions.irpp.org/wp-content/uploads/sites/2/2013/02/data-point.pdf.

Curry, Bill. “Robo–call furor focuses attention on massive Tory database,” *Globe and Mail* (29 February 2012), http://www.theglobeandmail.com/news/politics/robo-call- furorfocuses-attention-on-massive-tory-database/article4092455/.

DeCew, Judith Wagner, *Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, 1997).

Delacourt, Susan, “Conservative enemies’ lists hardly normal political business,” (19 July 2013) *The Star*, https://www.thestar.com/news/insight/2013/07/19/conservative_enemies_lists_hardly_normal_political_business.html.

----. “How the Big Red Machine Became The Big Data Machine,” *The Toronto Star* (21 May 2016), https://www.thestar.com/news/insight/2016/05/21/how-the-big-red-machine-became-the-big-data-machine.html.

----. *Shopping For Votes: How Politicians Choose Us and We Choose Them* (Douglas & McIntyre, 2016).

Dickson, Caitlin, "Trump launches America First app, a competitive social network," *Yahoo!Tech* (26 August 2016), http://www.yahoo.com/tech/trump-campaign-launches-america-first-000000643.html.

"Donald Trump's Campaign Was Hacked," *Fortune* (19 August 2016), http://fortune.com/video/2016/08/19/donald-trumps-campaign-was-hacked/.

Elections Canada, "Description of the National Register of Electors," http://www.elections.ca/content.aspx?section=vot&dir=reg/des&document=index&lang=e.

Elections Canada, "2015 Guidelines for Use of the Lists of Electors," http://www.elections.ca/content.aspx?section=pol&document=part3&dir=pol/loe&lang=e.

Gogolek, Vincent, "Two Bills Later, Political Parties Can Still Collect Your Info Scot-Free," *The Huffington Post* (24 June 2014), http://www.huffingtonpost.ca/vincent-gogolek/personal-data-collection-canada_b_5523176.html.

Heersink, Boris, "Reince Priebus vowed to punish Republicans who don't support Trump. It's an empty threat," *The Washington Post* (20 September 2016), https://www.washingtonpost.com/news/monkey-cage/wp/2016/09/20/reince-priebus-vowed-to-punish-republicans-who-dont-support-trump-its-an-empty-threat/.

Hill, Kashmir, "How this company tracked 16,000 Iowa caucus-goers via their phones," *Fusion* (12 February 2016), http://fusion.net/story/268108/dstillery-clever-tracking-trick/.

Howard, Philip N. and Daniel Kreiss, "Political Parties and Voter Privacy: Australia, Canada, the United Kingdom and United States in Comparative Perspective," (2010) 15:12 *First Monday*, http://firstmonday.org/article/view/2975/2627.

Issenberg, Sasha, "Obama's White Whale: How the Campaign's Top-Secret Project Narwhal Could Change This Race, and Many to Come," *Slate* (15 February 2012), http://www.slate.com/articles/news_and_politics/victory_lab/2012/02/project_narwhal_how_a_top_secret_obama_campaign_program_could_change_the_2012_race_.html.

"Issues Arising from Improper Communications with Electors: Round Table Report," (March 2013) *IRPP*, http://irpp.org/wp-content/uploads/assets/research/strengthening-canadian-democracy/communications-with-electors/roundtable-031513.pdf.

Kreiss, Daniel and Christopher Jasinski, "The Tech Industry Meets Presidential Politics: Explaining the Democratic Party's Technological Advantage in Electoral Campaigning, 2004–2012," (2016) *Political Communication* 1, http://www.tandfonline.com/doi/abs/10.1080/10584609.2015.1121941.

Maass, Dave, "Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election," *Electronic Frontier Foundation* (29 February 2016), https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election.

McCormick, John, "Republicans Fight to Regain Voter Data Parity with Democrats," *Bloomberg Politics* (31 May 2016), https://www.bloomberg.com/politics/articles/2016-05-31/republicans-fight-to-regain-voter-data-parity-with-democrats.

Mehta, Diana, "Ex-Tory staffer Michael Sona's sentence upheld in robocalls case," *The Toronto Star* (9 June 2016), https://www.thestar.com/news/canada/2016/06/09/ex-tory-staffer-michael-sonas-sentence-upheld-in-robocalls-case.html.

Morris, David Z., "With Trump's Campaign App, There's No Wall Protecting Your Contact Data," *Fortune* (28 August 2016), http://fortune.com/2016/08/28/trump-campaign-app-data-security/.

Morrow, Adrian, "Ontario Liberals to target ethnic voters with demographic database software" *The Globe and Mail (*14 April 2014), http://www.theglobeandmail.com/news/politics/database-helps-liberals-woo-ethnic-vote/article17953049/.

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books, 2009).

Office of the Information and Privacy Commissioner for British Columbia, "Sharing of Personal Information as part of the Draft Multicultural Strategic Outreach Plan: Government of British Columbia and the BC Liberal Party," Investigation Report F13-04 (1 August 2013), https://www.oipc.bc.ca/investigation-reports/1559.

Office of the Information and Privacy Commissioner for British Columbia, "Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's use of social media and passwords to evaluate candidates," https://www.oipc.bc.ca/mediation-summaries/1399.

Office of the Privacy Commissioner of Canada, "Audit reveals privacy gaps at federal agencies," News Release (12 February 2009), https://www.priv.gc.ca/media/nr-c/2009/nr-c_090212_e.asp.

Office of the Privacy Commissioner of Canada, Privacy Topics, https://www.priv.gc.ca/en/privacy-topics/#toc6.

Office of the Privacy Commissioner of Canada, "Statement from the Office of the Privacy Commissioner of Canada Regarding a Report by Elections Canada," Press Release (27 March 2013), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2013/nr-c_130327/.

Payton, Laura, "Privacy Concerns Raised by Marc Mayrand Over Election Changes," *CBC* (6 March 2014, http://www.cbc.ca/news/politics/privacy-concerns-raised-by-marc-mayrand-over-election-changes-1.2563048.

Rössler, Beate (ed.), *Privacies: Philosophical Evaluations* (Stanford University Press, 2004).

Regan, Priscilla M., *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995).

Small, Tamara A., "Canadian Politics in 140 Characters: Party Politics in the Twitterverse," (2010) *Canadian Parliamentary Review*, http://www.revparl.ca/33/3/33n3_10e_Small.pdf.

Solove, Daniel J., *Understanding Privacy* (Harvard University Press, 2008).

----. *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004).

Warren, Samuel D. & Louis D. Brandeis, "The Right to Privacy," (1890) *Harvard Law Review* 193.

Political Party Voter Management Systems

Conservative Party of Canada database, "Constituent Information Management System," https://apps.conservative.ca/login?rdr=https%3A%2F%2Fsupport.conservative.ca.

Liberal Party of Canada database, "Liberalist," http://liberalist.liberal.ca/.

New Democratic Party of Canada database, "Populus," https://populus.ndp.ca/foreAction/login/auth.

Privacy Policies

"America First" Privacy Policy, https://www.donaldjtrump.com/pages/app-privacy.

Conservative Party of Canada Privacy Policy, http://www.conservative.ca/privacy-policy/.

Green Party of Canada Privacy Policy, https://www.greenparty.ca/en/privacy.

Hillary For America Privacy Policy, https://www.hillaryclinton.com/page/privacy-policy/.

