Elections Canada

elections.ca

Political Communications in the Digital Age

Discussion Paper 3: The Protection of Electors' Personal Information in the Federal Electoral Context

Elections Canada (May 2020)

For enquiries, please contact:

Public Enquiries Unit
Elections Canada
30 Victoria Street
Gatineau, Quebec
K1A 0M6
Tel.: 1-800-463-6868
Fax: 1-888-524-1444 (toll-free)
TTY: 1-800-361-8935
elections.ca

 ElectionsCanE

 @Elections_Can_E

 ElectionsCanadaE

 Elections Canada

 electionscan_e

978-0-660-34851-3
Cat. No.: SE3-110/3-2020E-PDF

Table of Contents

Foreword

After each general election, the Chief Electoral Officer (CEO) is required to submit a report to Parliament outlining recommendations that, in his view, will improve the administration of the *Canada Elections Act.* In developing his recommendations report after the 2019 election, the CEO wishes to explore certain themes related to the way in which political actors communicate with electors in the digital age.

Over the past two decades, political communications have changed drastically. Communications around elections—and in general—are increasingly digital, taking place through text messages, on social media platforms, in online ads and in other formats. Many of these are enabled by big data and are highly targeted. There is every indication that this trend will continue into the future and that the significance of digital communications for electoral democracy will continue to grow.

The regulatory regime in place under the *Canada Elections Act*, however, dates originally from a time when broadcast television was the dominant advertising and communications medium. The Act is based on certain core values, such as transparency and fairness, that continue to underlie the way elections are delivered in Canada, but legislative improvements may be needed.

With a view to soliciting input from a diverse audience of stakeholders and experts to inform the CEO's recommendations to Parliament, Elections Canada has prepared a suite of three discussion papers on interrelated topics that are central to this question.

- The first paper, *The Regulation of Political Communications under the Canada Elections Act*, aims to foster discussion about whether existing provisions in the Act meet the challenges that have arisen in recent years, largely due to new communications technology.
- The second paper, *The Impact of Social Media Platforms in Elections*, looks more closely at social media and digital advertising platforms and aims to promote discussion on the impacts that these platforms may have on elections and democracy.
- The third paper, *The Protection of Electors' Personal Information in the Federal Electoral Context*, aims to encourage discussion on how fair information principles could be applied to political parties, taking into account their unique role in Canada's democracy.

Introduction

Over the past several years, there has been a growing chorus of support for the idea that federal political parties should be subject to rules that govern how personal information is treated.[1] These calls emerged after electors' personal information was used to communicate false, misleading or divisive content in an attempt to manipulate electoral outcomes in the UK and the US in 2016. These events raise important questions about the implications of collecting and processing personal information in order to communicate with electors, as well as how those activities should be regulated.

Cambridge Analytica inappropriately accessed Facebook user data, developed detailed voter profiles and used that information to target ads and attempt to influence electors.[2] Foreign entities (such as the Russia Internet Research Agency) used social media to spread divisive messages right before the US election.[3] In short, attempts have been made to manipulate electors and their electoral processes.

In Canada, calls for increased elector privacy protections emerged most recently, notably out of concern that elector information could be misused here at home during the 43rd general election.

The discussion about subjecting political parties to privacy laws requires careful consideration in order to balance a number of public interests, including the privacy rights of electors, the right and need for political parties to communicate with them, and fair and equal participation in the electoral process.

This discussion paper focuses on the building blocks of political parties' campaign strategies: electors' personal information. It begins with an overview of electors' privacy expectations. It then outlines the rules governing the lists of electors and parties' privacy policies. The final section discusses the fair information principles and poses questions for consideration to generate discussion on how the principles could apply to political parties, while taking into account the needs of political parties to understand and communicate with electors.

Canadians' Privacy Expectations

Canadians are concerned about protecting their privacy. Surveys from 2012 to 2018 indicate that 88% to 92% of Canadians are concerned, with those being "extremely concerned" rising from 25% in 2012 to 37% in 2016 and 2018.[4] But what do Canadians expect of their political parties when parties collect their personal information and use it to communicate with them?

In 2018, 72% of Canadians said they supported changing the law so that parties are subject to the same privacy rules as private companies.

In 2013, following the use of deceptive communication practices during the 2011 federal election, 14% of Canadian electors agreed that it was important that political parties be able to collect personal information on them, compared to 69% who disagreed. When presented with a trade-off between preserving electors' privacy and the need for political parties to communicate with electors, 68% opted for the privacy of electors (53% saying it should always prevail), compared to 15% who opted for the need to communicate (9% saying it should always prevail).[5]

In 2017, 65% of Canadian social media users reported being uncomfortable with political parties accessing their personal information.[6] Two thirds of Ontarians surveyed in 2018 did not think that parties should be allowed to use their social media data to assist with targeting them with communications. A majority (87%) felt that parties should only access publicly available information such as census data or elector lists.[7]

Recent surveys indicate that Canadians support the idea that parties should be subject to privacy rules. In 2018, 72% of Canadians said they supported changing the law so that parties are subject to the same privacy rules as private companies.[8]

In sum, Canadians are concerned about their privacy and tend to value the protection of their personal information more than the rights of parties to communicate with them. However, not all Canadians are opposed to parties collecting some information for the purposes of communicating with electors.

Current Rules Protecting Electors' Personal Information

The *Canada Elections Act* (CEA) touches on the issue of electors' personal information by establishing rules related to the lists of electors, the statements of electors who voted and a requirement that parties state how they handle personal information. Otherwise, the personal information that federal political entities collect, use and disclose is left unregulated.

At the federal level, personal information is mainly protected by two other laws: the *Privacy Act* (PA), which applies to the federal public sector, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to organizations that engage in commercial activities.[9] Neither applies to federal political parties. However, in British Columbia, political parties are subject to the *Personal Information Protection Act* (PIPA) because that law applies to "organizations" in broad terms. Recently, the BC Privacy Commissioner ruled that federal electoral district associations operating in British Columbia would be subject to PIPA.[10]

British Columbia is the only Canadian jurisdiction where privacy legislation, the Personal Information Protection Act (PIPA), applies to provincial political parties. PIPA provides that personal information cannot be collected, used or disclosed without informing individuals of the purpose and obtaining their consent.

