CANADIAN FEDERAL POLITICAL PARTIES AND PERSONAL PRIVACY PROTECTION:

A COMPARATIVE ANALYSIS

Prepared by Colin J. Bennett
Department of Political Science, University of Victoria, B.C.

Robin M. Bayley
Linden Consulting, Inc.

For the Office of the Privacy Commissioner of Canada

March 28, 2012

DISCLAIMER: The views expressed are those of the authors and not those of the Office of the Privacy Commissioner of Canada

About the Authors

Colin J. Bennett (BA, MA, University of Wales; Ph.D, University of Illinois, Urbana-Champaign) is a Professor of Political Science at the University of Victoria. His research has focused on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published six books on privacy and numerous policy reports on privacy protection for Canadian and international agencies.
http://www.colinbennett.ca

Robin M. Bayley (BA, MPA, University of Victoria), President of Linden Consulting Inc., Privacy & Policy Advisors, has co-authored several chapters and reports on privacy regulation and methodologies such as privacy impact assessments. She helps organizations subject to Canadian privacy laws identify privacy risks and address them with policies and processes, and has assisted privacy regulators develop privacy compliance guides and tools for organizations and the public.

Both authors live in Victoria, British Columbia, Canada.

Contents

INTRODUCTION

This paper presents a comparative overview of the ways that federal Canadian political parties collect, process and disseminate personal information. While the privacy protection laws in most other democratic countries generally regulate political parties, Canada's do not. Several privacy-related incidents associated with the Canadian party system have been covered in the media over the last decade or so, some of which have come to the attention of the Office of the Privacy Commissioner.

This paper is based mainly on documentary evidence, offline and online, rather than on interviews with party officials or other stakeholders. There is, of course, a wide literature on political parties in Canada, and an increasing attention to their use of new technologies, including social media. With the exception of one or two sources, however, there has been scant attention paid to the extent to which parties collect, use and disclose personal information, and the associated risks. In this paper, we focus mainly on the federal level, even though our research suggests that the same issues may exist in many of the provinces.

The paper begins with a discussion of the broader context: the trends in the Canadian party system and our political culture; the emergence of new information technologies and their impact on personal privacy; and the broader international picture concerning the protection of personal data by political parties in other countries. The main section of the paper describes the various kinds of personal data collected and processed by political parties, on voters, contributors, candidates and customers, and describe some of the voter profiling techniques reportedly employed. We then explain how these practices remain largely unregulated by Canadian privacy legislation, and how the parties' own attempts to develop voluntary policies, while welcome, are incomplete and inconsistent.

This report offers an overview rather than a comprehensive and systematic comparison of the practices and the evaluation of the risks. Further research is clearly necessary. It is also hoped that this paper will stimulate a greater public awareness of these issues, as well as heightened attention and engagement by the various stakeholders.

THE CONTEXT

TRENDS IN CANADA'S PARTY SYSTEM

Parties perform a range of different functions in democratic societies. They offer direction to government, formulating and implementing policy; they structure the competition and thereby define democratic choice; they function as agents of political recruitment; they aggregate interests, filtering the multitude of specific demands into manageable programs; and they mobilize voters.[1]

It is with respect to this last role that their influence has waned over the years, in Canada and in most other advanced industrial states. The trend is generally termed "partisan de-alignment" and is typically reflected in the data on declining voter turnout. Turnout reached its lowest level (58.8%) in many decades in 2008. It rose slightly in 2011 to 61.1%. [2] How much of this decline is attributable to disillusionment with the party system is difficult to evaluate, and there are no recent and systematic studies. Nevertheless, a recent comparative analysis of Canadian political parties concludes "it is no exaggeration to say that parties, as organizations, are facing perhaps their biggest challenges in their 150 years or so of existence."[3]

Partisan de-alignment is also reflected in declining membership levels. William Cross and Lisa Young's survey of the members of the five major federal parties in 2004[4] demonstrated that "few Canadians belong to political parties, and those who do belong are not representative of voters generally. The findings also suggest that members are primarily engaged in low-intensity activity and generally contribute little time to party affairs." The study concludes "the parties' inability to engage a significant number of voters as members, particularly younger Canadians, presents an ongoing challenge to their vitality as democratic institutions."[5] Party members were also found to be older, wealthier, better educated and more representative of the elite. The same authors estimated in 2006 "that between 1 and 2 percent of Canadians belong to a political party on a year-to-year basis. This places Canada at the bottom of the list of Western democracies." [6]

---

[1] Rod Hague and Martin Harrop, *Political Science: A Comparative Introduction* (Palgrave Macmillan, 2010), p. 204.

[2] Elections Canada, "Voter Turnout at Federal Elections and Referendums" at: http://www.elections.ca/content.aspx?section=ele&dir=turn&document=index&lang=e

[3] Alain-G. Gagnon and A Brian Tanguay, *Canadian Parties in Transition* (Peterborough: Broadview Press, 2007), p. 7.

[4] The Conservative Party of Canada, New Democratic Party of Canada, the Liberal Party of Canada, Green Party of Canada and the Bloc Québécois.

[5] William Cross and Lisa Young, "The Contours of Political Party Membership in Canada," *Party Politics*, (July 2004) vol. 10 no. 4: 427-444

[6] William Cross and Lisa Young, "Are Canadian Political Parties Empty Vessels? Membership, Engagement and Policy Capacity," *Choices,* Vol. 12. No 4 (June 2006), p. 16: at: http://www.irpp.org/choices/archive/vol12no4.pdf

A more recent study of the nature and causes of political disengagement, based on focus group studies, concludes that, "not only is voter turnout decreasing, but every year fewer Canadians are getting involved in other kinds of political activities, like joining or donating to political parties, signing petitions or attending protests."[7] This study sees a growing gap between the politically engaged and the disengaged. Of course none of this literature addresses the question of citizen trust in the parties' use of personal information. But the general message does suggest that privacy-related controversies might only increase the general disconnect between many Canadians and their party system.

Particular aspects of our first-past-the-post electoral system are also relevant to this debate about privacy and political parties. Canada's electoral system exaggerates the legislative seats for some parties and reduces it for others. Therefore, small swings in electoral support in key ridings can translate into a disproportionate accumulation of seats. Ken Carty describes the effects in these terms: "The first-past-the-post electoral system, which privileges the imperatives of geography over other bases of popular mobilization, has been central to the persistence of this pattern. Based on a winner-take-all principle, and offering the prospect of single-party majorities, it rewards the vote-vacuuming strategies of brokerage parties and discriminates against those that seek to articulate and represent the clearly defined interests of a particular social group."[8] In this environment, parties believe they need ever more precise information on voter behavior and intentions, so that they might target more precisely defined segments of an electorate in key competitive ridings.

Political party financing rules are also relevant to the debate and have an impact on the quantity and type of personal information captured and used by parties. The current Conservative government will end the $2 per vote subsidy that currently plays a very significant role in the financing of political parties. The subsidy will be phased out over the next three years effective April 1, 2012.[9] The removal of the subsidy will presumably place greater pressure on party fund-raising efforts, and on their perceived need to build more comprehensive databases of actual and potential contributors. The reform also is likely to affect the parties differentially, given their different contributing bases.

Political parties and politicians have continually contended that their needs for personal information are special and have succeeded, over the years, in ensuring that they are not subject to the privacy protection rules that now apply to governmental and commercial organizations in Canada. To be sure, the public interest in promoting widespread participation in our democratic institutions requires parties to have access to and use personal information, and poses some difficult challenges for privacy advocates and regulators. In general terms, the debate centers on the balance between the two values of personal privacy and political participation, both of which are crucial to the strength of

---

[7] Heather Bastedo, Wayne Chu, Jane Hilderman and Andre Turcotte, *The Real Outsiders: Politically Disengaged Views on Politics and Democracy*. (Samara Democracy Reports, December 2011) at: http://www.samaracanada.com/docs/default-document-library/sam_therealoutsiders.pdf

[8] R. Kenneth Carty, "The Shifting Place of Political Parties in Canadian Political Life," *Choices,* Vol. 12. No 4 (June 2006), p. 7: at: http://www.irpp.org/choices/archive/vol12no4.pdf

[9] Amendments to the Canada Elections Act, s. 181, S.C. 2011, c. 24, s.181, at: http://laws-lois.justice.gc.ca/eng/acts/E-2.01/nifnev.html .

our democracy, and to the trust that people have in our political system. So an appropriate balance needs to be struck. As Philip Howard and Daniel Kreiss conclude: "Given the unique challenges to democratic practice posed by the data practices of parties and candidates in mature democracies, what is needed are institutional and technical innovations that secure political privacy while promoting participation, deliberation, and competition."[10]

Moreover, the downward trend in democratic participation could be accelerated if a significant loss of confidence in the parties' respect for personal privacy were to occur. A well-publicized privacy breach could not only hurt the specific party, it could also damage the other parties and the whole political system. Potentially, the public disclosure about a party's personal information practices, if widely seen as unethical or unreasonable, could create a backlash against the parties and the democratic system as a whole.

These various conditions point to the need for any rules about political parties' use of personal information to be:

- Sufficiently sensitive to the parties' crucial role in mobilizing the electorate;
- Not seen to favor one party over another;
- Sufficiently general to embrace the possibility that the party system today may not be that of tomorrow;
- Sensitive to the innovations likely to be facilitated by rapidly evolving technologies;
- Generally consistent with accepted privacy principles that govern individuals' relationships with other organizations; and
- Framed in such a way that they enhance potential voters' trust of political parties, the party system and the democratic process.

TRENDS IN PERSONAL INFORMATION SURVEILLANCE

More personal information, of increasing sensitivity and scope is collected and stored on more and more people, by more and more organizations than at any time in human history. Various trends are at work. Monitoring of individuals now has a *routine* character, assumed as being a condition of participation in modern life and as the way that we engage with modern public and private organizations; one does not have to be a "suspect" to be subject to monitoring. More traditional surveillance by the state has been supplemented by increasingly complete *profiling* of our consumer behavior, desires and values, to anticipate our future actions. Organizations are not only interested in who we are, and what we are doing, but also where we are doing it; our *mobility and location* is increasingly tracked. New technologies are not only mobile, they are also *miniaturized* and increasingly embedded in material objects and also our bodies through biometric

[10] Philip N. Howard and Daniel Kriess, *Political Parties and Voter Privacy: Australia, Canada, the United Kingdom and United States in comparative perspective*, First Monday, Volume 15, Number 12 - 6 December 2010, at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2975/2627

devices. Advances in technologies such as facial recognition, increase the chances of *re-identification*, confusing the distinctions between personally identified information and personally identifiable information. It is not just big public and private organizations involved in this surveillance, but increasingly we watch each other*; peer-to-peer monitoring* or "horizontal" surveillance in social networking environments is commonplace. And these trends are inescapably *global* in character; the actions of one organization or state can have ripple effects around the world. [11]

Public concerns about these trends are also high, although it is difficult to generalize about a complex issue, and individuals clearly respond in different ways to the collection of their personal information in different contexts. Furthermore, Canadians' anxieties about these questions relate closely to whether they have a prior sense of trust in the organization concerned. Nevertheless, the overall pattern of findings over thirty years of surveys of the Canadian public suggests that a large majority of citizens are deeply concerned about their privacy, have increasing worries about the intrusiveness of new technologies, and expect strong privacy laws to be enforced.[12] In recent years, these concerns have also been exacerbated by the constant flow of stories in the news media about data breaches. The loss and theft of personal data brings home the risks and vulnerabilities of living in a society where huge volumes of personal data are captured, processed, and communicated using increasingly sophisticated technologies.