Liberal Party of Canada Privacy Policy, https://www.liberal.ca/privacy/.

New Democratic Party of Canada Privacy Policy, http://www.ndp.ca/privacy.

Private-Sector Data Companies

"America First," https://www.donaldjtrump.com/app.

"Actionsprout," www.actionsprout.com.

"Aristotle," http://aristotle.com.

"Acxiom Corporation," http://www.acxiom.com.

"Blue State Digital," www.5ivepoints.com.

"Cambridge Analytica," https://cambridgeanalytica.org.

"Catalist," http://www.catalist.us/about/.

"Cruz Crews," https://www.tedcruz.org/news/ted-cruzs-official-cruz-crew-campaign-app-tops-2016-field/.

"Data Trust," http://thedatatrust.com.

"Dstillery," http://dstillery.com.

"Environics Analytics," Segmentation Systems, http://www.environicsanalytics.ca/prizm5.

"Footwork App," www.gofootwork.com.

"Google's Political Campaign Toolkit," http://www.google.com/ads/politicaltoolkit/.

"i360," http://www.i-360.com.

"NGP VAN," https://www.ngpvan.com/.

"Nationbuilder," http://www.nationbuilder.com.

"Organizing for America App for the i-Phone," http://my.barackobama.com/page/content/iphone2010/.

"Response Unlimited," http://www.responseunlimited.com.

"Segment Metrix 2.0 from Comscore," http://www.comscore.com/Products_Services/Product_Index/Segment_Metrix_2.0.

"TargetPoint Consulting," http://www.targetpointconsulting.com.

"uCampaign," https://ucampaignapp.com.

Appendices

Appendix A : Privacy Policy of the Conservative Party of Canada[159]

Our Commitment to Protecting Your Privacy
Your privacy is important to us. The Conservative Party will respect your privacy through the protection of any of your personal information that you provide to us. We take great care to keep both confidential and secure all personal information in our possession.
As a federal political party registered under the Canada Elections Act, the Conservative Party including its "electoral district associations" (riding associations) are subject to extensive regulation under that Act, including in particular public disclosure requirements for contributions over $200.

What is "Personal Information"
"Personal Information" is information about an identifiable individual. It includes information such as name, address, e-mail address, telephone number and other contact information.

Collecting Personal Information
Elections Canada provides all political parties with a list of electors, including names and postal addresses. We collect other information from publically available data.
We collect personal information from donors and members when they contribute to our Party or purchase a membership. You may also choose to provide us with personal information on a voluntary basis, such as when registering for an event or signing a petition. We are required by law to keep records of donors for tax purposes.
If you submit your e-mail address and/or personal information through our website, you consent to being added to our e-mail list. You may unsubscribe from our e-mail list at any time using the link provided in each email message, or by clicking here.

Usage of Personal Information
We use your personal information to communicate with you. As a political party, we believe it is important to communicate with Canadians on a regular basis.
As a national organization with a riding-based membership system, your personal information may also be disclosed to our local riding associations, who may also communicate with you.
Additionally, non-personal information may be collected by the Conservative Party through the use of cookies, including third-party cookies. Cookies allow us to track how people are using our site and help us deliver better content to our visitors. We may use this information, in aggregate, to improve our site or to assist in advertising.
Visitors can opt-out of many of the advertising features used by this site and others by adjusting their Google Ads Settings, or through free services like the Network Advertising Initiative's Consumer Opt-Out page: http://www.networkadvertising.org/choices/.

Protecting your Personal Information

[159] Conservative Party of Canada Privacy Policy, http://www.conservative.ca/privacy-policy/.

We maintain security systems to safeguard your personal information from unauthorized access, disclosure or misuse, and from loss or unauthorized alteration.
We will not sell your personal information that you have chosen to provide us.

Accuracy of Personal Information
We always try to keep your personal information accurate and up-to-date. If you wish to update your personal information, contact us by e-mail at servicedesk@conservative.ca.

External Links
Our web site contains links to a limited number of other web sites. The Conservative Party is not responsible for the content of these web sites.

How to Contact Us
If you have any questions, concerns, or complaints about the Conservative Party privacy policy or the information we collect, please contact our privacy officer by e-mail at privacy@conservative.ca, or by regular mail at:

Attn: Greg Labuschagne, Privacy Officer
Conservative Party of Canada
1204 – 130 Albert St.
Ottawa, ON K1P 5G4

If you no longer wish to receive phone calls or mail from the Conservative Party, you may contact us at servicedesk@conservative.ca. Please include your name, address and phone number so we can accurately deal with your request.

Appendix B : Privacy Policy of the Green Party of Canada[160]

Important information and privacy policy

We respect your privacy and do not sell or lend our e-mail list to anyone. We use security measures to protect against the loss, misuse and alteration of data used by our system.

How we use your Personal Information

Personal information that you give us is used to communicate with you, or to facilitate your participation as a volunteer if you want to assist. We take great attention in the way we store and use your personal information. The Green Party is a national organization, with a riding-based membership system, due to this your personal information may also be used by our local riding associations. As a federal political party registered under the Canada Elections Act, the Green Party of Canada, including its EDAs (electoral district associations and riding associations) are subject to regulation under the Elections Act, including public disclosure requirements for contributions over $200.

Identification and unsubscribe information:

To update your mailing: email e-info@greenparty.ca. To unsubscribe immediately and automatically: click on the opt-out link at the bottom of the last email you received. If you received a mailing from us, you are (a) a member of the Green Party of Canada (b) a recent donor or volunteer (c) have recently taken action with one of our online tools or (d) otherwise have an existing relationship with us. We respect your time and attention by controlling the frequency of our mailings.

Privacy statement:

Our commitment to your privacy (This policy is in effect September 25, 2004.) We use security measures to protect against the loss, misuse and alteration of data used by our system. Security audits are conducted periodically to ensure the integrity of our systems.

Sharing and Usage

We do not share, sell, or rent individual personal information with anyone outside of the party, without your express advance permission or unless so ordered by a court of law. Information submitted is only available to Green Party personnel who manage this information for purposes of communicating with you on matters pertaining to Green Party business, or for determining how best to provide that information according to your wishes. If you have received unwanted, unsolicited email sent via this system or purporting to be sent via this system, please forward a copy of that email with your comments to abuse@greenparty.ca for review.

2. Web site privacy policy:

The Green Party of Canada's Website Privacy Policy

The Green Party of Canada respects your personal privacy and is committed to maintaining your trust and confidence. We believe in ensuring the security of your personal information. Please take the time to read this policy, and contact us if you have any questions or concerns. We strive

[160] Green Party of Canada Privacy Policy, https://www.greenparty.ca/en/privacy.

to protect any personal information you may provide us. If we ask you to provide us with any personal information, we will tell you the purposes for which we intend to use that information. Your personal information is not sold to anyone for any purpose. This statement discloses the privacy practices and policies for the Green Party of Canada's Web site, the information contained therein and the information collected therein. If you have any questions about these practices and policies, please email us at webadmin@greenparty.ca

Information Collection, Use and Disclosure

The purpose of this Web site is to educate and inform the public about the Green Party of Canada, its goals, its key values, its policies and platform, and its mission. When you visit this site and access information, you are anonymous. We do not require you to provide personal information to view it. Information gathered on Greenparty.ca falls under the following categories:

- Aggregate site use information
- Online donation information
- Green Party Membership Information
- Policy Forum, Discussion Boards, Organizing, and Automated Discussion Lists (ADLs/list serves)

Aggregrate Site Use Information

We record information about the pages viewed by all of our website visitors. This data includes internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, platform type, date/time stamp, connection speed, read time, display time and number of clicks. We use this data, in aggregate form only, to compile statistics and reports for the Green Party of Canadas use, and improve the online experience for all visitors. We reserve the right to provide general descriptions or portions of this aggregate information to vendors, consultants, partner NGOs or news services. Such uses of the data in this fashion would typically be to plan site architecture improvements or to measure public interest in our site.