The Lists of Electors

The lists of electors are based on data from the National Register of Electors, which is updated regularly from multiple sources, including information held by federal, provincial and territorial governments and by provincial electoral management bodies, and information provided by electors themselves.[11] The personal information that Elections Canada (EC) collects to develop the lists is regulated by the CEA and the *PA*.[12]

The CEA provides for the distribution of the lists of electors to political parties, candidates and/or members of Parliament during the electoral period and annually. These contain the elector's name, address and unique identifier.[13]

Authorized uses of the lists of electors include electoral purposes, communicating with electors, soliciting contributions and recruiting party members. It is prohibited to use personal information contained in the lists of electors for other purposes than those authorized by the CEA; offenders are liable to pay a fine up to $10,000 or spend up to one year in prison, or both.

A number of provincial and territorial (PT) election laws require or permit security measures to assist in ensuring that lists of electors distributed at the provincial and territory level are protected: for example, authorizing PT Chief Electoral Officers (CEOs) to include fictitious information in the list to trace unauthorized use;[14] instructions for the destruction, return or disposal of the list;[15] and direction to immediately inform the PT CEO of the loss of the list or information contained in it.[16] Some jurisdictions also require recipients to take

"reasonable steps" to protect lists from loss or unauthorized use;[17] in Quebec, recipients must undertake in writing to take appropriate measures to protect the list and restrict its use.[18]

Similar security measures are not enshrined in the CEA at the federal level. Nonetheless, best practices, including administrative, technical and physical measures, for safeguarding the lists of electors are included in EC guidelines. The guidelines provide templates so that recipients of the lists may declare their commitment to protect the information received, use it only for specified purposes and return it once it is no longer needed.[19] The guidelines also encourage list recipients to report any breaches so that EC may better understand where and when they occur and provide reassurances that they are being contained as much as possible and that potential privacy risks posed are being addressed.

Statements of Electors Who Voted

Political parties and candidates are also entitled to receive statements of electors who voted (sometimes referred to as "bingo sheets"). These documents contain numbers that, when matched with the lists of electors, allow parties to identify whether an elector assigned to a particular polling division has voted. With this information, parties and candidates can encourage registered electors who have not yet voted to do so.

For a number of years, the Act has provided that candidates' representatives who request them can get these statements after each day at the close of advance polling stations, as well as at intervals of no less than 30 minutes on polling day. The CEA was further changed to require the CEO to provide, to each candidate and each registered party that endorsed a candidate in an electoral district, the statements of the electors who voted on polling day in that electoral district; and more recently to require that the statements be provided in electronic form 180 days after the return of the writs.[20] In the lead-up to the next general election, the statements will assist parties in communicating with those electors who did or did not vote in the last election.

Unlike the lists of electors, there are no limits on the parties' uses on the statements of the electors who voted.

Privacy Policy Requirements

Under the CEA, political parties are required to adopt a policy with respect to the treatment of any personal information they collect, use or disclose. They must publish their policy online and provide it to the CEO in order to obtain and maintain their registration.[21]

The CEA also requires parties to list specific information that must appear in their policies,[22] including

- the type of information collected and how it is protected and used
- under what circumstances information may be sold
- details about employee training on the collection and use of personal information

- how the party collects and uses personal information created from online activity, and whether it uses cookies
- the name and contact information of a person to whom privacy concerns may be communicated

In British Columbia and Ontario, parties must provide their policies to the CEO in order to receive their lists of electors. Elections BC provides a template that parties are encouraged to use in creating their policies.[23] In Ontario, the legislation provides that every party must develop a policy to ensure that its candidates, elected members and employees comply with the authorized use of the lists of electors, and that the policy must follow guidelines set out by Elections Ontario.[24]

While the requirement to publish policies increases transparency into the personal information handling practices of political parties, some federal political parties already had substantive privacy policies on their websites before it was a requirement to do so. The new requirements have been broadly criticized as falling short of the fair information principles and for lacking any oversight mechanism to monitor whether parties actually abide by the contents of their policies.[25]

In response to proposed privacy policy requirements included in Bill C-76, the *Elections Modernization Act*, both the CEO and the Privacy Commissioner of Canada recommended that political parties be subject to privacy regulations. In addition, in response to the privacy-related provisions in the Bill, they also recommended that the new privacy policy requirements be amended to require policies to be consistent with the fair information principles set out in Schedule 1 of PIPEDA, and that there be some form of oversight to ensure parties are complying with their policies.[26] The Standing Committee on Access to Information, Privacy and Ethics also recommended subjecting parties to privacy laws,[27] to which the government responded that it "continues to reflect on the extension of Canada's privacy protection frameworks to political parties."[28]

Applying Fair Information Principles to Political Parties

The fair information principles are based on guidelines developed by the Organisation for Economic Cooperation and Development in 1980. These guidelines serve to harmonize privacy laws, uphold individual rights and facilitate the free flow of information across borders. They also served as the basis for the Canadian Standards Association's Model Code for the Protection of Personal Information. The voluntary model code set out minimum privacy standards to assist organizations in managing personal information. The model code was incorporated into Schedule 1 of PIPEDA in 2000. Ongoing reviews of PIPEDA and the *Privacy Act* acknowledge that the fair information principles may need to be reformed to protect privacy in the digital age.

In Canada, it has been widely recommended that political parties be required to adhere to fair information principles. The Office of the Privacy Commissioner of Canada (OPC) issued guidance that encourages parties to comply with the principles as outlined in PIPEDA.[29]

Moving beyond whether the fair information principles should apply to parties, this section poses questions in order to generate discussion on how the principles could be applied in practice to political parties. Consideration should be given to how these principles may apply to parties given their unique role in Canada's democracy, and to the amount and level of resources they may have.