In response, most countries have passed information privacy statutes, like the Canadian *Privacy Act* or the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Recent research suggests that there are now over 80 countries in the world, which have some form of comprehensive data privacy law.[13] This diffusion of legislation is also attributable to a number of international agreements from organizations such as the Council of Europe, the European Commission, and the Organization for Economic Cooperation and Development.[14] Increasingly, there has emerged a common consensus on what it means for the modern organization in western democracies to process personal data responsibly. Those expectations are expressed in a set of "fair information principles." The codification obviously varies, and there are important exemptions and derogations. The Canadian expression of these principles is expressed in Schedule One of PIPEDA, originally negotiated as the Canadian Standards Association's *Model Code for the Protection of Personal Information*:[15] These principles are:

---

[11] There is, of course a huge literature on these trends. A good contemporary overview is David Lyon, Kevin Haggerty and Kirstie Ball, *The International Handbook of Surveillance Studies* (London: Routledge 2012)

[12] See the Harris/Decima Poll, commissioned by the Office of the Privacy Commissioner of Canada, *2011 Canadians and Privacy Survey* (March 31, 2011) at: http://www.priv.gc.ca/information/survey/2011/por_2011_01_e.cfm

[13] Graham Greenleaf, *Graham Greenleaf's Global Table of Data Privacy Laws, version 10, November 2011* at: http://www2.austlii.edu.au/%7Egraham/DP_Table/DP_TABLE.html

[14] See Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006).

[15] Canadian Standards Association, *Model Code for the Protection of Personal Information* (Q830) at: http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code

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.

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.

3. Consent

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

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.

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.

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.

7. Safeguards

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

8. Openness

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

9. Individual Access

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.

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.

It is now widely argued that good organizational privacy practices foster trust in citizens and in consumers. To a significant extent, the implementation of these principles is in the interests of any organization as well as those of the individual.

INTERNATIONAL EFFORTS TO PROTECT PERSONAL INFORMATION HELD BY POLITICAL PARTIES

The notion of "political privacy" has a long tradition within our democratic cultures. The secret ballot is enshrined as a constitutional right in most Western societies. This principle protects our fundamental voting choices from bribery, intimidation or harassment. Moreover, and in the context of modern privacy law, political opinions are invariably defined as special or sensitive categories of personal data, which may only be processed under clearly defined conditions. For instance, the Council of Europe's Convention 108 on the "Protection of Individuals with Regard to Automatic Processing of Personal Data states that: "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards."[16] Provisions such as these stem from the sensibilities of countries with more recent traditions of authoritarian rule, and from the memories of the repression that did, and does, occur when political privacy is not respected.

As we will show below, political parties in many countries collect great quantities of data on the behavior and attitudes of individual voters, donors, candidates and employees. So what protections exist for these data? Are the activities of political parties covered by privacy legislation? For the most part, the answer is yes, but there are important exceptions, including Canada.

We begin with the situation in Europe, where a Directive, designed to harmonize protections across the 27 states of the EU, has governed personal data protection law since 1995. The intention is to replace this Directive with a new Regulation, a draft of which was published in January 2012.[17] In both documents, political parties are considered "data controllers" expected to abide by the basic set of fair information principles. Furthermore, under Article 8, information on political opinions is defined as a "special category of data" which may only be processed under clearly defined conditions.[18] Clause 36 in the preamble of the 1995 Directive, however, states: "Whereas

[16] The Council of Europe's Convention 108 on the *Protection of Individuals with Regard to Automatic Processing of Personal Data*, (Strasbourg: Council of Europe, 1981) at http://conventions.coe.int/treaty/en/treaties/html/108.htm

[17] *Proposal for a Regulation of the European Parliament and of the Council for the protection of individuals with regard to the processing of personal data and on the free movement of such data* COM (2012) 11 final at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[18] Article 8 of the European Union's *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of*

where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established." In practice, this means that political parties are allowed to process personal data for legitimate purposes of political communication, but that they must also abide by the general data protection rules, and keep that data secure, not use it for illegitimate purposes, be transparent about purposes, allow rights of access and correction and so on.

However, the direct targeting of potential voters by political parties is still not a widespread practice in countries outside North America. Parties still tend to communicate through mass messaging, rather than through the micro-targeting of individual voters or specific neighborhoods. An extreme case is that of Japan, where long-standing Japanese election law prohibits Japanese politicians from making use of any electronic media for campaigning in the 12 days prior to an election. Political candidates are allowed to have websites during this time, but they are not allowed to update them or post material via Facebook or Twitter.[19] Therefore, in the absence of extensive databases on voter attitudes and affiliations, the kinds of privacy issues that arise in North America, and are described below, tend not to arise to the same extent in other countries – at least not yet.

An important exception to this generalization is the United Kingdom, where the actions of political parties engaged in "direct-marketing" have come under close scrutiny as a result of complaints to the Information Commissioner's Office (ICO): "The complaints we have received reveal that individuals find unwanted direct marketing and unwanted contact from political parties in particular, to be extremely annoying. This is more likely to be the case where more intrusive means of contact are used or the individual has previously objected to marketing and where they are opposed to your views. In recent years [the ICO] have investigated complaints about political parties using direct marketing and on occasion we have used our enforcement powers to prevent the party doing the same thing again." The Information Commissioner has issued specific "Guidance for political parties for campaigning or promotional purposes" so that parties could act in compliance with both the UK *Data Protection Act* of 1998 and the *Electronic Communications Regulations* 2003.[20]

In other countries where political parties are encompassed by comprehensive information privacy laws, exemptions are typically included for information that is collected and processed in the course of an elected representative's democratic duties. In New Zealand, for instance, there is an important exception in the application of the data protection law for parliamentary privilege. However, the former Commissioner, Bruce Slane, as early as

---

Such Data. Brussels: European Commission, 1995 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[19] C. Masters, "Japan's Twitter-Free Election Campaign." *Time*. August 18, 2009: at: http://www.time.com/time/world/article/0,8599,1917137,00.html.

[20] The Information Commissioner's Office (ICO) has produced guidance material, *Guidance for political parties for campaigning or promotional purposes* at: http://www.ico.gov.uk/for_organisations/sector_guides/political.aspx (click on "promotion of a political party", under Marketing). In the same source is found guidance on specific data protection issues which relates to MPs and local councilors.

1997 expressed some considerable concerns about the use of the New Zealand electoral roll for "non-electoral purposes." He argued: "Officials might also find it useful to consider whether any new administrative safeguards are necessary to ensure that the electronic controls which currently exist in law are being complied with. This might involve randomly auditing the activities of political parties, researchers, local authorities and any others who are granted access to the electoral roll in electronic form."[21]

As a federated country with a Westminster parliamentary system, Australia provides perhaps the best lessons for Canada. Political parties are explicitly exempted from the Australian Privacy Act, even though the legislation does define sensitive information as including membership of a political association, philosophical beliefs, and political opinions. At the time of the passage of the law in 2000, the exemption was justified on the grounds that freedom of political communication was important for the Australian democratic process. The Privacy Commissioner at the time objected, as did other privacy advocates. As a result of a number of media stories about the inappropriate treatment of personal data by parties, there is significant pressure to bring them within the legislative framework. In 2008 the Australian Law Reform Commission (ALRC) wrote the following:[22]

> There are compelling policy reasons—as well as strong stakeholder support—for applying privacy obligations to registered political parties and political acts and practices. However, any lessening of the scope of the political exemption must take into account the strong public interest in promoting Australia's system of representative democracy. The ALRC has identified three options for balancing these competing interests:
>
> - removing the political exemption, subject to the relevant constitutional limitations;
> - providing limited exceptions to—rather than exemptions from—the *Privacy Act* for registered political parties and political acts and practices; and
> - requiring registered political parties and other entities engaging in political acts and practices to develop information-handling guidelines, in consultation with the OPC [Australian Office of the Privacy Commissioner].

The ALRC went on to recommend that:[23]

> In the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community. Unless there is a sound policy reason to the contrary, political parties and agencies and organisations engaging in

[21] Report by the Privacy Commissioner to the Minister of Justice on the Electoral Act 1993, April 29, 1997 at: http://privacy.org.nz/electoral-act-1993/ Mr. Slane reported concerns about information matching using the electoral roll. He also suggested the rules for the electoral roll "were established in an earlier age and which could usefully be reconsidered in the light of today's approach to privacy of personal information".
[22] Australia Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, para. 41 at: http://www.austlii.edu.au/au/other/alrc/publications/reports/108/41.html#Heading25
[23] Ibid, para 41.54.

political acts and practices should be required to handle personal information in accordance with the requirements of the *Privacy Act*.

Before amending the law, however, the ALRC recommended "the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act."[24] To date, no guidance has been issued.