Cookie Use

A cookie is a small text file stored on the users hard drive that may help you access pages faster and allows our server to recognize you as you navigate within the site. We use cookies to assist with anonymous site traffic analysis, which includes tracking the time/date of visits, pages viewed and referring URLs. Cookies are generally not required to use our site, although some sections of our site may not be available to you if you choose not to accept cookies. You may configure your Web browser to either refuse all cookies, accept them each time they are offered, or accept them at all times. Consult your browser's help files for assistance on changing cookie settings or removing cookie files.

Online Donation Information

The Green Party of Canada only reads cookies specifically written for our site and does not use cookies to track a user's internet history on other sites. If you donated money online, we only request the information needed to complete the processing of that transaction and provide a tax receipt. We also share our users' personal information with Elections Canada, Canada Customs

and Revenue Agency or other federal agencies as required by law. We do not provide any more information than necessary for these purposes. We may also use the information to contact you regarding your donation.

Our Site Security

We take appropriate security measures to protect your personal information against loss, theft, and unauthorized access and use Secure Sockets Layer (SSL) protocol, to encrypt, or encode, information sent to us. Any personal information you provide to us is exchanged via a secure server. Encryption protects your information, such as your credit card number, name and address information by scrambling it before it is sent from your computer. Only once we receive your information is it decoded. We make all reasonable efforts to ensure its security on our own systems and undergo periodic security audits to ensure the safeguarding of this information. Warning: e-mail is not encrypted, nor is it a secure means to send personal information. We urge you to use our secure severs to process online donations, or call our Ottawa office to make a donation by phone. Click here for Green Party of Canada telephone, postal mail and other contact information.

Green Party of Canada Membership Information

As a registered federal political party, the Green Party of Canada requires your assistance in providing us with your personal information to fulfill certain legal obligations. If you become a member, you must provide certain information, which is added to our internal membership database that by law must be maintained. The information maintained in the database includes:

- Member number;
- Member name, address and telephone number;
- Amount of member donation(s);
- Date on which the member registered as a member of the Green Party of Canada, and/or made (a) donation(s);
- Date on which any person ceased to be a member.

The information contained in the database can only be used for official Green Party business such as informational mailings, internal election materials, and other correspondence. The Green Party of Canada does not sell, rent, or lend our membership lists to anyone.

Updating Membership Data

Membership information previously provided to the Green Party of Canda can be up updated by calling our national office in Ottawa at 1-866-868-3447 (toll free), in Ottawa: 613.562-4916

Opting Out

If you wish to have any of your personal information removed from our databases, or if you no longer want us to send any further communications to you, please send an e-mail to membership@greenparty.ca with your request. Please note, however, that as a federal political party we are required by law to maintain certain information about our members, as noted above.

We may be required by law to maintain this information for a period of time after a member has terminated his or her membership.

E-newsletter and Green Canada Vert

Visitors to our site may choose to receive our email newsletters. Members may also choose to use our many automated discussion lists (ADLs or list serves).

E-Newsletter Subscriptions

E-newsletters are sent only to users who choose to provide us with their email address. Our newsletter subscriber database is not sold, rented or otherwise to any other parties. Subscribers wishing to update their contact information, or opt out of receiving newsletters, can use the links provided at the bottom of each newsletter email.

Green Canada Vert

Green Canada Vert is our quarterly, printed newsletter available by post to members. It is sent automatically to all members of the Green Party of Canada. Join and automatically subscribe to Green Canada Vert by becoming a member of the Green Party of Canada.

Other online services

Visitors using our online policy development platform and members choosing to use any of our online collaborative tools including our e-mail discussion lists, bulletin boards, etc., are bound by the user-provided content guidelines set out in our Terms of Use. Postings and articles submitted remain property of the Green Party of Canada and are archived.

Fraud and Crime Prevention

The Green Party of Canada reserves the right to co-operate with local, national, or international law enforcement or other authorities in the investigation of improper or unlawful activities and this may require the disclosure of personal information. If such an investigation requires disclosure of personal information on file in our records, we may be required by law to cooperate. We also reserve the right to report improper or unlawful user activities on our site, which may require the disclosure of personal information relating to those individuals conducting such improper or unlawful activities.

Links

This web site contains links to other sites or e-mail addresses. This privacy statement only applies to information collected by our web site. We are not responsible for the privacy practices and/or policies of these or any third parties, nor do we necessarily agree with or endorse the opinions or positions expressed. Links are provided for information only.

Accuracy of, and access to, personal information

We strive to ensure that any personal information we retain and use is as accurate, complete and up-to-date as necessary for the purposes for which we will use it. We do not routinely update personal information except where and as necessary for these purposes. If however our records regarding your personal information are inaccurate or incomplete, we will amend that information at your request. At your request we will provide to you a statement explaining the

extent to which we hold personal information about you, and we will explain how that information has been used by us.

Policy changes and updates

This page will be updated if and when information about the collection and use of your personal data changes, and/or policies regarding the use of the site are changed. Your comments and questions are welcome at our contact page.

Appendix C : Privacy Policy of the Liberal Party of Canada[161]

The Liberal Party of Canada (Liberal Party) is committed to respecting your privacy. The purpose of this Privacy Policy is to explain how we handle personal information to ensure its confidentiality, security and accuracy.

WHAT IS "PERSONAL INFORMATION"?

"Personal information" is information about an identifiable individual. It includes contact information such as your name, address, phone number and financial information.

HOW DO WE OBTAIN YOUR PERSONAL INFORMATION AND WHAT DO WE OBTAIN?

We obtain the information that you choose to give us. You may do so in a variety of ways including:
•When you visit our website for the purpose of becoming involved with the party as a member, volunteer or donor.
•When you subscribe to our communications.
•If you register at an event or at a Party convention.
•If you complete a membership or donation form either electronically or on paper.
•If you complete any other form on a Liberal website, including online petitions

It is also possible that your information could be provided to us by a volunteer or friend who thinks you would be interested in getting involved with the Liberal Party.

The information that we collect may include:
•Contact and identification information, such as your name, address, telephone numbers, e-mail address and social media contacts.
•Donation information such as date and amount of your donation.
•Financial information that we need to process your donation e.g. payment methods and preferences, billing and banking information (e.g. credit card number and expiry date).

HOW DO WE USE AND SHARE PERSONAL INFORMATION?

We will not, without your consent, use your personal information for any purpose other than as described in this privacy policy, except where permitted or required by applicable legislation. For example, under the Canada Elections Act, we are required to provide Elections Canada with our donors' names, addresses and contribution amounts.