Registered Third Parties

Third parties may also be organized to build and, in some cases, be capable of building complex databases that contain information on large numbers of Canadian electors, even though they do not receive lists of electors or statements of electors who have voted during the electoral period, and may reach these electors through micro-targeting.[30]

The CEA regulates certain activities of third parties during pre-election and election periods. A third party could be any person or group that wants to participate in or influence the election (other than political parties, electoral district associations, nomination contestants or candidates that are otherwise regulated). While the CEA does not contain any provisions restricting the collection, use and disclosure of personal information by third parties in the election context, third parties may be subject to restrictions in this regard under other legislation, depending on their particular context. This would be the case, for example, of private-sector agencies whose commercial activities are regulated under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Questions to consider:

- ***Should registered third parties be subject to privacy requirements as regulated entities under the CEA?***

Accountability

Organizations subject to PIPEDA are responsible for personal information under their control, which includes information they transfer to a third-party partner. They must establish policies and procedures to give effect to the principles under PIPEDA and designate a person accountable for the organization's compliance. Organizations should be transparent about their practices for handling personal information, including informing individuals of any breach of personal information that poses a significant risk of harm.[31]

As noted above, amendments to the CEA require political parties' privacy policies to indicate the name and contact information of someone responsible for privacy matters. Policies must explain what information is being collected, why, under what circumstances it would be sold, and employee training and practices related to collection of online information.

While privacy policies are notorious for being lengthy and unreadable, political parties' policies, while somewhat challenging to find on their websites, are written in laypersons' terms. This is positive from an openness perspective. However, informing the electorate may require more than a link to a policy, which may not be useful when canvassing or when sending automated texts.

Questions to consider:

- ***Besides publishing their privacy policies, what other requirements could parties be subject to in order to make them accountable for how they collect, use and disclose personal information?***
- ***When political parties share information with a third-party partner, should they continue to be held accountable for the use of that information?***

The European Union's General Data Protection Regulation (GDPR) prohibits the processing of personal data including political opinions, racial or ethnic origin, and religious or philosophical beliefs. Exemptions include when processing is for legitimate activities and appropriate safeguards are in place, the data is already public or processing is in the public interest.

The GDPR also states that in the course of electoral activities, political parties' processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

While political parties are exempt from some prohibitions on processing personal data, they are still responsible to ensure compliance with provisions of the legislation related to data protection, access requests, establishing consent to contact individuals, and data retention, minimization and deletion.

Consent

Under PIPEDA, knowledge and consent are required for the collection, use and disclosure of personal information, except where inappropriate. According to the OPC, "consent is considered meaningful when individuals are provided with clear information explaining what organizations are doing with their information."[32] Consent is important because it contributes to a trusting relationship between organizations and individuals.

The type of consent may vary. Explicit or express consent means that a person is informed of the purpose for collecting, using and disclosing their information and actively agrees to it. The OPC recommends that express consent be sought when the information being collected, used or disclosed is sensitive, outside what would be considered a

reasonable expectation, or could result in the risk of significant harm.[33] In other instances, consent may be implicit or implied, such as when the purpose is obvious.[34] In some instances it may not be appropriate to collect, use or disclose personal information even with consent.[35] Consent may also be withdrawn.

In the case of political parties in British Columbia that are subject to the PIPA, the BC Privacy Commissioner has recommended that when canvassing door to door, parties obtain express consent to collect information about gender, religion and ethnicity.[36] He also notes that parties do not have implied consent to develop voter profiles or predict voting behaviour, because this data analysis would not be obvious to a reasonable voter.[37]

As highlighted in a joint investigation into a BC firm that delivered micro-targeted ads on behalf of several Canadian political campaigns, appropriate consent must be obtained at the time of collection for all uses by the organization that originally collected the information or by any organization the information may be shared with. For example, if a party collected contact information for the purposes of keeping an elector up to date on a campaign, it should not share the information for the purposes of conducting data analysis or profiling without express consent.[38]

Canada's Anti-Spam Legislation is instructive regarding where a party/candidate has "implied consent" to send messages to persons with whom it has an existing non-business relationship. For example, if a person is a donor, is a volunteer or attended a meeting organized by a party/candidate, they are considered to have provided implied consent to a political party or candidate to receive a message. Implied consent is only valid if the relationship is established within the two years preceding the message.[39]

How organizations obtain consent may vary depending on how they interact with individuals (i.e., online consent may be provided by checking a box or by continuing to peruse a website, whereas in person it may be provided in writing, verbally or by voluntarily providing information). In certain circumstances, obtaining consent may not be possible in practice. For example, information can be collected in greater volume and velocity than before, as is the case with search engine indexing websites and big data analytics.[40]

In its September 2017 report on consent consultations, the OPC notes that achieving meaningful consent in the digital age has become increasingly difficult; the OPC recommends making consent more meaningful, providing alternatives to consent and improving governance. Similarly, in its recent PIPEDA paper, Innovation, Science and Economic Development Canada notes that the current consent model is challenged and may need to change.[41]

There are several exemptions[42] to the requirement to seek consent, including when collecting, using or disclosing the information is in the interests of the individual; to investigate the contravention of a law or the breach of an agreement or fraud; or for journalistic, artistic or literary purposes. Consent is not required when the information is publicly available, as defined by the regulations.[43] While some would appreciate that the regulations be updated to reflect today's digital reality (much of the information on the Internet is public), the OPC cautions that just because information is public does not mean there is no interest in protecting the information from misuse.[44] The OPC recommends that Parliament consider modernizing the rules on publicly available information and consider

examining the possibility of introducing exceptions where consent cannot be given or where societal benefits outweigh privacy incursions.[45]

The BC Privacy Commissioner has recommended that parties collect publicly available personal information without consent only if there is a "reasonable connection" between the purpose of collection and the purpose for which the information is publicly available.[46]

Consent is also not required for collection or disclosure if authorized by law, such as for the lists of electors and the statements of electors who voted, which are provided to political parties and candidates pursuant to the CEA.