The United States is the clear outlier. Privacy statutes in the US take the form of sets of rules directed towards specific sectors, such as health, banking, and consumer credit. The result is a complicated patchwork of federal and state laws with significant gaps. Furthermore, the activities of political parties are protected by the body of constitutional law stemming from jurisprudence under the First Amendment (freedom of speech). The Supreme Court has not only protected political communication, but has also found that the raising and spending of money to support that communication is also largely protected from regulation.[25]

In addition, the availability of much publicly available data means that parties in the United States appear free to collect, process and disseminate vast quantities of personal data on voters, candidates and donors. Paralleling developments in private sector marketing, the last decade has indeed seen dramatic developments in the scale and sophistication of technologies for reaching potential voters and donors in the US, gleaning more refined information about them, and building list management and profiling databases.[26] There is now a huge business in the US in "voter intelligence."[27] A few of the more prominent practices revealed during the current American electoral cycle include:

- Smart-phone applications for political canvassers such as the "Organizing for America App for the i-Phone" which gives campaigners "everything you need to canvass in the palm of your hand: Lists of neighbors to talk to; Interactive maps; Share news, photos, videos, and information right at the door; and real-time reporting of how many doors you've knocked and how the conversations went."[28]
- Targeted online ad software such as Google's Political Campaign Toolkit[29]
- Targeted e-mail campaigns matching IP addresses with other data sets showing party affiliation, donation history, race, religion and income level. [30]

---

[24] Ibid, Recommendation 41-4.
[25] The most recent, and controversial case, is that of *Citizens United v. Federal Election Commission*, 558 US 205 (2010)
[26] For analysis of new electoral technologies see the website of the Ace Project, *Elections and Technology*: http://aceproject.org/ace-en/topics/et
[27] See the various products available from one company's website, Aristotle, Smarter Tools for Politics, at: http://www.aristotle.com
[28] See Introducing the Obama 2012 Campaign App at:
: http://my.barackobama.com/page/content/iphone2010/
[29] Google, Political Campaign Toolkit at: http://www.google.com/ads/politicaltoolkit/
[30] Kate Kaye, "Political Data Firms Push Controversial IP Targeting," *Clickz*, January 17, 2012 at: http://www.clickz.com/clickz/news/2137312/political-firms-push-controversial-ip-targeting See also Elect Strategies, Persuading Voters, at: www.electstrategies.com

- Sophisticated market segmentation strategies aligning online and offline behavior including "insights into the online behavior of U.S. voters and non-voters by political affiliation through segments based on voter registration, commercial, and census data for more than 265 million persons across the U.S."[31]
- Sophisticated strategies to plan campaigns through social media, target likely voters and donors, and measure likely impact and engagement.[32]
- Extensive use of "robocalling" and "robotexting" in state, local and federal campaigns, even producing national "do not call" lists expressly designed to control these practices.[33]

So what then is the situation regarding the processing of personal data by Canadian federal political parties, and what protections for privacy exist?

[31] A new product entitled Segment Metrix 2.0 from Comscore at: http://www.comscore.com/Products_Services/Product_Index/Segment_Metrix_2.0

32 IContact study of social media and political campaigns, Small Businesses Can Learn from Candidates' Social Media Campaigns, at: http://www.icontact.com/social-media-and-political-campaigns

[33] See Citizens for Civil Discourse's Stop Political Phone Calls campaign at: http://stoppoliticalcalls.org

CANADIAN POLITICAL PARTIES AND PERSONAL INFORMATION

The *Canada Elections Act* (CEA) defines a political party as "an organization one of whose fundamental purposes is to participate in public affairs by endorsing one or more of its members as candidates and supporting their election." There is no legislation regulating the formation of federal political parties. However, once a party exists, it may apply to be registered under the *Elections Act* and be formally recognized and regulated. Registration requires the party to provide, among other things, the names of officers, the leader, auditor and the names and addresses of 250 electors as well as a declaration by each of these 250 electors that they are members of the party and support its registration.

The Act imposes obligations and provides advantages to registered parties. For example, registered parties must file annual financial returns and disclose political contributions and expenditures. It also allows the party to have its name below that of its candidates on the ballot paper. Party affiliations are seen as a sort of certification that candidates hold certain beliefs and will work toward specified objectives, as adherents of a party platform.

According to Elections Canada, as of September 28, 2011, eighteen separate parties are listed as registered political parties, which vary widely in public profile, administrative sophistication and geographic base. For the purposes of this analysis, we concentrate on those parties which have representation in the current Parliament: Conservative, New Democratic (NDP), Liberal, Bloc Québécois and Green .

So what personal information do these parties collect, and from what sources? How do they use, safeguard and disclose personal information? Given their exemptions from access to information and privacy statutes, and natural tendencies not to share details about information management practices within a competitive political environment, it is impossible to provide an accurate picture. We certainly know the personal information they are provided by Elections Canada, under the authority of the CEA. In addition, there is considerable evidence that they also collect and process personal information on donors, supporters, employees and volunteers, as well as on the small number of individuals who may purchase party merchandise. And they obviously need this personal information for some essential and legitimate purposes within our democratic system. But what further do we know about the nature and quantity of personal information collected?

INFORMATION CONTAINED ON THE LISTS OF ELECTORS

Elections require personal information in order to ensure that only qualified electors are allowed to vote, (eligible Canadian citizens aged 18 and over), and to administer the one person, one vote principle.

Section 44 of the CEA provides that: “The Chief Electoral Officer shall maintain a register of Canadians who are qualified as electors, to be known as the Register of Electors”. The register contains the surname and given name of each elector included in it, his or her sex, date of birth and civic and mailing addresses. Each elector is assigned a

unique identifier, randomly created by Elections Canada and used only for the purposes of the register of electors. Elections Canada has legislative authority to enter into information sharing agreements with provincial agencies, such as vital statistics bodies and other electoral management bodies, to update and verify the accuracy of the list.

The *raison d'être* of the National Register of Electors is the production of lists of electors, both for the purposes of elections (s. 93, 104.1, 105, 107, 109) as well as for distribution on an annual basis to Members of Parliament and, on request, registered parties (s. 45). Inclusion in the Register of electors is optional. However, an elector who does not wish his or her name to be included in the Register of Electors but still wishes to vote must register during the election period for his or her name to be added on the list of electors. Not all information in the Register is shared by Elections Canada with political parties.

As indicated before, during an election, returning officers (the election officials responsible for the running of the election in each of Canada's 308 electoral districts) produce lists of the electors, disaggregated by each poll, for their electoral district or riding, using the data contained in the national register of electors. The preliminary lists of electors are produced as soon as possible after the issue of the writ. Pursuant to s. 93 of the Act, they contain only the name and address of each elector as well as their unique identifier. The returning officer distributes a paper copy and an electronic copy of the lists to each candidate in the electoral district who requests them (s. 94). An electronic copy of the lists of a particular electoral district may be forwarded to each registered party or eligible party who requests it. Following revision of these lists by the returning officer and his or her staff, candidates who request it may obtain an electronic copy of the updated preliminary lists of electors (s. 104.1).

Revised lists of electors are prepared on the day before the start of advance polls for use at the advance polls (s. 105) and official lists of electors are prepared on the third day before polling day for use on that day (s. 106). A paper and electronic copy of the revised and official lists are delivered to each candidate. These lists contain for each elector on the lists, their surname and given name, their civic and mailing address and the unique identifier (s. 2, definition of list of electors). Deputy returning officers responsible for the administration of the vote in each polling station receive a copy of the list of electors for the polling division that contains the elements listed above as well as the sex and date of birth of electors. These two pieces of information were added by Parliament in 2007 to facilitate identification of individuals and provide greater integrity to the voting process. The lists prepared for election officials are not given to candidates' representatives.

The final lists of electors are prepared for each electoral district without delay after the election (s. 109). This list includes voters who registered at the polls. These lists are given to registered parties that ran a candidate in the electoral district, as well as to the member who was elected for the district. These lists contain the electors' surnames and given names, their mailing and civic addresses and their unique identifier.

Under s. 45, the Chief Electoral Officer (CEO) is also required to provide members of Parliament, on an annual basis, with a list of the electors of their electoral district. This list contains the registered electors' surname, given names, civic and mailing address and

unique identifier. As is the case for all other lists given to political entities, it does not include the sex or date of birth of the electors. On request, the list of electors of a particular electoral district may also be provided in electronic form to political parties who endorsed a candidate in a particular electoral district in the last election. The Act provides, at s. 110, that the Members of Parliaments (MPs) and registered parties who receive a copy of lists of electors may use them to communicate with electors, including using them for soliciting contributions and recruiting party members. Only parties who support candidates in all electoral districts (generally speaking the four largest parties) receive copies of these lists; of course, the Bloc Quebecois receives copies of the lists only for Quebec.

The Act specifies at sections 110 and 111 how parties, candidates and MPs may use the lists of electors, and stipulates the prohibitions related to the same lists. Parties, candidates and MPs are expressly authorized to use the lists for communicating with electors, including using them for soliciting contributions and recruiting members (s.110). However, the Act provides (at s. 111(f) that no person may knowingly use personal information that is recorded in a list of electors for a purpose other than the one specified above or at a federal election (or referendum), and there are penalties for failing to comply in Part 19 of the Act.

The preliminary voters lists included 24,257,592 electors for the 2011 federal general election.[34] Additional voters were added to the lists as a result of revision or registration at advance polls or on polling day. There are on average approximately 200 lists per electoral district communicated to election officers. Political parties who support candidates in all electoral districts (generally speaking the 4 largest parties) receive copies of all these lists for every poll within the electoral district. As noted above, the parties only receive name, address and unique identifier.

INFORMATION FOR FINANCIAL REPORTING AND CONTRIBUTIONS

Beginning in 2004, all registered political parties could qualify for quarterly allowances drawn from public funds. To have been eligible, a registered party must have received at least 2% of the valid votes cast in the general election preceding the quarter, or at least 5% of the valid votes cast in the electoral districts in which the party endorsed a candidate. Up to now, only the five larger parties have qualified for this allowance.[35] As noted above, the subsidy will be gradually phased out beginning in April 2012.

[34] Elections Canada, "Voter Turnout at Federal Elections and Referendums," http://www.elections.ca/content.aspx?section=ele&dir=turn&document=index&lang=e
[35] Elections Canada, *Did you know?* at: http://www.elections.ca/content.aspx?section=res&dir=did&document=index&lang=e

The following table indicates that a large number of Canadians provide parties with personal information for the purposes of making donations, but the number of individuals (150,000) is a tiny fraction of the population of over 34 million. 2010 was not a national election year, and therefore, it is likely to represent lower contribution activities than the following general election year, but 2011 figures are not yet available.

Select Figures from 2010 Annual Financial Returns of parties with representation in the House of Commons[36]

	amount of contributions	number of contributors*
Conservative	$ 17,416,856	95,010
NDP	$ 4,363,086	22,807
Liberal	$ 6,402,210	32,448
Bloc Québécois	$ 641,613	5,855
Green	$ 1,291,687	8,961
Total	**$ 30,115,452**	**165,081**

Notes:

* No attempt has been made to remove individuals contributing to more than one party or contributors making more than one contribution to the same party.