We also use your personal information to communicate with you about the Liberal Party and its activities, as well as to provide you with news and information. We use your financial information to process your contributions. If you have been a contributor, we may contact you

[161] Liberal Party of Canada Privacy Policy, https://www.liberal.ca/privacy/.

again to seek your financial support. Under no circumstances, however, do we sell your personal information.

Given that the Liberal Party is a national organization, personal information may be shared internally, for instance between the Party and its electoral district associations (riding associations). In addition, we may engage third party providers to perform tasks on our behalf such as processing your donation, making phone calls and providing technical services to our website. When information is shared with third parties for these purposes, we include privacy protective clauses in written contracts to help safeguard personal information.

HOW DO WE PROTECT PERSONAL INFORMATION?

The security of your personal information is important to us. For information provided online, our website contains security measures in order to protect against the loss, misuse, or alteration of the information under our control. Our server is located in a controlled and secure environment.

HOW CAN I UPDATE MY INFORMATION OR UNSUBSCRIBE?

You may update or correct the information you provide to us by e-mailing us at assistance@liberal.ca. If you have subscribed to receive information, you may unsubscribe by clicking "Unsubscribe" at the bottom of the email message.

WHAT ABOUT ANTI-SPAM LEGISLATION?

Most of the messages sent by the LPC and its other political entities are exempt from the application of Canada's anti-spam law as it relates to commercial electronic messages sent to electronic addresses. This is because: the electronic messages that we send are generally either those soliciting donations, which are specifically exempt under the law, or are messages of a political, not a commercial, character. If we do send any messages to which the law applies and for which there are no exemptions, we will ensure that we have consent to do so, as required by the law, and that any other legal requirements e.g. an unsubscribe mechanism, are met.

As a best practice, we have an unsubscribe mechanism for our electronic messages, even where the law does not require us to do so.

DOES THE LIBERAL PARTY LOG IP ADDRESSES?

We log IP addresses, or the location of your computer network on the Internet, for systems administration and troubleshooting purposes. We may also use IP addresses to track which pages people visit in order to improve the quality of our website.

DOES THE LIBERAL PARTY USE COOKIES?

Like many websites, we use cookies which are small text files stored on the user's browser. We use cookies to, for example, assist with site traffic analysis which includes tracking the time and

date of website visits, pages viewed and referring URL's. There are simple ways to refuse cookies, or accept them each time they are offered. Consult your browser's online help for assistance on changing cookie settings or removing cookie files.

LINKS TO OTHER WEBSITES

Our website contains links to a limited number of other websites including those for our provincial and territorial associations. The Liberal Party is not responsible for the content or the privacy policies of these websites.

CONTACT US

If you have any questions about our privacy policy or the information you have provided to us online, simply email us at assistance@liberal.ca.

You can also reach us by regular mail at the following address:
Liberal Party of Canada
350 Albert Street, Suite 920
Ottawa, Ontario, K1P 6M8
Attention: Deputy Director of Compliance

Appendix D : Privacy Policy of the New Democratic Party of Canada[162]

Our Commitment to Respecting and Protecting Your Privacy

Canada's NDP is committed to respecting and protecting your privacy, including your personal information. Our policy is in strict compliance with Canadian privacy principles, as well as our obligations under the Canada Elections Act . We are committed to ensuring the confidentiality and security of your personal information.

This page summarizes our privacy policy and information practices for NDP.ca. It is intended to provide information to help you make informed decisions when choosing to communicate with us via this site.

Collecting Personal Information

"Personal information" is information about an identifiable individual. It includes information such as your name, email address, telephone number, and financial information.

Elections Canada provides all registered political parties with the List of Electors, which includes names and addresses.

We collect the personal information that you choose to provide to us when you become a donor, a member, when you voluntarily subscribe to our communications, when you register for an event or sign a petition either in person or online, or when you complete any of the forms on NDP.ca. If you submit your email address and/or personal information through NDP.ca, you consent to being added to our email and/or contact list.

Using Personal Information

We use your personal information to communicate with you about the NDP, to provide you with news and information about the NDP and our activities, and to contact you about your past and future donations and membership.

As we are a federal party, we may share your information internally within our national organization, including with NDP riding associations.

We use your financial information to process your donations. We are also required by the Canada Elections Act to provide Elections Canada with information related to the donations you make to us.

Protecting Your Personal Information

[162] New Democratic Party of Canada Privacy Policy, http://www.ndp.ca/privacy.

Your privacy is very important to us. We protect your personal information by employing rigorous security systems and strict access controls in order to safeguard your personal information from unauthorized access, disclosure, alteration, or misuse.

We may engage third parties to provide us with services from time-to-time, such as hosting servers and websites, processing online donations, or providing technical or communications services. When information is shared with third parties for these purposes, we ensure that your personal information is rigorously protected by including privacy safeguards in all our contracts, including stringent confidentiality and non-disclosure provisions.

Visiting NDP.ca

When visiting NDP.ca, your privacy is respected and protected.

Any information collected while you are visiting NDP.ca, such as server log data, is managed in accordance with this privacy policy and is protected by applicable law. Server logs include statistical information, such as visitors' IP addresses, time and duration of visits, and pages visited. These statistics may be used to improve your experience on NDP.ca.

In addition, non-personal information may be collected through the use of cookies. Cookies are small text files maintained by your browser in order to remember user settings as you navigate the site. NDP.ca uses cookies, for example, to remind your browser whether you chose to view our website in English or in French. You can also adjust your browser's settings to refuse cookies, or to accept them on a case-by-case basis.

Linking to External Sites

Other sites to which we provide links may be governed by different policies. The NDP does not assume responsibility for the information practices of these other sites, and we strongly encourage all our visitors to review the privacy policies and statements of all externally-linked sites.

Updating your Personal Information

We aim to keep your information accurate and up-to-date. To update or correct the personal information you provide to us, please contact us at info@ndp.ca .

Contacting Us

Questions or concerns about our privacy policy or the information we collect may be directed to CanadasNDP-LeNPDduCanada@ndp.ca .

You can also contact us by phone at 613-236-3613 or by postal mail at the address below:

New Democratic Party of Canada
Suite 300 - 279 Laurier Avenue West

Ottawa, Ontario K1P 5J9

If you no longer wish to be contacted by us or wish to be placed on our internal Do-Not-Call list, please let us know by emailing support@ndp.ca . You may also unsubscribe from our communications by using the unsubscribe mechanisms contained in all of our electronic messages.

Appendix E : Leak from the Jeb Bush Presidential campaign[163]

[163] Retreived from Maass, Dave, "Voter Privacy: What You Need to Know About Your Digital Trail During the 2016 Election,," *Electronic Frontier Foundation* (29 February 2016), https://www.eff.org/deeplinks/2016/02/voter-privacy-what-you-need-know-about-your-digital-trail-during-2016-election.

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

6.0 SUMMARY OF RECOMMENDATIONS[164]

RECOMMENDATION 1

Government should provide training for its employees regarding the use of personal email accounts for government business in order to ensure that reasonable security measures are in place to protect personal information, and that personal information is not stored or disclosed outside of Canada.

RECOMMENDATION 2

Government should ensure that copies of all records created by its employees that relate to government business are located in government controlled information management systems.

RECOMMENDATION 3

Government should provide its employees with sufficient technological resources to ensure that they do not have a reason to use personal email accounts in the performance of their government duties.

RECOMMENDATION 4

Government should ensure that employees with roles that are closely tied to the governing party participate in mandatory privacy training sessions regarding the need to keep personal information obtained in their government role separate from personal information obtained in any role they might have with the political party.