Questions to consider:

- ***Under what circumstances should an elector's consent be implicit or explicit? Should consent be required for the collection and use of publicly available information?***
- ***Would any uses or disclosures of personal information be unacceptable, even with consent? Should such areas be expressly delineated by law?***
- ***Should there be any regulation about how information that Elections Canada provides to parties can be combined with other sources of information?***
- ***Should electors' consent be obtained for providing lists of electors and statements of electors who voted to political parties and candidates?***

Identifying Purposes, Limiting Collection and Limiting Use, Disclosure and Retention

At or before the time it is collected, organizations subject to PIPEDA must identify why they collect personal information; organizations must also limit its use, collection and disclosure to those identified purposes; and retain the information only as long as necessary to fulfill those purposes.[47]

Parties have a legitimate need to collect and use personal information in order to better understand the electorate's needs, communicate with them and increase their own chances of electoral success. However, based on the breadth of information that may be collected, directly or indirectly, there may be a risk that voter profiles contain information that is beyond what is necessary for campaigning purposes, and that such information is shared for unrelated purposes. Limiting collection also reduces the impact of potential security breaches, as well as inaccurate data. In British Columbia, sensitive information such as religion, gender or ethnicity must not be collected (unless there is express consent to do so).[48]

Recent amendments to the CEA require parties' privacy policies to be published online and to specify what information is collected and how it is used. However, not all transactions with parties, candidates or their volunteers occur online, and not all electors may be aware that policies exist. As such, and closely aligned to the principles of openness and consent, it is particularly important to identify why information is collected if the purpose is not directly linked to campaigning. For example, when signing a petition, individuals should be informed if their information may subsequently be used for any other purposes.[49]

Some have suggested that parties should delete data after every election[50]; however, the ability to communicate with electors for political purposes may be necessary between elections. Collecting data again from scratch would pose an organizational burden and does not align with the fact that federal parties receive the voters' lists annually (for electoral districts where they ran a candidate). In addition, requiring deletion could hinder any enforcement measures after an election. However, there may be some instances, such as when a party is deregistered or ceases to exist, where deletion, or other measures to ensure personal information is protected, may be warranted.

Parties may transfer personal information to organizations for a number of reasons, such as supporting provincial parties in their electoral campaigns, processing donations, making automated phone calls, targeting ads on social media or doing data analysis. While parties may share information with a spectrum of organizations for different purposes, the recent amendments to the CEA require only that parties indicate whether they sell data. At the time of writing, none of the policies of parties currently represented in the House of Commons indicate to whom parties may disclose personal information.[51] Given that parties now receive electronic statements of the vote in addition to lists of electors, their ability to share data, conduct data matching and target electors is increased.

Questions to consider:

- ***Should there be mandatory restrictions on what type of information parties collect, including sensitive information such as religion or sexual orientation?***
- ***Should there be restrictions on how long parties can retain personal information? How might that vary depending on the type of information (i.e., political opinions, financial information and address information)?***
- ***To what extent should parties be subject to clarifying the purposes for which personal information is collected, used and disclosed?***
- ***Should the CEA be amended to require that party privacy policies indicate under what circumstances a party may share personal information with a third party, such as provincial political parties?***

Accuracy and Individual Access

Organizations subject to fair information principles are responsible for ensuring that personal information is as accurate, complete and up to date as is necessary for the identified purposes, including by allowing individuals to challenge the information and have it amended, as appropriate. Upon request, an individual must be informed of the existence, use and disclosure of their personal information and must be given access to it.[52]

In order to communicate with electors, there is a strong incentive for parties to maintain up-to-date accurate information on their supporters as well as non-supporters.[53] It could be argued that parties' information is very accurate because they obtain lists of electors, because candidates and volunteers have connections to the local community, and because they go door to door collecting information. However, parties may not have perfect data, and as such they may also have an interest in allowing individuals to have access to their own information and to correct it.

PIPEDA requires that a refusal to provide access to information must be explained in writing. Schedule 1 states that "exceptions to the access requirement should be limited and specific … [and] may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege."[54]

Unlike PIPEDA, BC's PIPA, which applies to provincial parties in British Columbia, contains a clause that permits organizations with commissioner approval to disregard frivolous and vexatious access requests.[55] Such a provision could limit the risk that the right to access is used by political opponents to inundate their rivals' operations.

Lastly, the concepts of a right to data portability and the right to be forgotten have emerged following the passage of the GDPR. While there are complex challenges related to implementing either approach in the Canadian context, the right to access is the starting point for each. Through a right to access, individuals may obtain and move their data to a competitive organization or they may request that their data be deleted (or deindexed). However, political parties do not operate as private sector competitors or search engines. They have a legitimate need to retain information on persons who are not their members or even supporters to compete effectively in the electoral process.

Questions to consider:

- ***Should Canadians have the right to access their personal information from political parties?***
- ***Are there circumstances when it would be legitimate for political parties to decline access?***

Safeguarding Personal Information

Organizations subject to PIPEDA are required to employ safeguards to protect personal information against loss or theft and from unauthorized access, disclosure, copying, use or modification. Safeguards should be proportionate to the sensitivity of the information.[56]

In the 2019 federal budget, the government proposed to provide the Communications Security Establishment with additional funding of up to $4.2 million over three years, starting in 2019–2020, to provide cyber security advice and guidance to Canadian political parties and election administrators.

Following reports by the Communications Security Establishment, as well as increased funding in Budget 2019 to assist parties with cyber security efforts, it is clear that protecting against security risks to party databases is a priority of the government. It is also in parties' best interests not to be subject to a cyber attack or breach that could result in embarrassment or appearance of mismanagement, as mitigating such risks upholds the integrity of the electoral process. Privacy policies must include statements about how parties protect personal information they collect. As noted above, Elections Canada (EC) has issued guidelines for safeguarding the lists of electors, whereas many of those guidelines are enshrined in provincial and territorial election laws.

Aside from foreign cyber threats, inappropriate access and use of data may happen via party insiders. Improper communication with electors during the 2011 federal election allegedly stemmed from unauthorized access to a party database.[57] On the other hand, broad access to personal information by their volunteers enables parties to connect with and mobilize voters.

Since 2018, in cases where a breach of security safeguards creates a real risk of significant harm, PIPEDA requires not only that organizations report the breach to the OPC, but also that they notify all affected individuals. Breach notification requires striking the right balance between organizational flexibility and how prescriptive regulations should be.[58] Depending on how they are formulated, breach notification requirements could pose an organizational burden to smaller parties. There are also penalties for organizations that knowingly fail to report a breach, which could be ruinous for a smaller party. Also, in contrast to PIPEDA, EC guidelines for the lists of elections encourage parties and candidates to report privacy breaches of the lists of electors to EC, not to concerned individuals.