All political entities that receive donations[37] must report them to Elections Canada. The Act requires, in s. 424(2)(c) that the report provide the name and address of each contributor who made contributions of a total amount of more than $200 to the registered party, that total amount, as well as the amount of each such contribution and the date on which it was received by the party. The name, city, province and postal code of contributors as well as the dates and amounts of the contributions are made public. For the purpose of issuing tax receipt and audits, the parties must keep records of all of the contributions they receive.[38]

INFORMATION ON VOTER ATTITUDES, AFFILIATIONS AND INTENTIONS

From various sources, we can begin to build some idea of how data on voter identification is captured and processed. The starting-point appears to be the poll-by-poll results released by Elections Canada after the prior election. These are searchable online, and provide a listing of polls in each riding, and the raw number of votes cast for each candidate at that poll. [39] Parties then can cross-reference this data with the list of electors

[36] Elections Canada, Financial Reports, Registered Parties Financial Returns, Annual Return Summaries, by party,available from http://www.elections.ca/scripts/webpep/fin2/select_parties.aspx?entity=6&lang=e
[37] This includes parties, riding associations, leadership contestants, and individual candidates.
[38] See s. 404.4 for a description of the regime applicable to contributions equal to or less than $20.
[39] Elections Canada, 41st General Election - Poll-by-poll results at:
http://www.elections.ca/scripts/resval/ovr_41ge_pollbypoll.asp?lang=e

and addresses provided by Elections Canada. These data provide the "basement starting point" for building more complete databases on voters' attitudes, affiliations and intentions.[40]

We know that each of the main political parties has developed their own customized databases, using off-the-shelf voter list management software, either for download to a desktop personal computer or laptop, or for access through the Internet.[41]

The Conservative Party of Canada uses the Constituent Information Management System (CIMS) reportedly the first centralized Canadian system for voter management developed back in 2004.[42] The Liberal Party has introduced "Liberalist" a "Voter identification and relationship management system" – similar to the US Democratic Party's Voter Activation Network. That system, we are told, will: "Easily keep track of your membership levels, donors, sign requests and supporters; manage your local campaign team, events and volunteers; strategically contact voters by telephone, e-mail, canvass or direct mail; map out support and opposition across your riding down to a household level; track key or emerging local and national issues; facilitate grassroots campaigns using Obama's neighbour-to-neighbour model; develop micro-targeted and demographic-specific messaging."[43] The NDP uses its own custom database system called "NDP Vote."

In the absence of an oversight authority that is authorized to audit or investigate these systems, evidence on what is included in these databases tends to be anecdotal and speculative. The practices of the parties probably also differ in some significant ways. Howard and Kriess suggest that parties might capture information about voters from a variety of sources including: publicly stated positions (such as letters to local newspapers or postings on blogs); public petitions; telephone polling; canvassing by phone, writing or on the doorstep; donor databases; and by the observations of party volunteers who record the addresses at which opposition election signs are posted. Inferences about party preferences and voting intentions (strong, leaning, or none) can be gleaned from many places. From these sources, parties can track key issues and voting trends for use in polling, advertising, direct mailing and strategy formation, especially in marginal seats.[44] These data are now considered crucial for parties in making decisions about how, when and where to target their limited resources.[45] Given the number of Canadian elections over the last ten years, the data have been refreshed quite regularly.

---

[40] Janet Davison, quoting Geoff Norquay, Earnscliffe Strategy Group: "Robocalling and the art of finding voters," CBC News, February 29, 2012 at: http://www.cbc.ca/news/politics/story/2012/02/29/f-voter-identification.html

[41] One of the best media reports is a 2008 CBC segment t by Keith Boag," Voter Databases" cached at: http://video.google.com/videoplay?docid=1277939542743658378

[42] The story of the development of CIMS, in association with Responsive Marketing Group Inc., is reported by Tom Flanagan, *Harper's Team: Behind the Scenes in the Conservative Rise to Power* (McGill-Queens: 2007)

[43] Liberal Party of Canada, Overview page, What is Liberalist? at: http://liberalist.liberal.ca/learn/overview/

[44] Some of this anecdotal evidence is reported in Howard and Kriess, pp. 17-19.

[45] "Robocalling and the art of finding voters," Janet Davison, CBC News, February 29, 2012 at: http://www.cbc.ca/news/politics/story/2012/02/29/f-voter-identification.html

The party, which provides the most detail about the operation of its voter management system, is the Liberals. The Liberalist website contains a significant amount of information for party members in the form of FAQs and User Guides. We know, for instance that Liberalist provides three levels of access: Basic (for new users); Intermediate (for those allowed to a Search facility); and Advanced (allowing for the creation of lists and contacts).[46] Liberalist is divided into two groups: MyVoters, the complete Elections Canada list of voters in the riding; and SharedContacts, anyone who may have had contact with the Liberal campaign in that district. The User Guide then offers instructions on creating and managing lists, door canvassing, phone canvassing, robocalling, e-mail "blasting," volunteer and event management, and get-out-the-vote strategies.

Some of these practices are long-standing and uncontroversial. But it is questionable that the average voter would expect doorstep conversations with party canvassers about current issues to be recorded, along with their identity and address. Even raising concerns or asking the representative about the party's policies on pensions, schools or health care can be done in a way that divulges employment, family and health status. Sharing such information with canvassers entails privacy risks. Canvassers may live in the same community and may be temporarily active in the party and not subject to training about the appropriate use of personal information. Parties are also beginning to use applications for their mobile devices, which allows them to send information directly from their canvassing activities to central databases. The Liberals, for instance, are now reportedly using the Voter Activation Network's "MiniVan" app for the i-Phone and i-Pad.

Often we get anecdotal reports on party practices from ex-politicians. Garth Turner was dismissed from the Conservative caucus in 2006, and ultimately crossed to the Liberals. He later blogged about the Conservative Party's use of the CIMs database in the 2004 campaign: "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."[47] It was reported at the time that the Liberals and the NDP have separate databases for voter tracking and constituency management.[48]

Of course, some voters will have individual contact with their MPs from time to time. If a voter or potential voter discloses personal information to his or her MP in order to seek assistance with a problem, that MP might legally disclose the information in a number of ways, including to a relevant minister or agency, or in the course of parliamentary proceedings. That disclosure would generally fall under the doctrine of parliamentary privilege. Should that MP enter the personal information into an electoral database for the

---

[46] The Liberalist User Guide at: http://liberalist.liberal.ca/learn/user-guide

[47] Turner, Garth. *Nowhere to Hide* (October 12) 2007. Available at: http://www.garth.ca/2007/10/12/nowhere-to-hide/

[48] "Tory database draws ire of privacy experts" at: http://www.ctv.ca/CTVNews/QPeriod/20071018/tory_privacy_071018/

purpose of party fundraising, however, this use or disclosure would presumably fall outside the doctrines of parliamentary privilege, and would also probably fall outside the reasonable expectations of the Canadian electorate. Could it also have a chilling effect on voters' willingness to contact their elected representatives?[49] Furthermore, if communications with elected officials are merged with voter data, the potential for differential treatment based on political support is a serious risk that could undermine the integrity and fairness of our representative system. On the other hand, there is nothing in current Canadian law that prevents this form of data-sharing or data linkage.

Parties may also populate their voter management databases from non-identifiable, but geographically precise information from other sources, such as Statistics Canada. They have also begun to use geo-demographic databases available from marketing companies.[50] Employing systems such as "Prizm" from Environics Analytics, the parties can break down a population in a critical riding into a large number of types.[51] It has been reported that the Conservative Party has been combining these data with internal polling information since the 2006 election to allow more and more refined segmentation according to a host of demographic and attitudinal variables, permitting ever more precise targeting of specific messages.[52]

The power and implications of these "micro-targeting" technologies is readily evident from the marketing pitches on the Environics website: "With consumer segmentation, businesses and not-for-profits can classify their customers according to shared demographic, lifestyle and behavioral traits. Our pioneering PRIZM C2 segmentation system captures the diversity of Canada's population using 66 segments based on the most important drivers of consumer behaviour: demographics, lifestyles and values."[53] For example: "Gaybourhoods provides neighbourhood-level data on the propensity of residents to be gay and details the spending potential of the gay population for key categories. Derived from a variety of sources, Gaybourhoods is currently available for the first wave of major metros, including Toronto, Ottawa, Calgary and Vancouver."[54]

Finally, of course, parties are becoming increasingly sophisticated in their uses of social media to get targeted messages across to supporters. The political use of social media has generated a good deal of research in Canada, as elsewhere.[55] The extent to which parties process and mine the enormous amounts of user-generated data from sites such as

---

[49] Ibid.
[50] Valpy, Michael. "What the Tories Know About You; Conservatives Are Targeting Canadians Like Never before with Detailed Databases and Profiles of Fictional Voters to Convert" (September 12). *Globe and Mail*, at: http://www.theglobeandmail.com/servlet/story/RTGAM.20080912.welxnpolling13/BNStory/politics/home
[51] Environics Analytics, Segmentation Systems at: http://www.environicsanalytics.ca/data_consumer_segmentation.aspx
[52] Joe Friesen, "'Micro-targeting' lets parties conquer ridings, one tiny group at a time", ," *The Globe and Mail*, April 22, 2011 at: http://www.theglobeandmail.com/news/politics/micro-targeting-lets-parties-conquer-ridings-one-tiny-group-at-a-time/article1996155/ .
[53] Environics Analytics, Segmentation Systems at: http://www.environicsanalytics.ca/data_consumer_segmentation.aspx
[54] Ibid.
[55] Tamara Small, 2010. "Canadian Politics in 140 Characters: Party Politics in the Twitterverse." *Canadian Parliamentary Review*, Fall 2010: 49 – 45 at: http://www.revparl.ca/33/3/33n3_10e_Small.pdf

Facebook and Twitter is less well known. Numerous companies now track social media for marketing purposes. Those data already constitute a rich source of "voter intelligence" in the United States and have become, according to some sources, a key strategic advantage for the Obama campaign in the 2012 election.[56]

All the websites of the major parties have links to a variety of social media platforms. To differing extents, these sites encourage the sharing of personal information. For instance, the exercise of the "Like" button in Facebook displays the icon of that party on that individual's social media page, perhaps unintentionally displaying that individual's political beliefs. Friending a political party on Facebook without the user implementing the appropriate privacy controls can result in the users' name and photo being listed on the parties' social media page. Thus, the practices of Canada's political parties, and the privacy rights of their members, are closely related to the privacy policies and mechanisms embedded within these social media platforms, as well as to the privacy choices that individuals make according to varying degrees of knowledge about privacy and sophistication about the technology.

INFORMATION ON CANDIDATES, VOLUNTEERS AND EMPLOYEES

There is a trend for political parties to ask more and more increasingly sensitive information of candidates for political office, under the logic that they do not want embarrassing personal information to be revealed in the heat of a campaign. This long standing vetting process has become more comprehensive as technologies have grown more sophisticated. Most political parties administer an extensive questionnaire including authorizations for information to be communicated to the party from federal agencies such as the Canada Revenue Agency, the Canadian Border Services Agency and Citizenship and Immigration Canada.[57]

Parties have also become interested in the postings of prospective candidates on social-networking sites. The most notorious example concerned one BC NDP candidate who was forced to resign in April 2009 after racy photographs posted on his Facebook page became public.[58] As a result of this scandal, the BC NDP required large amounts of personal information to be supplied for vetting purposes by potential candidates to the party, including social media login and passwords. A 23-question disclosure statement asked potential candidates to state any legal troubles, past political affiliations or disagreements with party policy - any incidents that could be considered politically controversial. The questionnaire also asked: "Do any of your social-media sites have

[56] "Obama, Facebook and the power of Friendship: The 2012 Data Election," *The Guardian,* February 17, 2012. "Obama's 2012 Campaign is Watching You" *Politico*, March 16, 2012 at: http://www.politico.com/news/stories/0312/74095.html

[57] See, for example, the application procedures of the Conservative Party at: http://www.conservative.ca/media/NominationRules2010.pdf

[58] CBC News, April 20, 2009, "Candidate's race Facebook photos showed lack of judgment" at: http://www.cbc.ca/news/technology/story/2009/04/20/bc-facebook-ray-lam-facebook-photos-james.html

material 'behind' privacy settings? Please provide details including site URL and your username and password for all social networking sites to which you belong." [59] BC NDP Leadership candidate, Nicholas Simons found this overly intrusive and refused to provide his Facebook password.