RECOMMENDATION 5

The BC Liberal Party should ensure that employees and volunteers who also have roles within government participate in mandatory privacy training sessions regarding the need to keep personal information obtained in their BC Liberal Party role separate from personal information obtained in their government role.

[164] Office of the Information and Privacy Commissioner for British Columbia, "Sharing of Personal Information as part of the Draft Multicultural Strategic Outreach Plan: Government of British Columbia and the BC Liberal Party", Investigation Report F13-04 (1 August 2013), https://www.oipc.bc.ca/investigation-reports/1559.

Appendix G : Fair Information Principles

Below is a concise description of the ten information principles:[165]

Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Principle 2 – Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 – Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Principle 6 – Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 – Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9 – Individual Access

[165] PIPEDA Fair Information Principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/.

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 – Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Appendix H : Liberalist iPhone/iPad app[166]

New Version: MiniVan iPhone/iPad app

Thanks in part to your feedback, the popular iPhone App MiniVan has been upgraded to include many exciting new features.

- You can now add new contacts into the database directly from your device.
- The app will suggest addresses from your list based on your actual location.
- The app is now bigger and more interactive for use on iPads.
- IPad users can now select Landscape or Portrait screen orientation.
- You can now load lists onto your device using the list numbers on printed lists.
- Canvas coordinators can now set expiry dates for lists they send to the app.

The MiniVan App allows you to send a virtual version of your canvas sheet to any volunteer with an apple device (iPad, iPhone, iPod). The volunteers enter canvas results on their device and return the data to you with the click of a button.

You can download the MiniVan App here: http://itunes.apple.com/ca/app/minivan-touch/id352087547?mt=8

Become a Liberalist Champion

Your Liberal Party Help Desk is pleased to launch the Liberalist Champions Training Program. This 8 week online adult learning program is carefully designed to comprehensively train you and your team on the Liberalist system.

Each riding should have at least one person participate in the program. There is no limit to the number of participants from each riding.

The course includes 8 live one-hour sessions on a variety of tools, topics and strategies and 3 short quizzes to help you track your progress. Successful participants will be certified as "Liberalist Champions". The Liberalist Champions Training Program will take place from March 13th to May 2nd.

[166] Liberalist, https://liberalist.liberal.ca/new-ipad-app-more-2/.

Appendix I : Donald Trump Privacy Policy[167]

PRIVACY POLICY

LAST REVISED: JULY 7, 2015

This Privacy Policy explains the information that Donald J Trump for President ("DJT," "we," or "us") collects, uses, shares, and discloses with respect to the use of DJT's website and mobile application, "America First" about users. DJT reserves the right to change the provisions of this Policy at any time for any reason. Please review this Policy from time to time to make sure that you understand it and any changes. This Privacy Policy may change at any time. If we make any changes to our privacy practices, we will post a revised Privacy Policy on this page, as well as the effective date of the change. By accessing or using the website/mobile application, you accept the terms of this Privacy Policy.

If you have any questions about this Policy or the use of your information by DJT, please contact us by emailing apphelp@donaldtrump.com or writing to _____.

1. WHAT IS PERSONAL INFORMATION?

For purposes of the use of DJT's website and mobile application, including America First, Personal Information means information that specifically identifies and individual, such as their name, address, telephone number, cell phone number, email address, voter registration history, or credit card number as well as information about your activities on this site when it is linked with other information that would enable a reader to identify you. Personal Information does not include aggregate data that we collect about the use of our website or America First, or about a group or category of services or users, from which identifying information about the user has been removed. The collection of such aggregate information is in no way limited or restricted by this policy.

2. INFORMATION COLLECTED AUTOMATICALLY

When you use our website or America First, we may automatically collect and store information about your computer or mobile device and your activities. This information may include your mobile device's unique ID number, your mobile device's geographic location while the app is actively running, your computer's IP address, technical information about your computer or mobile device (such as type of device, web browser or operating system), your preferences and settings (time zone, language, privacy preferences, product preferences, etc.), the URL of the last web page you visited before coming to one of our sites, the buttons, controls and ads you clicked on (if any), how long you used our website or app and which services and features you used, and the online or offline status of America First.

3. INFORMATION YOU PROVIDE

[167] "America First" Privacy Policy, https://www.donaldjtrump.com/pages/app-privacy.

In order to register, you will be asked to provide certain identifying information, including your phone number. In order to maximize your experience with our website and America First and to provide its features and services, we may periodically access your contact list and/or address book on your mobile device. You hereby give your express consent to access your contact list and/or address book.

Whenever you voluntarily disclose personal information on publicly-viewable screens or pages, that information will be publicly available and can be collected and used by others. For example, if you post your email address, you may receive unsolicited messages. We cannot control who reads your posting or what other users may do with the information you voluntarily post, so we encourage you to exercise discretion and caution with respect to your personal information.

You may also (but are not required to) provide information about yourself (such as your gender, ethnicity, location, URL, political viewpoints, mailing address, phone number, or a biography). This information may be provided as part of the registration process, by volunteering, or responding to a survey. This information may be used by us in accordance with this policy and will be treated as confidential personal information.

Any additional image or information you provide may be publicly displayed. If you wish, we will delete your account information; to do so, please close your account by sending an email to apphelp@donaldtrump.com.

4. INFORMATION ABOUT OTHERS

We may access, collect, and store personal information about other people that is available to us through your contact list and/or address book. The website and mobile app allows users to complete contact information for entries on their contact list/address book, match their information with information available from other sources, and identify issues of interest. To revoke your consent for this access, you can change the settings on your device if that option is available, delete your profile, or delete or uninstall the mobile app from your device.

5. HOW WE USE YOUR INFORMATION

We use your information to provide and improve our services, award loyalty points to you, make special offers, customize services for you, better understand our users, or diagnose and fix problems.

6. GEO-LOCATION INFORMATION

While the America First application is in use, we may keep track of your device's geographic location so that we can connect you to other America First users based on your particular geographic location.

7. USE OF YOUR INFORMATION BY OTHERS

Except as described below, we will not share your personal information with other companies or organizations. What information we make available to other organizations depends on the nature

of our relationships with them. Examples of circumstances in which we would share personal information include:

1. Service Providers: We may share all of the types of information we collect with vendors, consultants or service providers who provide services to us and who require access such information to carry out their work.

2. Aligned Organizations: We may share your information with other organizations, groups, causes, campaigns or political organizations that we believe have similar viewpoints, principles or objectives to us.

3. Analytics Companies: We allow analytics companies to use tracking technologies to collect information about our users' computers or mobile devices and their online activities. These companies analyze this information to help us understand how our sites and apps are being used. Analytics companies may use mobile device IDs, as described in the paragraph below ("Mobile device IDs"). Unlike cookies, device IDs cannot be deleted.

4. Mobile device IDs: In order to recognize you, store your preferences, and track your use of our application, we may store your mobile device IDs (the unique identifier assigned to a device by the manufacturer) when you use the America First application. Unlike cookies, device IDs cannot be deleted.

5. Aggregated Information: We may publicly disclose aggregated information about our users, such as the total number of our users and their overall demographics.

6. Legal matters: We may disclose any information: in response to a legal request, such as a subpoena, court order, or government demand; to investigate or report illegal activity; or to enforce our rights or defend claims.