Questions to consider:

- ***Should the CEA impose mandatory security requirements on parties/candidates who receive the lists of electors?***
- ***Beyond legislating safeguards, what can be done to protect personal information held by political parties? How can parties manage their information holdings to safeguard information while also enabling campaign workers or volunteers to use that information to communicate with electors?***
- ***Could there be any challenges when applying PIPEDA's breach notification requirements to political parties? Should there be variations for political parties and/or candidates?***

Challenging Compliance

Under PIPEDA, individuals should be able to contact someone within an organization who is accountable if they have a complaint about its compliance with these principles or to lodge a complaint with a regulatory body that regulates the organization.[59] Further to amendments to the CEA, contact information of the person accountable is to be made public in parties' privacy policies. However, it is not clear whether parties have instituted complaints or grievance procedures should an individual contact them about how their personal information was or is being handled.[60]

This principle is reflective of PIPEDA's compliance model in which, prior to a formal investigation, individuals are encouraged to resolve complaints with the organization directly. Should a dispute not be resolved independently, the OPC conducts an investigation and issues a decision. However, the OPC cannot order an organization to comply. It largely relies on public shaming, audits, compliance agreements and, for certain violations, the courts.[61]

In order to promote compliance with the fair information principles, the Standing Committee on Access to Information, Privacy and Ethics, privacy commissioners, the CEO and academics have recommended that parties be subject to some form of external oversight.

While EC receives parties' privacy policies to maintain their registered status, the CEO has noted that the OPC is best suited to provide oversight over whether parties are indeed following the claims made in their policies.

Related to oversight are the potential penalties for non-compliance. Under PIPEDA, many have recommended that enforcement powers be enhanced to protect privacy in the digital age.[62] Under the CEA, penalties range broadly, depending on the nature of the offence. Administrative monetary penalties were recently introduced to promote compliance, instead of punishing offenders for minor violations. In other instances, such as the voter contact registry, the CRTC's enforcement options range from warning letters to negotiated undertakings or financial penalties.[63] It is also an offence to knowingly use the lists of electors for unauthorized purposes (that is, anything other than communicating with electors, soliciting contributions or recruiting members); the penalty is a fine of not more than $10,000 or one year in prison, or both.[64]

Another option may include voluntary codes of practice.[65] A voluntary code may be more palatable to political parties than legislated change, while at the same time moving towards increasing electors' privacy.

This is not to say that oversight cannot be shared, but that it is important to determine whether one or a mix of existing or new regimes is best suited to protect electors' privacy so that Canadians can continue to trust their electoral process.

Questions to consider:

- ***What type of privacy compliance model is best suited for political parties? Which body should provide oversight? Should parties be audited? What is the appropriate role for electoral management bodies, data protection authorities or other regulators?***
- ***What should be the nature of offences and penalties, if any?***
- ***Should there be recourses for individuals when their personal information is not treated in accordance with fair information principles?***
- ***Would a code of practice that political parties have agreed to be more appropriate than legislative action? Who should lead the development of such a code?***

Endnotes

[1] The Chief Electoral Officer (CEO) of Canada, the Directeur Général des Élections du Québec, the federal, provincial and territorial privacy commissioners, the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), as well as numerous academics have called for political parties to be subject to fair information principles.

Minister of Democratic Institutions Karina Gould has noted that subjecting political parties to privacy regulation requires further study to reach a balance between electors' privacy rights and the needs of parties to communicate with electors. The Minister said that, while ETHI recommended that parties be subject to privacy rules, the Standing Committee on Procedure and House Affairs (PROC) should study how privacy rules should be implemented to ensure that parties can engage with voters but have a regulatory framework that provides oversight.

Gould, Hon. Karina, and Hon. Navdeep Bains. "Government Response." (No date). https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-17/response-8512-421-502/; Radio-Canada. « Que font les partis politiques de vos données personnelles? » April 7, 2019. https://ici.radio-canada.ca/nouvelle/1162731/partis-politiques-utilisation-donnees-personnelles/

[2] The Cambridge Analytica scandal involved Facebook users' personal information being used without their knowledge or consent. A third-party app offered a cash reward for participating in an online survey about personality. The app directly reached approximately 320,000 users. Facebook's settings allowed the app to access the respondents' friends' page likes as well, resulting in a global network of up to 87 million users' data (including the data of 620,000 Canadians). This personal information was used to develop voter profiles and send targeted messages during the Brexit referendum and the US presidential election in 2016. It raised questions about the implications of digital campaigning and how it should be regulated.

Federal Trade Commission. FTC Sues Cambridge Analytica. July 24, 2019. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer/; UK Information Commissioner's Office. *Investigation into the Use of Data Analytics in Political Campaigns.* Report. 2018. 26. https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf; Standing Committee on Access to Information, Privacy and Ethics. *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process.* Report. 2018. https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf; Scott, Mark. "Cambridge Analytica Helped 'Cheat' Brexit Vote and US Election, Claims Whistleblower." Politico. March 27, 2018. https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/; Embury-Dennis, Tom, and Andrew Griffin. "Facebook Facing Maximum £500,000 by UK Privacy Watchdog over Breach of Data Laws." The Independent. July 11, 2018. https://www.independent.co.uk/news/uk/home-news/facebook-data-uk-election-brexit-referendum-fake-news-fine-commissioners-office-watchdog-a8441301.html/; Radio-Canada. « Que font les partis politiques de vos données personnelles? » April 7, 2019. https://ici.radio-canada.ca/nouvelle/1162731/partis-politiques-utilisation-donnees-personnelles/

[3] Report on the Investigation into Russian Interference in the 2016 Presidential Election. March 2019. https://www.justice.gov/storage/report.pdf

[4] Office of the Privacy Commissioner of Canada, 2018–19 Survey of Canadians on Privacy. March 2019. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

[5] Elections Canada. Survey of Electors on Communications with Electors. March 2013. https://www.elections.ca/res/cons/sece/sece_e.pdf

[6] Gruzd, Anatoliy, Jenna Jacobson, Philip Mai, and Elizabeth Dubois. "Social Media Privacy in Canada." *Ryerson University Social Media Lab* (2018): 9. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195503

[7] Esselment, Anna Lennox. "Perceptions of Parties in an Era of Big Data and Social Media: Data, Privacy, and the Ontario 2018 Election." University of Waterloo, 2019.