BC's Personal Information Protection Act (PIPA) is not confined (unlike PIPEDA) to commercial activities. Uniquely in Canada it also applies to non-profit organizations. The BC Information and Privacy Commissioner, Elizabeth Denham, believed, therefore that she had jurisdiction to begin an investigation of these practices.[60] After a period, the provincial NDP accepted her jurisdiction. The resulting investigation concluded that:

> The BC NDP collected a large amount of personal information, including information that may be outdated, irrelevant or inaccurate. It [the investigation] also concluded that the BC NDP collected personal information from third parties that it did not have consent to collect. There were also reasonable alternatives that could have been used to meet the purposes of vetting candidates. These factors all weighed against the collection being considered to be what a reasonable person would consider appropriate in the circumstances. The Office of the Information and Privacy Commissioner found that the BC NDP did not have the authority to collect personal information under s. 11 of PIPA.[61]

The BC NDP agreed to suspend the practice of asking for passwords for social networking services, as well as to abide by the BC Commissioner's set of general guidelines issued for social media background checking. [62]

At the same time that candidates are subject to an unprecedented level of scrutiny, there is a general lack of awareness about the personal information captured on other individuals who may work for parties in different capacities before, during and after election campaigns. This includes regular employees, whose data might be protected under privacy legislation in BC, but not elsewhere although they might be afforded some privacy protections under provincial labour and human rights legislation. There are also a vast and fluctuating number of more temporary workers, consultants and volunteers, all of whom might be given access to large amounts of personal information about voters and their behavior, intentions and preferences.

---

[59] Justine Hunter, *Globe and Mail Update*, "B.C. NDP screening leadership candidates to head off Internet embarrassments", Jan. 25, 2011 at: http://www.facebook.com/note.php?note_id=500514730821

[60] CBC News, March 7, 2011, "B.C. Facebook password spat resolved" at: http://www.cbc.ca/news/canada/british-columbia/story/2011/03/07/bc-nicholas-simons-passwords-agreement.html

[61] BC Information and Privacy Commissioner, P11-01-MS *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* at: http://www.oipc.bc.ca/Mediation_Cases/pdfs/2011/P11-01-MS.pdf

[62] BC Information and Privacy Commissioner, *Guidelines for Social Media Backgrounds Check,s* October 2011 at: http://www.oipc.bc.ca/pdfs/private/Guidelines-SocialMediaBackgroundChecks.pdf

INFORMATION ON CUSTOMERS

Finally, and a little recognized aspect of this issue concerns the extent to which parties might be collecting information through clearly commercial activity. Two parties sell a variety of products on their websites: logo clothing, signs, books and other souvenirs. Arguably, these commercial activities are covered by PIPEDA or other substantially similar provincial legislation governing the private sector. Privacy policies for the online stores are posted and give the typical assurances.[63] Purchases of party merchandise may provide clear indications of potential support. These privacy policies do indicate, however, that there is no disclosure of personal information from the commercial operations to the electoral arms of the parties.

The Conservative Party of Canada uses a third party to operate its online store, where logo wear and other branded items are sold. This commercial enterprise has its own, fairly extensive, privacy policy (that of Brymark Promotions Inc. of Ottawa). That policy indicates that personal information may be shared with third party advertisers, that it may be used for satisfaction surveys, and that an opportunity will be provided to opt-out of subscriptions, indicating that one could get on a mailing list if one makes a purchase. It also has a description of information security practices and a disclaimer that transmission of information is at the risk of the individual. The response to an inquiry to the company could also result in an individual getting on a mailing or call list. The policy also indicates that personal information provided for the purpose of making a purchase is only used for order fulfillment and is not shared.[64]

The Green Party's online store, GPC Gear, also has a separate privacy policy that indicates it will "never share or sell your personal information with any third parties", describes its information security and provides contact information for questions. [65]

[63] See the merchandise online store for the Conservative Party of Canada at: http://www.brymark.com/cboutique/
[64] Brymark, Privacy Policy, at: http://www.brymark.com/cboutique/privacy_en.cfm
[65] Green Party of Canada, GPC Gear Privacy Policy at: http://www.gpcgear.ca/miva5/merchant.mvc?Screen=PVCY

THE RISKS TO PRIVACY

The conclusion of this survey suggests that parties can, and do, collect a significant amount and variety of information on Canadian citizens, only some of which is openly understood and regulated by the CEA. The personal information practices of political parties affect their employees, donors, volunteers, members and supporters as well as registered voters whose information they obtain from Elections Canada. They can also affect anyone with whom the parties' canvassers come in contact. A disparate and fluctuating number of employees and volunteers might also have access to these data - individuals who may have no privacy training. Increasingly the data are communicated through highly mobile electronic formats.

Privacy risks come in a number of forms, and stem from various sources. Some risks include personal information getting into the wrong hands or being used for unauthorized purposes. Information can also get into the wrong hands through carelessness, lack of appropriate controls, inappropriate sharing, or nefarious intent. This may result in harm to individuals in terms of identity theft, harassment or the denial of services and rights. The various complaints to federal and provincial privacy commissioners over the years provide ample testimony to the range of serious harms that individuals can suffer when basic privacy rules are not followed.

Beyond the individual risks, there are also social risks as individuals lose trust in organizations when it is discovered that personal data is being used and disclosed for purposes they were not aware of, and to which they had not consented. There are social costs to excessive monitoring, just as there is a social value in ensuring that personal information is only collected, used, and disclosed for legitimate and transparent purposes.[66]

With respect to political parties, a series of incidents that might prove a harbinger of further trends have already occurred. We report them in chronological order.

In 2006, Conservative Party MP Cheryl Gallant sent birthday cards to her constituents using data from passport applications. The Privacy Commissioner of Canada was asked by several of her constituents to investigate this incident, even though she could not, for lack of jurisdiction.[67] The Office of the Ethics Commissioner subsequently took up the matter under the Conflict of Interest Code for Members of the House of Commons. Although the Ethics Commissioner did not find that there was any breach of the code because no "private interest" was advanced, he did remind MPs of Canada's privacy protection laws and that: "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 used for the purpose for

[66] See Colin J. Bennett, "In Defense of Privacy: The Concept and the Regime," *Surveillance and Society*, Vol. 8. No 4 (April 2011) at: http://www.surveillance-and-society.org/ojs/index.php/journal

[67] "MP must explain her use of privacy voter data," *The Ottawa Citizen*, January 4, 2006 at: http://www.canada.com/ottawacitizen/news/business/story.html?id=aa6d1f88-53ae-465e-998d-e9f0d4bba065

which it is gathered, or for a use consistent with that purpose."[68] Thus, an officer of Parliament has established the principle that despite Canadian privacy laws not applying to Members of Parliament, their treatment of personal information should be guided by the very principles derived from those laws.

Also in 2006, the RCMP found lists of voter names and addresses in the office of a Toronto cell of the Tamil Tigers, classified as a terrorist organization.[69] The documents were allegedly used to target potential supporters of the Tamil cause. The case was later cited in a larger Privacy Commissioner audit report of four government agencies. The Commissioner commented, "maintaining full control of electoral documents is a significant challenge."[70]

In October 2007, Rosh Hashanah cards were sent by the Prime Minister's Office to supporters with Jewish sounding names, many of whom were reportedly unsettled by this practice, and left wondering how such a list could be compiled.[71] The Privacy Commissioner received a number of complaints about this incident, but determined that the issue fell outside her jurisdiction. Religious beliefs are widely considered to be some of the most sensitive personal information, warranting special protections.

In April 2011, a Conservative Candidate from Winnipeg mistakenly sent a misdirected e-mail, containing the names, address, phone numbers and e-mails of six thousand of her constituents to a local environmental activist. The case prompted several to question why candidates receive this information in the first place.[72] The incident also highlights the need to ensure that candidates understand privacy principles and how to safeguard personal information entrusted to them.

In the context of the reform of Nova Scotia's election laws in 2011, the provincial Privacy Review Officer raised objections to the fact that the provincial chief electoral office was providing political parties with voters' year of birth. Ostensibly this information was provided to promote turnout among young people. Review Officer Dulcie McCullum said that she did not believe that Nova Scotians would be comfortable allowing parties to regularly compile lists that have each voter's year of birth attached to their name, address and voting rate.[73]

In the 2011 election, a woman from Oshawa complained that email correspondence with her MP about changes to CRTC regulations resulted in her receiving Conservative

---

[68] Office of the Ethics Commissioner, *The Gallant Inquiry,* June 2006 at: http://ciec-ccie.gc.ca/resources/Files/English/Previous%20Offices/Archives%20from%20the%20former%20Ethics%20Commissioner/Inquiry%20Reports/Members%20of%20the%20House%20of%20Commons/2006/The%20Gallant%20Inquiry%20%28June%202006%29.pdf

[69] "Tamil Tigers Using Electoral List, RCMP say," Colin Freeze, *Globe and Mail*, May 6, 2008 at: http://www.theglobeandmail.com/news/national/article684481.ece

[70] Privacy Commissioner of Canada News Release, "Audit Reveals Privacy Gaps at Federal Agencies," at: http://www.priv.gc.ca/media/nr-c/2009/nr-c_090212_e.cfm

[71] "Many Jews Unsettled over Harper Holiday Greetings," *Ottawa Citizen*, October 8, 2007 at: http://www.canada.com/ottawacitizen/news/story.html?id=198690d9-d9b8-4bbc-983f-d7236a2dfc8e

[72] Tim Brodbeck, "Giving voters lists to candidates violates privacy," *Winnipeg Sun*, April 25, 2011.

[73] "Watchdog Asked to Weigh in on Elections Act Concerns," Canadian Press, May 19, 2011 at: http://www.cbc.ca/news/canada/nova-scotia/story/2011/05/19/ns-elections-act-privacy-watchdog.html

campaign literature. In response, a Conservative party spokesman stated that it was party policy to remove a name from distribution lists on request.[74]

The privacy rights of candidates for office was also brought to light by the 2011 case of the NDP leadership race in British Columbia, and the practice of requesting passwords for Facebook accounts (discussed above).