7. With Your Consent: If you consent to the sharing of certain information, including information you enter during the registration process or while using the application, we may share that information consistent with the consent you provide.

We are not responsible for the actions of any service providers or other third parties, nor are we responsible for any additional information you provide directly to any third parties. Before disclosing information to any organization, we encourage you to familiarize yourself with their privacy policy. Nothing herein restricts the sharing of aggregated or anonymized information, which may be shared with third parties without your consent.

8. CHILDREN'S PRIVACY

We do not allow persons under 13 to register for any service, and we do not knowingly collect any personally identifiable information from persons under the age of 13.

10. INFORMATION FROM USERS OUTSIDE THE UNITED STATES

If you're outside the United States, your information will be sent to and stored in the United States, where our servers are located. By using our website and/or America First, you agree to the information collection, use, and sharing practices described in this Privacy Policy.

Appendix J : Hillary Clinton Privacy Policy[168]

HILLARY FOR AMERICA

PRIVACY POLICY

Last Updated: February 11, 2016

This Privacy Policy explains how information about you is collected, used and disclosed by Hillary for America ("HFA") and its affiliated organizations, including the Hillary Victory Fund. This Privacy Policy applies to information we collect when you use the websites, mobile sites, mobile applications and other online services that link to this Privacy Policy (collectively, the "Sites").

We may change this Privacy Policy from time to time. If we make changes, we will notify you by revising the date at the top of the policy and, in some cases, we may provide you with additional notice (such as adding a statement to our homepage or sending you an email notification). We encourage you to review the Privacy Policy whenever you access the Sites to stay informed about our information practices and the ways you can help protect your privacy.

Collection of Information

Information You Provide to Us

We collect information you provide directly to us. For example, we collect information when you fill out a form, send us an email, sign up to receive email or text message updates, request information, sign a petition, sign up as a volunteer, create an account, participate in a contest or promotion, make a donation or purchase, communicate with us via third party social media sites, , or otherwise communicate with us. The types of information we collect may include your name, email address, social media handles, user names, postal address, phone number, mobile number, credit card information, location, and other contact or identifying information you choose to provide.

In addition, the Federal Election Commission (FEC) may require us to collect certain personal information from donors. For example, the FEC requires us to collect (and disclose) the name, mailing address, occupation, and employer of all individuals whose donations exceed $200 per election cycle.

Information We Collect Automatically When You Use the Sites

When you access or use our Sites, we automatically collect information about you, including:

[168] "Hillary For America" Privacy Policy, https://www.hillaryclinton.com/page/privacy-policy/.

Log Information: We log information about your use of the Sites, including the type of browser you use, access times, pages viewed, your IP address and the page you visited before navigating to our Sites.

Device Information: We may collect information about the computer or mobile device you use to access our Sites, including the hardware model, operating system and version, device identifiers and mobile network information.

Information Collected by Cookies and Other Tracking Technologies: We use various technologies to collect information, and this may include sending cookies to your computer or mobile device. Cookies are small data files stored on your hard drive or in device memory that helps us to improve our Sites and your experience, see which areas and features of our Sites are popular and count visits. We may also collect information using web beacons (also known as "tracking pixels" or "clear GIFs"). Web beacons are electronic images that may be used in our Sites or emails and help deliver cookies, count visits, understand usage and campaign effectiveness and determine whether an email has been opened and acted upon. For more information about cookies, and how to disable them, please see "Your Choices" below.

Information We Collect From Other Sources

We may also obtain information from other sources and combine that with information we collect through our Sites. For example if you create or log into your account through a social media site, we will have access to certain information from that site, such as your name, account information and friends lists, in accordance with the authorization procedures determined by such social media site. We may also use such information for list matching purposes.

Use of Information

We may use information about you for various purposes, including to:

Provide, maintain and improve our Sites and send you confirmations, receipts, technical notices, updates, security alerts and support and administrative messages;

Provide and deliver the information or products you request, process donations and transactions and send you related information, including confirmations and invoices,

Respond to your emails, submissions, comments, questions and requests, provide customer service, request feedback, and otherwise contact you about your use of the Sites;

Send you newsletters and otherwise provide you with information or services you request or that we think will be of interest to you, such as sending you

information to keep you informed about various campaigns, candidates, issues, events, resources, promotions, contests, products and services;

Help connect you with other supporters, and to solicit volunteers, donations and support for HFA and for candidates, issues and organizations that we support;

Contact you if other information is necessary under Federal election laws;

Remind you to vote and register to vote and assist you in finding your registration information, polling location and campaign events near you;

Monitor and analyze trends, usage and activities in connection with our Sites;

Personalize and improve the Sites and provide advertisements, content or features that match user profiles or interests or that are based on the information you provide or the actions you take;

Notify and contact contest or sweepstakes entrants; and

Carry out any other purpose for which the information was collected.

HFA is based in the United States and the information we collect is governed by U.S. law. By accessing or using the Sites or otherwise providing information to us, you consent to the processing and transfer of information in and to the U.S. and other countries.

Sharing of Information

We may share information about you as follows or as otherwise described in this Privacy Policy:

With vendors, consultants and other service providers or volunteers who need access to such information to carry out work on our behalf;

With candidates, organizations, campaigns, groups or causes that we believe have similar political viewpoints, principles or objectives or share similar goals and with organizations that facilitate communications and information sharing among such groups;

With other participants in a joint fundraising committee;

To report required information to the Federal Elections Commission, including name, mailing address, occupation, and name of employers of individuals whose contributions exceed $200 in an election cycle (for additional information, visit the FEC website at http://www.fec.gov);

When we believe in good faith that we are lawfully authorized or required to do so or that doing so is reasonably necessary or appropriate to comply with the law or legal processes or respond to lawful requests, claims or legal authorities, including responding to lawful subpoenas, warrants, or court orders;

If we believe your actions are inconsistent with the spirit or language of our user agreements or policies, or to protect the rights, property and safety of HFA, its employees, volunteers, constituents or others;

In connection with, or during negotiations of, any reorganization, formation of new committee or successor organization, asset sale or transfer, financing or lending transaction or in any other situation where personal information may be disclosed or transferred as one of the assets of HFA; and

With your consent or at your direction, including if we notify you through our Sites that the information you provide will be shared in a particular manner and you provide such information.

We may also share aggregated or anonymized information that does not directly identify you.

Online Petitions

If you sign an online petition, you understand that such petition is public information and that we may make the petition, and your name, city, state, and any comments provided in connection therewith publicly available. In addition, we may provide such petitions or compilations thereof, including your comments, name, city, and state to national, state or local leaders, or to the press.

Social Sharing Features

The Sites may offer social sharing features and other integrated tools (such as the Facebook "Like" button), which let you share actions you take on our Sites with other media, and vice versa. The use of such features enables the sharing of information with your friends or the public, depending on the settings you establish with the entity that provides the social sharing feature. For more information about the purpose and scope of data collection and processing in connection with social sharing features, please visit the privacy policies of the entities that provide these features.

Advertising and Analytics Services Provided by Others

We may allow third parties to use cookies, web beacons, or other technologies or otherwise collect information about you in order to provide analytics and advertising services, including serving ads on the Sites or on other sites based on your visits to the Sites and other sites across the Internet and across various mobile applications. These entities may collect or receive information about your use of the Sites and other websites and mobile applications, including your IP address, browser, device information, pages viewed, time spent on pages, links clicked

and conversion information. This information may be used by HFA and others to, among other things, analyze and track data, determine the popularity of certain content, deliver advertising and content targeted to your interests and better understand your online activity.