[8] Henry, Victoria. Open Media. June 12, 2018. https://openmedia.org/en/72-people-canada-support-stronger-privacy-rules-political-parties/

[9] Personal information is defined in the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act* as "information about an identifiable individual." *Personal Information Protection and Electronic Documents Act*, c. 5, s. 2(1) (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/P-8.6/; *Privacy Act*, c. P-21, s. 3 (R.S.C. 1985). https://laws-lois.justice.gc.ca/eng/acts/p-21/. Office of the Privacy Commissioner of Canada, Summary of Privacy Laws in Canada, January 2018. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/. Note that there is one exception to PIPEDA's coverage to organizations engaged in commercial activities listed in Schedule 4: the World Anti-Doping Agency.

[10] For an overview of the reasoning in the case, see Teresa Scassa, Decision Paves the Way for Federal Riding Associations in BC to Be Subject to BC's Data Protection Laws. August 30, 2019. http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=313:decision-paves-the-way-for-federal-riding-associations-in-bc-to-be-subject-to-bcs-data-protection-laws&Itemid=80/

[11] Elections Canada. "Description of the National Register of Electors." July 17, 2019. https://www.elections.ca/content.aspx?section=vot&dir=reg/des&document=index&lang=e#optout/

[12] See an overview of privacy at Elections Canada for further details: https://www.elections.ca/content.aspx?section=abo&dir=pri&document=index&lang=e/

[13] *Canada Elections Act*, c. 9, s. 44(2) (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/E-2.01/; for an overview of provincial and territorial lists of electors, see Élections Québec. *Partis politiques et protection des renseignements personnels: Exposé de la situation québécoise, perspectives comparées et recommandations.* Report. 2019. 33. https://www.electionsquebec.qc.ca/english/news-detail.php?id=6299/

[14] For example, see Nova Scotia, *Elections Act*, c. 50, s. 62(1) (S.N.S.). https://nslegislature.ca/sites/default/files/legc/statutes/elections.pdf; Manitoba, *The Elections Act*, c. E30, s. 63.9(5) (C.C.S.M. 2006). https://web2.gov.mb.ca/laws/statutes/ccsm/e030e.php#63.1/; Alberta, *Election Act*, c. E-1, s. 18(7) (R.S.A.). http://www.qp.alberta.ca/documents/Acts/E01.pdf; British Columbia, *Election Act*, c. 106, s. 51(3) (R.S.B.C. 1996). http://www.bclaws.ca/civix/document/id/complete/statreg/96106_04#division_d2e4406/

[15] For example, see Nova Scotia, *Elections Act*, c. 50, s. 62(2) (S.N.S.). https://nslegislature.ca/sites/default/files/legc/statutes/elections.pdf; Northwest Territories; *Elections and Plebiscite Act*, c. 15, s. 75(3) (S.N.W.T. 2006). https://www.electionsnwt.ca/sites/electionsnwt/files/2018-11-20_elections_and_plebiscites_act.pdf

[16] For example, see Manitoba, *The Elections Act*, c. E30, s. 63.9(2) (C.C.S.M. 2006). https://web2.gov.mb.ca/laws/statutes/ccsm/e030e.php#63.1/; Alberta, *Election Act*, c. E-1, s. 19.1(2) (R.S.A.). http://www.qp.alberta.ca/documents/Acts/E01.pdf

[17] For example, see Manitoba, *The Elections Act*, c. E30, s. 63.9(1) (C.C.S.M. 2006). https://web2.gov.mb.ca/laws/statutes/ccsm/e030e.php#63.1/; Alberta, *Election Act*, c. E-1, s. 19.1(1) (R.S.A.). http://www.qp.alberta.ca/documents/Acts/E01.pdf; Yukon, *Elections Act*, c. 63, s. 49.13(1) (R.S.Y. 2002). http://www.gov.yk.ca/legislation/acts/elections_c.pdf

[18] *Election Act*, c. E-3.3, s. 40.38.3 (C.Q.L.R.). http://legisquebec.gouv.qc.ca/en/showdoc/cs/E-3.3?langCont=en#ga:l_ii_1-h1/

[19] Elections Canada. "Guidelines for Use of the Lists of Electors." August 1, 2019. https://www.elections.ca/content.aspx?section=pol&document=page4&dir=ann/loe_2019&lang=e/

[20] See *Canada Elections Act*, s. 541.1 and s. 162 (i.1).

[21] Party registration includes such benefits as the ability to issue tax receipts for contributions, have the party name appear on an election ballot, reimbursement of election expenses, allocation of broadcasting time, ability

to provide the returning officer with the names of suitable persons to act as election officers, and receipt of the annual lists of electors for electoral districts where they ran confirmed candidates in the previous election.

Elections Canada. "Registration of Federal Political Parties." (No date). https://www.elections.ca/content.aspx?section=pol&dir=pol/bck&document=index&lang=e/

[22] *Canada Elections Act*, c. 9, s. 385(2) (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/E-2.01/

[23] BC's legislation defines a privacy policy as a policy that sets out "reasonable security arrangements" in respect of personal information. The template includes the scope of the policy (to whom and to what it applies); restrictions on use of personal information; responsibilities of the recipients of the personal information; security (including precautions taken to ensure the security and confidentiality of personal information); disposition of personal information; tracking of distribution; loss, theft or unauthorized access; and compliance audits.