Finally, the recent 2012 controversies over potential vote suppression in key ridings through the practice of "robocalling" are, at writing, still under investigation by Elections Canada and by the RCMP. Regardless of the results of these investigations into voter suppression, these incidents have shed light upon the previously opaque internal practices of political parties. Voters have learned, for instance, that their information is disclosed to telemarketing organizations, some of whom may reside outside Canada.[75] They have learned that many of the CRTC's calling rules do not apply to political parties. The online and offline commentary on these controversies have been extensive, and demonstrate a high level of interest and engagement in the broader issues about Canadian electoral processes. Not far beneath the surface, however, lay a number of unanswered privacy-related questions.

Even though the breadth of the economy in political data is not yet as broad as that in the United States, where higher levels of technical sophistication and campaign spending combine with extensive levels of publicly available data, these cases do reflect some trends that are unmistakable and concerning. We broadly agree with the assessment of Howard and Kriess:

> Even as data practices support political participation and mobilization, they come with a social cost. While the risks of poor data management practices may be partially borne by political parties, ultimately it is citizens whose personal records have been compromised. Political data is collected and traded on a vast and opaque market, with documented cases of breaches in security. Meanwhile, the extent and nature of political data has the potential to threaten associational freedom, as citizens become increasingly aware that much of their online and offline behavior is subject to monitoring and act accordingly.[76]

So what protections currently exist for the personal data processed by political parties in Canada?

---

[74] "Email to MP lands woman in campaign database," Brendan Kennedy, *Thestar.com*, April 15, 2011: http://www.thestar.com/news/article/975620--email-to-mp-lands-woman-in-campaign-database?bn=1

[75] For example, Craig Mcinnes, "Robocalling raising privacy issues," Vancouver Sun, March 4, 2012 at: http://www.vancouversun.com/technology/Robocalling+raising+privacy+issues/6249603/story.html

[76] Howard and Kriess, ibid.

CURRENT LAW AND POLICY FOR FEDERAL POLITICAL PARTIES

FEDERAL AND PROVINCIAL PRIVACY LEGISLATION

Political parties fall between the cracks of a national privacy regime that grew up pragmatically, and with necessary sensitivities to the constitutional division of powers. The 1982 Privacy Act regulates government institutions, explicitly referenced in Section 3 of that Act, which does not include political parties. The only real consideration for political issues in this legislation is the provision that federal ministries are authorized to disclose personal information "to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem" (S. 8 (2)(g)).

Political parties are not covered by the federal private sector legislation (PIPEDA), either. Part 4 (1) of PIPEDA stipulates that "This Part applies to every organization in respect of personal information that:

(a) the organization collects, uses or discloses in the course of commercial activities; or
(b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

Political parties do not meet the definition of "federal work, undertaking or business." Moreover, it is likely a stretch to suggest that the political activities of political parties are "commercial activities" with the exception of the small aspect of their operations relating to the sale of party merchandise, and perhaps where fees are charged for database access within the Conservative party and possibly others.[77] But general fund-raising by political parties is not considered a commercial activity.[78] By extension, the recently proposed amendment to PIPEDA (Bill C-12, *Safeguarding Canadians' Personal Information Act.)*, including the new requirements for the notification to the Office of the Privacy Commissioner of data breaches, would not apply either.[79]

Neither are political parties covered under Canada's new Anti-Spam legislation, designed to prevent unsolicited email.[80] Political parties and charities are explicitly exempted if

[77] Garth Turner, Political Commentaries, *Historical Archive, 2005-2009*, http://www.garth.ca/2007/10/12/nowhere-to-hide/
[78] See the comments by Michael Geist in Keith Boag's report on "Voter Databases" on CBC, cached at: http://video.google.com/videoplay?docid=1277939542743658378
[79] Bill C-12, *An Act to Amend the Personal Information Protection and Electronic Documents Act*, 41st Parliament, First Session, at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5144601&file=4
[80] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) at: http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2010_23/

their email communications do not involve selling or promoting a product. Further exemptions apply when organizations engage in commercial activities with people who have made a donation or gift in the last 24 months, volunteered or performed volunteer work in the last 24 months, or were a member of the organization in the last 24 months. These exceptions would also apply, therefore, to political parties and to candidates in federal, provincial, territorial or municipal elections.[81]

Political parties and other political entities are also exempted from the "Do not Call List" procedures implemented through the CRTC.[82] As provided for in section 41.7 of the *Telecommunications Act*, the National DNCL Rules do not apply in respect of a telecommunication:

> (c) Made by or on behalf of a political party that is a registered party as defined in subsection 2(1) of the *Canada Elections Act* or that is registered under provincial law for the purposes of a provincial or municipal election; (d) made by or on behalf of a nomination contestant, leadership contestant or candidate of a political party described in paragraph (c) or by or on behalf of the official campaign of such contestant or candidate; (e) made by or on behalf of an association of members of a political party described in paragraph (c) for an electoral district;

Although political parties are exempt from the prohibition against calling numbers on the do not call list maintained by the CRTC, some of their calling practices are regulated.[83] Under CRTC Automatic Dialing-Announcing Device (colloquially known as "robo-call") Rules, they are limited by time of day and required to identify the person on whose behalf the call is made and provide contact information, and display the originating phone number. They must also maintain an internal do not call list, but are not obliged to disclose this to callers.

The only provincial privacy legislation, substantially similar to PIPEDA, that has been held to cover political parties is BC's Personal Information Protection Act (PIPA), which unlike its equivalents in Alberta and Quebec, defines an organization to include "a person, an unincorporated association, a trade union, a trust or a not for profit organization"[84] and does not limit application to commercial activities. The recent case involving the BC NDP, described above, confirms the jurisdiction of the BC Information and Privacy Commissioner over political parties. As far as we know, this is the first time that a Canadian commissioner has formally investigated the internal operations of a Canadian political party. A precedent has therefore been set, at least in BC. A further interesting dimension of the issue is raised with respect to federal political parties, to the extent that they are collecting personal information in British Columbia. The law is untested, but it can be argued that the federal parties are also acting as non-profit organizations under BC

---

[81] Industry Canada, Questions and Answers, Bill C-28:Canada's Anti-Spam Legislation, at: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00569.html#q12

[82] Canadian Radio-Television and Telecommunications Commission, *Key Facts for Consumers about the National Do Not Call List*, at: http://www.crtc.gc.ca/eng/info_sht/t1031.htm

[83] Canadian Radio-Television and Telecommunications Commission, Unsolicited Telecommunications Rules, Part 1V at: http://www.crtc.gc.ca/eng/trules-reglest.htm

[84] BC *Personal Information Protection Act*, Section1 at: http://www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm

PIPA and would be subject to the various requirements of the BC legislation with regards to their personal information practices within British Columbia.

However, it should also be noted that BC's 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."[85] Similar exemptions for provincial politicians appear in other provincial information and privacy statutes relating to the public sector.[86] In 2007, the former BC Information and Privacy Commissioner explicitly refused to investigate a complaint that the constituency office of a federal member of parliament had improperly disclosed personal information contrary to PIPA, on the grounds that he did not have jurisdiction.[87] Thus 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.

INFORMATION AND PRIVACY PROVISIONS IN THE CANADA ELECTIONS ACT

The Canada Elections Act (CEA) is a lengthy and complex piece of legislation, within which there are many provisions relating to personal information. The CEA provides a fairly comprehensive regime regarding personal information used in the electoral process, primarily as it relates to the information collected by Elections Canada to maintain the Register of Electors for the production of lists of electors, their distribution to those involved in the electoral system and their use of that information. The regime authorizes direct collection of specified data elements from electors and indirect collection from named entities (or under named statutes) and the Minister of National Revenue, and restricts the use of that information. Those named sources include Canada Post Corporation's National Change of Address Database, Info-direct™, and the Public Curator (Quebec). Those statutes include provincial and territorial driver licensing, elections and vital statistics statutes.

Because EC is charged with maintaining the Register of Electors, it must therefore collect information to determine if voter eligibility requirements are met. Further, EC must provide information on registered voters to political parties and parties must provide information on donors to EC. Being on the voters' list is optional, so EC must remove names at that person's request, and must also remove names of deceased persons (entailing information sharing agreements with provincial vital statistics agencies and other sources). They must also make corrections to voter information if requested by the voter. Thus, parties must have a way to update their records as well.

---

[85] Ibid, Section 3(2) g.
[86] BC *Freedom of Information and Protection of Privacy Act* (FOIPPA), Section 3(1) c. at http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00
[87] Office of the BC Information and Privacy Commissioner, Decision P-07-03, *Constituency Office of Federal Member of Parliament* at: http://www.oipc.bc.ca/PIPAOrders/2007/DecisionP07-03.pdf

Under s. 46(1) of the CEA, the Register of Electors must be updated from information provided by the elector to EC, from a federal department or body, with express consent of the elector, or if necessary, from reliable scheduled sources. Under s. 46(1.1), retention of voter personal information obtained from external sources is regulated. Sections 46.1 and 46.2 allow the Minister of National Revenue to collect and disclose to EC, citizenship and death information from tax returns for the purpose of updating the Register.

The accuracy of information is addressed in a number of sections. Under s. 48(2), electors wishing to be on the Register must confirm or correct the information sent to them by the CEO, and certify their eligibility. The CEO may ask the elector for additional information required pursuant to information-sharing agreements with other agencies, but the provision of this information is optional for the elector. The CEO is required to make changes and corrections to the register from information provided by electors, under s. 50, and the CEO may contact the elector to verify information or request confirmation or correction under s. 51. The CEO is required to delete names from the Register if the elector is dead, requests it, or is not an elector, under s. 52(1). The CEO even has the ability under s. 52(2) to delete the name of an elector who has not confirmed or corrected his or her information as requested. The Act also speaks to the ability of an elector to restrict the use of his/her information to federal electoral purposes and thus prevent it being shared with provincial electoral bodies as would happen under agreements made pursuant to s. 55.

The process set out in the Act for the registration of political parties requires that parties provide to EC a significant amount of personal information relating to at least 250 of their members. As Elections Canada is subject to the Privacy Act, the information it collects must be dealt with in accordance with the provisions of that Act. "The prescribed form is entitled *Declaration of a Member of the Party* (EC 20225) and includes:

- the member's surname and given name(s)
- the member's full residential address and mailing address, if different
- the member's date of birth (optional) along with authorization for Elections Canada to verify the information using the National Register of Electors (optional)[88]
- confirmation that the member is a qualified elector under the Act (i.e., 18 years old and a Canadian citizen), is a member of the political party and supports its application for registration
- acknowledgement that the member is aware that it is an offence under the Act to make a false or misleading declaration

The CEA creates offences for making unauthorized use of information in the Register of Voters and providing false or misleading information regarding many reporting requirements.