For example, we may use Remarketing with Google Analytics or other remarketing tools to advertise online. This enables third-party vendors, including Google, to show our ads on sites across the Internet. Such third-party vendors, including Google, may use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the DoubleClick cookie) together to inform, optimize, and serve ads based on your past visits to our Sites. For information on how you can opt out of Google's use of cookies for interest-based ads please visit Google's Ads Settings. Other advertising vendors we may use include, without limitation, Yahoo!, MSN, Facebook, Twitter.

Another third party that may collect information by placing cookies and web beacons on your computer is IBM, who provides HFA with a cloud-based digital marketing platform. For information on IBM's data collection and use practices please see http://www.ibm.com/software/marketingsolutions/privacy/index.html

For more information about Internet-based ads, or to opt out of having your web browsing information used for behavioral advertising purposes, please visit www.aboutads.info/choices.

Security

HFA takes reasonable measures to help protect information about you from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction.

Your Choices

Cookies

Most web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove or reject browser cookies. Removing or rejecting browser cookies does not necessarily affect third party flash cookies that may be used in connection with our Sites. To delete or disable flash cookies please visit www.adobe.com/products/flashplayer/security for more information. Please note that if you choose to remove or reject cookies, this could affect the availability and functionality of our Sites.

Promotional Communications

You may opt out of receiving text messages, updates and newsletters by following the instructions in those emails or text messages. If you opt out, we may still send you other types of emails, such as those about your use of the Sites or any donations or transactions.

Contact Us

If you have any questions about this Privacy Policy, please contact us using this form.

Appendix K : Table of Relevant Legislation

Legislation	**Purpose**	**Commercial Activity**	**Personal Information**	**Political Information**
PIPEDA	"…to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances." ***s. 3***	"…any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." ***s. 2(1)***	"…information about an identifiable individual." ***s.2(1)***	
Privacy Act	"…to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of		"…information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (a) information relating to the race,	

	access to that information.” ***s. 2***		national or ethnic origin, colour, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, (f) correspondence sent to a government institution by the individual that is	

			implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but, for the purposes of sections 7, 8 and 26 and	

			section 19 of the Access to Information Act, does not include (j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including, (i) the fact that the individual is or was an officer or employee of the government institution, (ii) the title, business address and telephone number of the individual, (iii) the classification, salary range and responsibilities of the position held by the individual, (iv) the name of the individual on a document prepared by the individual in the course of employment, and (v) the personal opinions or views of the individual given in the course of employment, (k) information	

			about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services, (l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and (m) information about an individual who has been dead for more than twenty years" ***s. 3***	
Canada Elections Act			"…personal information as defined in section 3 of the Privacy Act." ***s. 2(1)***	

Appendix L : List of Known Data Intermediaries

Name of Company	Website	Brief Description from their website
Data Trust	http://thedatatrust.com.	"…our national file includes over 260 million Americans across all 50 states, and is updated on a daily basis. Our political data inventory goes back decades and includes historical election results, voter registrations, voter scoring projects, census data, list collection and voter contact results." "Your snapshot is delivered as a raw database and updated on a monthly basis with the latest voter list and contact information. If you need the very latest data, please scroll down for our Direct API option."
TargetPoint Consulting	http://www.targetpointconsulting.com.	"…a full service public opinion and MicroTargeting market research firm lead by the nation's foremost experts, seasoned political managers, leading statistical experts, and respected analysts." "MicroTargeting became part of the political lexicon after President George W. Bush deployed our services for his successful 2004 campaign. Since that time, we have remained the leading provider of services for Republican candidates, right of center organizations, and hosts of corporate and association clients." "The next generation of MicroTargeting, our TPC Scoring System, is an analytics, targeting and metrics infrastructure that serves as the backbone of strategic decision-making and uses sophisticated analytical and modeling tools that are highly accurate and extremely flexible. Using this system, our scores can provide key information underlying political, financial and targeting decisions in all spaces including voters, influentials, customers, prospects and jury selection."
Trail Blazr	http://www.trailblz.com.	"Our political campaign software tools track contributions and pledges, manage your volunteer's grassroots efforts, coordinate poll watching via smartphone, handle political campaign finances, coordinate GOTV and polling, generate walk lists and call lists, broadcast mass email, identify and

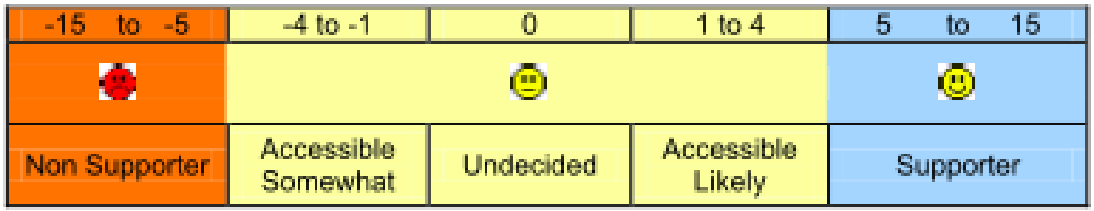
		target voters, increase political fundraising donations and file FEC compliance reports." "Whether you're a Republican, a Democrat or from a third party, our political software is available to you. This means you'll get to use the latest sophisticated techniques used by all parties."
Environics Analytics	http://www.environicsanalytics.ca.	"Using DemoStats or PRIZM5, EA analyzes your best customers (or other groups) by comparing them to a benchmark, typically a base geography or all category consumers. The results identify under- and over- penetrating subsets, and are often the foundation for defining custom target segments." "Using geodemographic profiling as the foundation, we help you create custom target segments by analyzing customer subsets across the data variables and themes most relevant to your business. Because these segments are PRIZM5-based, you can connect them to EA's extensive databases and create comprehensive personas and actionable engagement strategies."
Cambridge Analytica	https://cambridgeanalytica.org.	"Our core database contains information on demographics, consumer and lifestyle habits and political affiliation, as well as unique psychographic information on motivation and decision-making. "We combine this with cross-channel surveying across the United States to probe nuanced or localized issues, and make sure our data is always accurate and up to date." "Our psychographic analysis is a powerful and unique tool for gaining a deeper knowledge of your audience groups by revealing the core personality traits and motivations that drive behavior."
i360	http://www.i-360.com.	"As a first-of-its-kind enterprise, i360 fully integrates and continually updates a database of all 250 million 18+ Americans, including the 190 million who are registered to vote. The information in the i360 database goes beyond voting data and includes hundreds of variables on every individual including survey response data, consumer demographic, lifestyle and behavioral data, census data and precinct level election returns, and more that can be used to determine and reach your targets. "i360's comprehensive data is a unique combination of hard data points and predictive modeling. Our dataset incorporates extensive political identification,