Election Act, c. 106, s. 275(4.3) (R.S.B.C. 1996). http://www.bclaws.ca/civix/document/id/complete/statreg/96106_04#division_d2e4406/; Elections BC. "Privacy Policy Template for Political Parties." 2015. https://elections.bc.ca/docs/privacy/00157.pdf; Elections BC. "Privacy Policy Acceptance Criteria." 2016. https://elections.bc.ca/docs/privacy/00158.pdf

[24] Guidelines provide for minimum criteria to be included in parties' privacy policies. These include the scope and application of the policy; restrictions on use of the lists of electors, including the relevant provisions of the Ontario *Election Act* and measures implemented to track the distribution of lists and administer written acknowledgement forms (which must be signed by each person authorized to receive the list and state that the person understands how the list is to be used and protected); privacy requirements (including the measures implemented to ensure compliance with the privacy requirements); and roles and responsibilities of the Chief Privacy Officer and all political entity representatives.

Election Act, c. E.6, s. 17.6 (R.S.O. 1990). https://www.ontario.ca/laws/statute/90e06/; Elections Ontario. "Guidelines for the Use of Electoral Products." 2019. https://www.elections.on.ca/content/dam/NGW/sitecontent/2017/resources/policies/Guidelines%20For%20the%20Use%20of%20Electoral%20Products.pdf

[25] See, for example, comments made by the Privacy Commissioner of Canada, stating before the House of Commons Standing Committee on Procedure and House Affairs that the new requirements in C-76 "fall short" of globally accepted fair information principles and that Bill C-76 "adds nothing of substance." June 5, 2018. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180605/

[26] Elections Canada, Proposed Amendments to Bill C-76 Presented by the Acting Chief Electoral Officer to the Standing Committee on Procedure and House Affairs. May 28, 2018. https://www.elections.ca/content.aspx?section=med&dir=spe&document=c76&lang=e/; Office of the Privacy Commissioner of Canada, Appearance before the Standing Committee on Procedure and House Affairs on the study about Bill C-76, *Elections Modernization Act.* June 5, 2018. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20180605/

[27] Standing Committee on Access to Information, Privacy and Ethics. "Democracy under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly. December 2018. https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-17/

[28] Gould, Hon. Karina, and Hon. Navdeep Bains. "Government Response." (No date). https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-17/response-8512-421-502/

[29] Office of the Privacy Commissioner of Canada. "Guidance for Political Parties on Protecting Personal Information." April 1, 2019. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/

[30] Such concerns were expressed before the Standing Committee on Access to Information, Privacy and Ethics on November 1, 2018. https://www.ourcommons.ca/Content/Committee/421/ETHI/Evidence/EV10151086/ETHIEV124-E.PDF

[31] *Personal Information Protection and Electronic Documents Act*, c. 5, Schedule 1 (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/P-8.6/; Office of the Privacy Commissioner of Canada. "Guidance for Political Parties

on Protecting Personal Information." April 1, 2019. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/

[32] Office of the Privacy Commissioner of Canada. "Consent." 2019. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/

[33] Office of the Privacy Commissioner of Canada. "Guidelines for Obtaining Meaningful Consent: Determining the Appropriate Form of Consent." 2018. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#_determining/

[34] *Personal Information Protection and Electronic Documents Act*, c. 5, Schedule 1, s. 4.3 (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/; McEvoy, Michael. *Full Disclosure: Political Parties, Campaign Data, and Voter Consent.* Report. Office of the Information and Privacy Commissioner for British Columbia. 2019. 9. https://www.oipc.bc.ca/investigation-reports/2278/; Office of the Privacy Commissioner of Canada. "Interpretation Bulletin: Form of Consent." 2014. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_07_consent/

[35] Office of the Privacy Commissioner of Canada. *2016–17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act.* Report. 2017. 14–15. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1/

[36] McEvoy, Michael. *Full Disclosure: Political Parties, Campaign Data, and Voter Consent.* Report. Office of the Information and Privacy Commissioner for British Columbia. 2019. 16. https://www.oipc.bc.ca/investigation-reports/2278/

[37] McEvoy, Michael. *Full Disclosure: Political Parties, Campaign Data, and Voter Consent.* Report. Office of the Information and Privacy Commissioner for British Columbia. 2019. 21–23. https://www.oipc.bc.ca/investigation-reports/2278/

[38] See Office of the Privacy Commissioner of Canada. Joint Investigations of AggregateIQ Data Services Ltd. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia. November 26, 2019. Paras 63–66, 85–98 and 94. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-004/

[39] The collection of personal information or contact information and the sending of commercial electronic messages (CEMs) (i.e., emails, texts or telephone calls that offer or promote goods or services for sale) are prohibited without consent. The regulations exempt CEMs sent by or on behalf of political parties, candidates and nomination contestants where the "message has as its primary purpose soliciting a contribution" as defined by the CEA. This means that parties and candidates do not need consent to send messages that, for example, request a donation or non-monetary contribution or promote a fundraising event.

Electronic Commerce Protection Regulations, SOR/2013-221, s. 3(h). https://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-221/page-1.html#h-5/; Canadian Radio-television and Telecommunications Commission. "Frequently Asked Questions about *Canada's Anti-Spam Legislation*." (No date). https://crtc.gc.ca/eng/com500/faq500.htm/; 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 Ac*t and the *Telecommunications Act*, c. 23, s. 10(13)(a)(b) (S.C. 2010). https://laws-lois.justice.gc.ca/eng/acts/E-1.6/page-1.html/

[40] Office of the Privacy Commissioner of Canada. *2016–17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act.* Report. 2017. 3–4. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1/

[41] Office of the Information and Privacy Commissioner of Canada. "Results of Consent Consultation Highlighted in Commissioner's 2016–17 Annual Report." September 21, 2017. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2017/bg_170921_consent/; Innovation, Science and Economic Development Canada. "Strengthening Privacy for the Digital Age: Proposals to Modernize the *Personal Information Protection and Electronic Documents Act*." 2019. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html/

[42] See PIPEDA, s.7.

[43] According to the *Regulations Specifying Publicly Available Information*, publicly available information is defined as information contained in phone books (where the person may choose not to have their information listed), in a publication (where the person has provided their information), professional or business directories, publicly available registries, and judicial or quasi-judicial records (so long as the information is collected for the same purpose that it is in the directory, registry or records).