[88] Because of this optional date of birth collection, parties commonly require exact date of birth on membership applications.

EC publishes guidance for the use of personal information from the Register**.** The Guidelines include sample declarations for lists distributed to members of Parliament, political parties, and candidates, which require signatures of the party receiving the information and a witness.[89] The Guidelines also include advice on use, and safeguarding and disposition of the lists, as well as a FAQ and best practices. The latter lists training authorized users on the importance of protecting privacy, limiting distribution on a need to know basis, the preference for paper lists, securing lists when not in use, securing electronic copies with passwords and hard copy in locked cabinets, and restricting passwords. The FAQ explains how the information may be shared, used and not used, including not telling others whether someone is on the list.[90] However, Elections Canada does not have the legislative authority to verify whether those guidelines are applied. Nor is there any data breach-reporting requirement. This guidance does, however, address the question of accountability, in part, by recommending that a person be assigned responsibility for safeguarding the lists.

Regarding the individual access principle, s. 54 states that, **"**At the written request of an elector, the Chief Electoral Officer shall send the elector all the information in the Chief Electoral Officer's possession relating to him or her." Under s. 55, the CEO may enter into agreements with provincial counterparts and other specified bodies such as vital statistics agencies and driver licensing organizations. Those agreements must include conditions for the use and protection of the personal information provided.

In conclusion, most of the principles outlined in Schedule One of PIPEDA, are addressed in the CEA, although in the case of some principles, they only apply to EC. Where the regime applies to the personal information practices of political parties, it primarily relates to the right of parties to personal information on the lists of electors (preliminary and final) and their use of it. There is, therefore, a large gap in regulation of the parties' collection, use and disclosure of personal information from other sources.

The powers of the Chief Electoral Officer (CEO) are broad. That statutory position is charged with providing direction and supervision over elections, with ensuring fairness, impartiality and compliance, with issuing necessary instructions and with performing necessary functions and duties, under s. 16. The powers also include a public information and communication component including to "implement public education and information programs to make the electoral process better known to the public, particularly to those persons and groups most likely to experience difficulties in exercising their democratic rights" under s. 18(1) and "using any media or other means that he or she considers appropriate, to provide the public, both inside and outside Canada, with information relating to Canada's electoral process, the democratic right to vote and how to be a candidate" under s. 18(2).

Thus, it appears that it is within the mandate of EC to educate voters about what might happen to their personal information during the electoral process and in their interactions

---

[89] Elections Canada, *Guidelines on Use of the Lists of Electors from the Office of the Chief Electoral Officer of Canada* – 2010**,** at http://www.elections.ca/content.aspx?section=pol&document=part4&dir=pol/LOE&lang=e#p42

[90] Ibid.

with political parties.[91] But EC's role with respect to investigating the internal workings of political parties with respect to the personal information made available to them, and thus ensuring that the guidelines described above are followed, is very limited.

THE PARTIES' OWN PRIVACY STATEMENTS AND POLICIES

What do the parties themselves claim that they do with personal information? The various privacy statements of the Conservatives, NDP, Liberals and Greens are contained in the appendices. The Bloc Québécois has some notices and assurances about how personal information will be used on its webpages but no privacy policy *per se* or overall description of its privacy practices that we could find.[92] We approach these statements from the point of view of the average citizen. If that person wanted to discover how her/his personal information were being processed, what would she/he learn from the public statements?

The first point to emphasize is that the privacy policies of Canada's federal political parties, if they exist, are not always easy to locate. As of March 2012, neither the Liberal Party nor the NDP has any link from their homepage to a privacy policy. Indeed it is not even clear that the Liberal Party has such a policy, even though one set of commitments was found from the homepage of the Young Liberals.[93] Howard and Kreiss report that the Liberal Party has voluntarily declared that it will abide by PIPEDA[94], but we have not been able to find any independent evidence of such a commitment. The Conservative Party of Canada homepage has a well-placed link to a one-page set of commitments.[95] The NDP does have a privacy policy with respect to the website, NDP.ca, but it is not clear how far these commitments extend to personal information collected through other means.[96] The Green Party has the most comprehensive policy, clearly linked from the homepage. [97]

Secondly, the scope of coverage of these policies is sometimes not clear. In none of the policies do we find a clear description of the kinds of personal information collected and processed. None specifies whether the policies apply to voters, contributors, employees,

---

[91] See for example the Elections Canada Backgrounder entitled "Description of the National Register of Electors", at http://www.elections.ca/content.aspx?section=vot&dir=reg/des&document=index&lang=e

[92] For example (translation),"The Bloc takes seriously the issue of protection of privacy. Rest assured that we will not provide your details to anyone. They will be used only to provide you with news and information about the Bloc Quebecois."
http://www.blocquebecois.org/dossiers/participez/jappuie_index.aspx

[93] Young Liberals of Canada, *Privacy Policy*, at: http://www.ylc-jlc.ca/privacy_e.aspx This was not found by navigating on the page, but by conducting an internet search. The URL: www.liberal.ca/privacy takes one to a donation page.

[94] Howard and Kriess, p. 18. We do note, however, that the Ontario Liberal Party has declared that handling of all personal information by the Ontario Liberal Party is governed by the *Freedom of Information and Protection of Privacy Act (FIPPA)*: http://www.ontarioliberal.ca/Privacy.aspx

[95] Conservative Party of Canada, Privacy Policy at: http://www.conservative.ca/footer/privacy_policy

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

[97] Green Party of Canada, Important information and privacy policy at: http://greenparty.ca/en/privacy

volunteers or all of the above. None specifies how broadly it applies to national and regional units of the party. As noted, some appear confined to the information collected through the website. The electronic stores of the Conservative and Green parties have separate privacy statements relating to these commercial operations. In other instances, the broader question of privacy tends to be conflated with the narrower question of data security.

Thirdly, each of these privacy policies appears to fall short of the CSA standard inherent in PIPEDA. Nowhere is there a systematic statement of each of the privacy principles and how they are implemented within the organization. Nowhere is there a link to a more complete organizational code of practice, something that is often seen on some corporate websites.

Fourthly, the kinds of accountability mechanisms now common for government and corporations do not appear to be publicized. For example, none of the party privacy policies or statements specifies the name of a designated individual, equivalent to a Chief Privacy Officer, who would be responsible for the implementation of good privacy protection practices. Privacy training is also an accepted feature of good privacy management, as is the conduct of privacy impact assessments (PIAs) when new products or services are being introduced. None of these mechanisms appears to be mentioned.

Fifthly, another component of good privacy management is the publication of clear and easy-to-use procedures by which individuals can control the collection, use, and disclosure of their personal information. The procedures for requesting access and correction of personal information are either absent or somewhat vague. Some policies allow procedures to unsubscribe from mailing lists. None indicates if the parties operate a general do-not-call list, and how an individual might place his/her name on that list. None of the parties mentions a privacy complaints process; individuals would generally have to rely on the generic "Contact Us" forms.

Finally, vague and expansive statements of purpose are common. Many web forms are designed to collect much more personal information than is *necessary* for a particular transaction. For instance, postal code and full name are often requested, when all one needs to fulfill an electronic subscription is an email address. Full mailing address, email and phone number are commonly collected during the process of sending input or questions. Donation forms also request details of occupation.[98] Some membership forms collect demographic information such as sex, race, and sexual preference, although these fields are generally labeled optional.[99] Further, at the point where personal information is

[98] Liberal Party of Canada, Join the Party, New Membership page, where there are optional fields for occupation, gender and full date of birth, at: https://action.liberal.ca/en/membership

[99] The Liberal Party New Membership form has a radio button for "Are you of aboriginal ancestry (optional)?" and the NDP membership form, Step 2, Add any additional information, has tick boxes to indicate if the member is a member of a union, un(der)employed or 26 and under. It also has tick boxes to "indicate if you identify as part of one of the following equity seeking groups and would like to receive mail on relevant issues." Choices are: Aboriginal, Gay, lesbian, bisexual, transgendered, Person living with a disability, Visible minority and Woman, at https://secure.ndp.ca/membership_e.php. These choices are not labeled optional.

collected, there is commonly little or no notification about how it will be used, and thus it is difficult to infer that collection practices are always consensual.

These existing privacy statements are welcome, and constitute a start. Further documentation may, of course, exist, but it is not apparent to the average user from any of the parties' online presence. There are, for example, certain user agreements for those given access to voter management databases. That of the Liberals is published and provides some strong warnings about the inappropriate use and disclosure of personal information accessed from Liberalist.[100]

From the point of view of an ordinary supporter or contributor who wishes to exercise control over his or her personal information, however, the commitments are often vague, and the remedies incomplete. In terms of personal-information handling information and processes, none discloses or hints at the presence of a privacy management framework, or a designated individual with responsibility for privacy issues. These shortcomings are nothing new, but given the relative progress that has been made in other areas of Canadian society, they are quite notable.

[100] Liberalist User Agreement Form at: http://liberalist.liberal.ca/user-agreement/

CONCLUSIONS

Canadian federal privacy protection law does not cover federal political parties. Parties do not engage in much commercial activity and are therefore largely unregulated under PIPEDA, or substantially similar provincial laws, with the exception of PIPA in BC, which applies to personal information practices of all organizations acting within the province. The *Privacy Act* does not cover political parties. The only federal law that governs their practices is the CEA. But this legislation only applies to those voter registration data collected and shared with parties and candidates under the authority of that legislation. It leaves unregulated the collection of personal data captured by parties from other sources.

As Canadian parties continue to capture and process personal data, there are likely to be further incidents and media coverage of data breaches, non-consensual use and disclosure of personal information and unsolicited marketing practices. Presumably, there will continue to be pressure on the Office of the Privacy Commissioner to respond, despite the Commissioner's lack of jurisdiction.

There is now a commonly accepted understanding in Canada of what it means for an organization to process personal data responsibly. Essentially, those responsibilities are outlined in the code of fair information practices embodied within Schedule I of PIPEDA. Canadians have gradually grown to expect that they have certain personal information rights, and that organizations have certain responsibilities.

Yet, the current reality is that the parties are managing vast databases within which a variety of sensitive personal information from disparate sources is processed. For the most part, individuals have no legal rights to learn what information is contained therein, to access and correct those data, to remove themselves from the systems, or to restrict the collection, use and disclosure of their personal data. For the most part, parties have no legal obligations to keep that information secure, to only retain it for as long as necessary, and to control who has access to it.

This report has presented information drawn from a large range of public sources about the nature and scale of these issues. It is, however, only an overview and there is clearly need for some more comprehensive research. It is also obvious that the questions concerning the personal information practices of Canada's federal political parties are ongoing and will continue as long as they need and use this information. There is therefore a need for further engagement with the various stakeholders, and for a broader public debate.