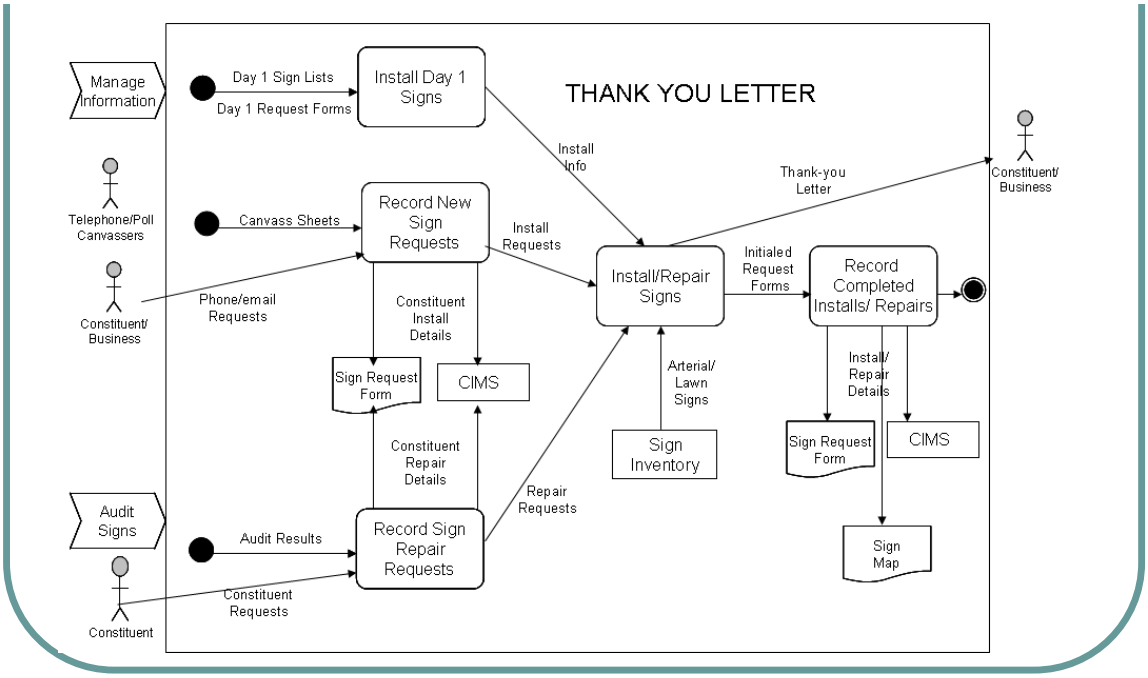
		coalition and membership information collected by way of in-person, phone and online surveys, as well as through partner relationships. In addition, this data is enhanced by our team of data scientists who build and refine sophisticated predictive models (microtargeting) that predict how likely voters are to support issues, candidates and how likely they are to take an action, like voting."
Blue State Digital	www.bluestatedigital.com.	"The campaign mobilized tens of millions of voter contacts and raised $690 million online. BSD's infrastructure and on-call systems experts scaled complex applications, ensuring outlets like barackobama.com handled massive traffic surges in key moments like the Democratic National Convention and presidential debates. Our work helped President Obama bring home 332 electoral votes on election day."
Catalist	http://www.catalist.us.	"Catalist provides data and data-related services exclusively to progressive organizations to help them better identify, understand, and communicate with the people they need to persuade and mobilize. "For a decade, Catalist has been the data utility powering the progressive community. Owned by a trust, we collaborate with data-driven progressive organizations with a variety of goals: issue advocates, organizers, pollsters, analysts, consultants, campaigners, researchers, and more."
Aristotle	http://aristotle.com.	"Aristotle is the global leader in providing technology to political campaigns and organizations, offering a seamless solution for campaign software, voter data, PAC and grassroots software and services. "Since 1983, every U.S. president—from Reagan through Obama—has used Aristotle's solution, in addition to countless senatorial and congressional campaigns, Democratic and Republican state party initiatives and many of the largest PAC and grassroots organizations."
Response Unlimited	http://www.responseunlimited.com.	"…Response Unlimited is all about providing you with exceptional service for whatever is needed for your organization to grow exponentially – so you can accomplish what your mission statement demands of you! "This means picking the right direct mail, email or tele-marketing list, creating the most compelling copy and design, producing your direct mail and

		printed communications for less, getting through the mass of spam so your email message gets read, keeping your lists clean, or flooding those you want to influence with postcards while generating added revenue for your organization."
Acxiom Corporation	http://www.acxiom.com.	"It's about more than making better marketing decisions. If it were that simple, we would have been crowded out years ago by the "me too" companies – the ones who claim to have more data and more insight than anyone else. "So what's our story? We believe our value is in helping our clients do something they never dreamed possible. Giving them that certain moment when clarity becomes confidence. Finding a whole new customer segment. Reaching everyone who needs to be reached. Understanding those tiny market nuances. There's more, of course, but these are the kinds of things that make the difference to our clients – the things that help them sleep at night."
Actionsprout	www.actionsprout.com.	"Build a complete profile of your community members over time by tracking the interactions each supporter has with your Facebook content. Identify your most active, newest or talkative community members so you can give them more of what they like. Upload your existing supporter lists to identify which supporters from your email lists are engaging with your Facebook content — learn what each donor, volunteer, member, or anyone else you have relationships care about and engages with on your Facebook page."
NGP VAN	https://www.ngpvan.com/.	"Nearly every major Democratic campaign in America is powered by NGP VAN, including the Obama campaign's voter contact, volunteer, fundraising and compliance operations in all 50 states. The organizers, fundraisers, and strategists that use our tools work tirelessly to advance important causes and elect inspiring leaders, like President Barack Obama and Senator Elizabeth Warren. From equality + reproductive rights to education + climate change, the passions of these leaders and organizations are shaping a brighter future - and we're passionate about offering them the technology they need to bring their goals to life."
Campaign Grid	http://www.campaigngrid.com/.	"Our data scientists use our patented process to match voter registration records with other data sources, allowing clients to reach their exact

		audience online with less waste and better results." "CampaignGrid's voter-targeting platform allows you to deliver ads across all devices, including mobile, tablets, PCs and addressable TV, with laser-like accuracy."
Nationbuilder	www.nationbuilder.com.	"Your contacts and social media followers are a goldmine, don't ignore them! NationBuilder will match your email lists to social media accounts and unlock a real person you can activate as a donor, customer, volunteer, partner, or whatever you want to inspire them to do."
Google's Political Campaign Toolkit	http://www.google.com/ads/politicaltoolkit/.	"Each campaign message is an opportunity to educate, inspire, and persuade voters. Google helps you make the most of everything you do, with digital advertising solutions from search, display, and video ads to programmatic media buying and powerful analytics tools." "Understanding visitor behavior is the key to a strong campaign website. Google Analytics shows you how visitors are interacting with your site, so you can learn more about donations, volunteers, and what drives your site's traffic."
Segment Metrix from comScore	http://www.comscore.com.	"comScore partners with eight industry leaders to provide audience profiles across a variety of industry-leading segmentation schemes to help you align offline customer characteristics with online behavior. "Segment Metrix provides the ability to analyze and target audiences using any number or combination of segments. Advertisers can identify the core website categories and specific sites to reach the right segments, and publishers can demonstrate site ability to reach target segments."

Appendix M : Images from CIMS database[169]





[169] Susan Delacourt, "Conservative enemies' lists hardly normal political business," (19 July 2013) *The Star*, https://www.thestar.com/news/insight/2013/07/19/conservative_enemies_lists_hardly_normal_political_business.html. The CIMS presentation can be found at www.**thestar**.blogs.com/files/**cims**.ppt.