Regulations Specifying Publicly Available Information, s. 1 (SOR/2001-7). https://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-7/page-1.html#h-679226/; Office of the Privacy Commissioner of Canada. "Publicly Available Information." 2014. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_06_pai/

[44] Office of the Privacy Commissioner of Canada. *2016–17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act.* Report. 2017. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1/

[45] Office of the Information and Privacy Commissioner of Canada. "Results of Consent Consultation Highlighted in Commissioner's 2016–17 Annual Report." September 21, 2017. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2017/bg_170921_consent/; Innovation, Science and Economic Development Canada. "Strengthening Privacy for the Digital Age: Proposals to Modernize the Personal Information Protection and Electronic Documents Act." 2019. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html/

[46] McEvoy, Michael. *Full Disclosure: Political Parties, Campaign Data, and Voter Consent.* Report. Office of the Information and Privacy Commissioner for British Columbia. 2019. 21, 24. https://www.oipc.bc.ca/investigation-reports/2278/

[47] *Personal Information Protection and Electronic Documents Act*, c. 5, Schedule 1, s. 4.6, 4.9 (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/; Office of the Privacy Commissioner of Canada. "Guidance for Political Parties on Protecting Personal Information." April 1, 2019. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/

[48] McEvoy, Michael. *Full Disclosure: Political Parties, Campaign Data, and Voter Consent.* Report. Office of the Information and Privacy Commissioner for British Columbia. 2019. 15–16. https://www.oipc.bc.ca/investigation-reports/2278/

[49] McEvoy, Michael. *Full Disclosure: Political Parties, Campaign Data, and Voter Consent.* Report. Office of the Information and Privacy Commissioner for British Columbia. 2019. 19. https://www.oipc.bc.ca/investigation-reports/2278/

[50] Élections Québec. *Partis politiques et protection des renseignements personnels: Exposé de la situation québécoise, perspectives comparées et recommandations.* Report. 2019. 87. https://www.electionsquebec.qc.ca/english/news-detail.php?id=6299/

[51] OpenMedia. *Canada's Political Parties' Privacy Policies: An Assessment Against Best Practices Defined by Elections Canada and the Office of the Privacy Commissioner.* Report. 2019. 2. https://act.openmedia.org/sites/default/files/Political%20party%20policies_%20scorecard%20analysis.pdf

[52] *Personal Information Protection and Electronic Documents Act*, c. 5, Schedule 1, s. 4.2, 4.4, 4.5 (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/; Office of the Privacy Commissioner of Canada. "Guidance for Political Parties on Protecting Personal Information." April 1, 2019. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/

[53] Of the five parties represented by more than one member in the House of Commons, all make statements in their privacy policies that individuals can contact them to keep their information up to date.

[54] *Personal Information Protection and Electronic Documents Act*, c. 5, Schedule 1, s. 4.9 (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

[55] Alberta's PIPA, which does not apply to political parties but applies to some non-profit organizations, contains a similar provision. Note that the BC Information and Privacy Commissioner is determining whether

PIPA applies to federal parties that campaign in BC. *Personal Information Protection Act*, c. 63, s. 37 (S.B.C. 2003). http://www.bclaws.ca/civix/document/id/complete/statreg/03063_01#section37/

[56] *Personal Information Protection and Electronic Documents Act*, c. 5, Schedule 1, s. 4.7 (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/; Office of the Privacy Commissioner of Canada. "Guidance for Political Parties on Protecting Personal Information." April 1, 2019. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/

[57] R. v. Sona. (ONCJ 2014). Para 5, 9–11. https://www.canlii.org/en/on/oncj/doc/2014/2014oncj365/2014oncj365.html/

[58] Innovation, Science and Economic Development Canada. "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians." 2019. https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html/

[59] *Personal Information Protection and Electronic Documents Act*, c. 5, Schedule 1, s. 4.10 (S.C. 2000). https://laws-lois.justice.gc.ca/eng/acts/p-8.6/; Office of the Privacy Commissioner of Canada. "Guidance for Political Parties on Protecting Personal Information." April 1, 2019. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/gd_pp_201904/

[60] Of the five parties represented by more than one member in the House of Commons, only the CPC and Bloc Québécois privacy policies refer to contacting them if there are "complaints"; the NDP refers to questions or concerns; the Green Party of Canada and LPC refer to questions.

[61] *Personal Information Protection and Electronic Documents Act*, c. 5, s. 12 (1)(a); see also Office of the Privacy Commissioner, Enforcement of PIPEDA, https://www.priv.gc.ca/biens-assets/compliance-framework/en/index#/. For a recent example of the OPC commencing court proceedings, see Office of the Privacy Commissioner of Canada. *Joint Investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia.* Report of findings. 2019. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/; Office of the Privacy Commissioner of Canada. "Facebook Refuses to Address Serious Privacy Deficiencies Despite Public Apologies for 'Breach of Trust.'" April 25, 2019. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/nr-c_190425/

[62] For example, see Scassa, Teresa. Reforms to PIPEDA Must Give the Privacy Commissioner Real Enforcement Powers. June 7, 2018. https://policyoptions.irpp.org/magazines/june-2018/enforcement-powers-key-pipeda-reform/; Recommendation 15: That the *Personal Information Protection and Electronic Documents Act* be amended to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance. ETHI Report, Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act. February 2018. https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12/

[63] CRTC. Voter Contact Registry. https://crtc.gc.ca/eng/phone/rce-vcr/guide-pol-en.pdf; CRTC's maximum administrative monetary penalties (AMPs) range from $1500 for individuals to $15,000 for corporations. In the CEA, AMPs range from $1500 for individuals to $5000 for corporations or entities.

[64] See *Canada Elections Act*, s. 485(1), s. 56(e), s. 110 and s. 500(3). Note that under 110(3), candidates may use the lists only for fair authorized purposes during election periods.

[65] Information Commissioner's Office. *Guidance on Political Campaigning: Draft Framework Code for Consultation.* 2019. https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf; Elections Canada. A Code of Ethics or Code of Conduct for Political Parties as a Potential Tool to Strengthen Electoral Democracy in Canada. 2018. https://www.elections.ca/content.aspx?section=res&dir=rec/tech/cod&document=p1&lang=e/