APPENDICES

APPENDIX A: CONSERVATIVE PARTY OF CANADA PRIVACY POLICY

The Conservative Party of Canada has a brief privacy policy, available from a link on its home page and many other pages.[101] Its privacy policy is reprinted below.

Privacy Policy

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.

What is "Personal Information"

"Personal Information" is information about an identifiable individual. It may include information such name, address, telephone number and other contact information.

How Your Personal Information may Reach Us

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.

We do obtain personal information when you join or make a contribution to the Conservative Party. As well, when you visit our web site, you may wish to provide us with information that permits us to keep you informed about Conservative Party policies and activities or which enables you to become a volunteer or make a financial contribution.

Personal information is also collected as part of the registration process for Conservative Party conventions and other events.

Our collection of personal information is limited to what is necessary and reasonable.

How we use your Personal Information

Your information is used to communicate with you, or to facilitate your participation as a volunteer if you wish to assist. We take great care in the way we store and use your personal information.

Because the Conservative Party is a national organization with a riding-based membership system, your personal information may also be used by our local riding associations including by contestants for nominations. For example, if you have made a financial contribution, the local riding may contact you to see if you would like to continue your support.

[101] Conservative Party of Canada, Privacy Policy, at: http://www.conservative.ca/?section_id=4799&section_copy_id=77476

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.

We will not sell your personal information that you have chosen to provide us, nor will we disclose it to third parties except as required by the Elections Act.

How we Protect Your Personal Information

We maintain security systems to safeguard your personal information from unauthorized access, disclosure or misuse, and from loss or unauthorized alteration.

Accuracy of Personal Information

We will strive to ensure that the personal information we have on file for you is accurate and up-to-date as is necessary for the purposes for which it is to be used. If any information needs to be updated or amended, we will make every effort to change our records, and will inform those of our offices having access to the information in question.

You may update or correct the personal information you provide to us by e-mailing us at membership@conservative.ca.

Links to Other Web Sites

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

Each employee or agent of the Conservative Party is responsible for maintaining and protecting all personal information under their control. If you have any questions about the Conservative Party privacy policy or the information we collect, please contact us, or by regular mail at

Conservative Party of Canada
1204 - 130 Albert St.
Ottawa, ON K1P 5G4

The privacy policy for the NDP appears to relate solely to the information collected through its website. There appears to be no privacy policy link from its home page. One may find the following privacy statement using a web search. [102]

Privacy policy

This page summarizes our privacy policy and information practices for NDP.ca. It is intended to provide complete and accurate information to help you make informed decisions when choosing to communicate with our campaign via this site. A detailed outline of privacy issues you may wish to consider is below.

When visiting NDP.ca, your privacy is respected. Our policy is in strict compliance with Canadian privacy laws, as well as Elections Canada requirements. We do not collect personal information unless you choose to send us an e-mail, join our E-Newsletter, donate to the campaign, or otherwise voluntarily provide your name and contact information. Information you provide is held in the strictest confidence, and will not be shared with any third party without your express permission.

Our Web site is hosted on servers that are managed by Web Networks, a third party service provider. Any personal information collected on our behalf by Web Networks such as server log data (see below), is managed in accordance with this privacy policy, and is protected by applicable law.

If you have questions about your privacy that are not answered below, please don't hesitate to e-mail us at contact us or call 613.236.3613.

Online Donations
Our online donation site made through a secure server managed by Web Networks. The information you provide to the NDP is used solely for processing your online donation according to the conditions set out in the Elections Act. More information about the Elections Act is available at www.elections.ca.

Your information will be handled directly by the Donations Department of the New Democratic Party of Canada. If you are uncomfortable donating online, please contact the Donations Department at 613.236.3613.

E-mail
Personal information received via e-mail is provided only to campaign staff, who require the information to respond to inquiries. We will not provide your e-mail address or other information to any third party without your express permission. We protect your personal information with strong security safeguards, including strict access controls. We do recommend that you avoid sending sensitive personal information electronically, as we cannot guarantee the security of electronic systems or e-mail. For all such matters, please call us at 613.236.3613, or contact us by postal mail at:

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

New Democratic Party of Canada
Suite 300 - 279 Laurier Avenue West
Ottawa, Ontario K1P 5J9

IP Tracking
Your Internet Protocol (IP) is a unique Internet "address," assigned to you by your Internet Service Provider (ISP). IP addresses are automatically logged by Web servers, collecting information about a user's traffic patterns. While the IP address does not identify an individual by name, it may, with the cooperation of the ISP, be used to locate and identify an individual using the Web. The IP address is considered personal information because it is an identifying number, and IP addresses are protected by most privacy legislation. The privacy issues surrounding IP addresses are explained further below.

Server logs
Server logs include statistical information, such as visitors' IP addresses, type of operating systems, time and duration of visit, Web pages requested, and identify categories of visitors by items such as domains and browser types. Our servers automatically log information about visits to our Web site in the normal course of establishing and maintaining Web connections. These statistics are reported in the aggregate to our Web and communications staff, and are used to improve our Web site and ensure that it provides the optimal Web experience for visitors.

We do not link server log information to any other data in a way that would enable us to identify individual visitors. However, we may review server logs for security purposes, for example, to detect intrusions into our network. In the event of a criminal investigation, server log data could be used to trace and identify individuals for prosecution.

Cookies
Cookies are small text files maintained by your computer in order to help your browser remember user settings as you navigate the site. For example, NDP.ca uses cookies to remind your browser whether you chose to view the site in English or in French.

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

Still have questions?
Questions about this policy may be directed to our Webmaster. Contact our Webmaster by e-mail here, by phone at 613-236-3613 or by postal mail at:

New Democratic Party of Canada
Suite 300 - 279 Laurier Avenue West
Ottawa, Ontario K1P 5J9

APPENDIX C: YOUNG LIBERALS OF CANADA PRIVACY POLICY

There is no privacy policy visible from the home page of the Liberal Party of Canada. Using the search function for "privacy", one finds the Young Liberals of Canada Privacy Policy,[103] reprinted below.

Privacy Policy [Young Liberals]

The Liberal Party of Canada is committed to ensuring that the information you provide to us remains private and secure. Our privacy policy contains information relating to the following topics:

- How we collect information about you
- How we use your information
- How to update records or to unsubscribe from our website
- How we protect your information
- Information about children
- Links to other websites
- How you may contact us

How we collect information about you:

We collect no personal information about you, such as your name, address and telephone number, without your permission. When you visit our website, you may choose to provide us with personal information for the specific purpose of becoming involved with the Liberal Party of Canada, whether as a member, volunteer or as a financial contributor. You may also wish to become a subscriber to our website in order to receive news and information which may be of interest to you.

How we use your information:

We only use your personal information to communicate with you about the Liberal Party of Canada and its activities, as well as to provide you with news and information. We do not sell your personal information to anyone under any circumstances.

The information you provide when you make a contribution to the Liberal Party of Canada, other than your credit card information and telephone number, will be communicated to Elections Canada in accordance with the Canada Elections Act. Once your online contribution has been fully processed, your credit card information will be destroyed.

Because the Liberal Party of Canada is a national organization, we may share your personal information internally with our provincial and territorial offices, as well as our local riding associations. If you have been a contributor, we may contact you again to seek your financial support.

[103] Young Liberals of Canada, Privacy Policy, http://www.ylc-jlc.ca/privacy_e.aspx

How to update records or to unsubscribe from our website:

You may update or correct the information you provide to us by e-mailing us at info@liberal.ca. If you have subscribed to our website to receive information from us, you may unsubscribe by replying to an e-mail and inserting the word "unsubscribe" in the subject line. If you change your email address, you can unsubscribe from our mailing list and sign up again with your new e-mail address.

How we protect your information:

It is very important to us that the personal information you provide to us is secure. 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 locked and secure environment.

We use 128 bit encryption and entrust digital certificates for authenticity. If you wish to view our Entrust SSL certificate, click here.

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 in the aggregate to track which pages people visit in order to improve the quality of our website. We do not use this data to develop profiles of individual visitors to our website.

Information about children:

The Liberal Party of Canada does not ask for personal information about children under 14 years of age. Membership in the Liberal Party of Canada is restricted to persons aged 14 and over. Persons under the age of 18 are not permitted to contribute via our website.

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 of Canada is not responsible for the content or the privacy policies of these websites.

How you may contact us:

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

You can also reach us by regular mail at the following address:

Liberal Party of Canada
81 Metcalfe Street, Suite 400
Ottawa, Ontario K1P 6M8

Attention: Privacy Officer

The privacy policy of the Green Party can be found as a small text link at the bottom of the home page.[104] It is available in both official languages and is the most extensive of all the party privacy policies. It is reprinted below.

* Please note that there were discrepancies between the French and English versions on the Green Party website.

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, Opt-In and unsubscribe information:

To update your mailing: email webadmin@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 have either registered this address for the purpose of receiving information in the future ("opt-in"), are (a) a member of the Green Party of Canada (b) a recent donor or volunteer, or (c) otherwise have an existing relationship with us. If a friend who believed you would be interested in the information contained herein sent this, your address will not be stored on file and/or used unless you opt in to mailings by subscribing to our e-newsletters. Click here to subscribe or follow the instructions at the end of this e-mail. 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.

[104] Green Party of Canada, accessed March 20, 2012, http://www.greenparty.ca/

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 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)

Aggregate 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 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.

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 opt in 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 our online subscriber services at http://app.greenparty.ca/lists/?p=subscribe&id=1

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. You Click here to 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 either by postal mail, telephone or e-mail at: **By E-mail** General Information: info@greenparty.ca Web site Administrators: webadmin@greenparty.ca **By Mail** Green Party of Canada P.O. box 997, Station B Ottawa ON K1P 5R1 **By Telephone** Toll-free: 1-866-VOTE-4-GPC (1-866-868-3447) Telephone: (613) 562-4916 (Ottawa) Fax: (613) 482-4632 (Ottawa) Effective date: September 25, 2004.

GPC Gear

There is a link to a different and brief privacy policy for the commercial activities of the Green Party at its online store, reprinted below.

Privacy Policy [105]
We respect your privacy. Therefore we never share or sell your personal information with any third parties.

Any information collected through this site is intended to be used for this transaction only. Your personal information is secured via SSL (Secure Socket Layer) Technology".

It's time - Vote Green - The Green Party of Canada
Need Help? Please call 905-586-1059 or email ian@gpogear.ca

[105] Green Party of Canada, GPC Gear Privacy Policy, at: http://www.gpcgear.ca/miva5/merchant.mvc?Screen=CTGY&Store_Code=GPC&Category_Code=GPCSale