Canada

Preventing Deceptive Communications with Electors

Recommendations from the Chief Electoral Officer of Canada
Following the 41st General Election

Library and Archives Canada Cataloguing in Publication

Elections Canada

Preventing deceptive communications with electors – Recommendations from the Chief Electoral Officer of Canada following the 41st general election [electronic resource]

Electronic monograph in PDF format.

Issued also in French under title: Prévenir les communications trompeuses avec les électeurs – Recommandations du directeur général des élections à la suite de la 41e élection générale.

Issued also in printed form.

ISBN 978-1-100-21939-4
Cat. No. : SE3-78/2013E-PDF

1. Canada. Parliament — Elections.
2. Elections — Canada.
3. Elections — Corrupt practices — Canada.
4. Political campaigns — Canada.
5. Canada. Parliament — Elections, 2011.
6. Election law — Canada.

I. Title.
II. Title: Recommendations from the Chief Electoral Officer of Canada following the 41st general election.

JL193 E43 2013 324.60971 C2013-980031-X

For enquiries, please contact:

Public Enquiries Unit
Elections Canada
257 Slater Street
Ottawa, Ontario
K1A 0M6
Tel.: 1-800-463-6868
Fax: 1-888-524-1444 (toll-free)
TTY: 1-800-361-8935
www.elections.ca

The Chief Electoral Officer • Le directeur général des élections

March 26, 2013

The Honourable Andrew Scheer
Speaker of the House of Commons
Centre Block
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Speaker:

Please find enclosed my report *Preventing Deceptive Communications with Electors – Recommendations from the Chief Electoral Officer of Canada Following the 41st General Election*.

This report is in response to incidents that occurred during the 41st general election of May 2, 2011, involving deceptive communications with electors. The report is made pursuant to section 535 of the *Canada Elections Act* and proposes amendments that, in my opinion, are desirable for the better administration of the Act.

Under section 536 of the Act, the Speaker shall submit this report to the House of Commons without delay.

Yours truly,

Marc Mayrand
Chief Electoral Officer

257 Slater Street/257, rue Slater, Ottawa, Canada K1A 0M6 • 613-993-2975 Fax/Télécopieur : 613-993-5380
1-800-463-6868 TTY/ATS 1-800-361-8935 www.elections.ca

Table of Contents

Introduction

This report is in response to incidents that occurred during the 41st general election of May 2, 2011, involving deceptive communications with electors. While the investigation by the Commissioner of Canada Elections remains ongoing and the full scope of these incidents as well as the identity of persons involved remain to be established, the nature of the conduct that took place is well known. The public reaction to those incidents demonstrates the importance that Canadians attach to the integrity of their electoral process and the need to take steps to prevent a recurrence of such tactics in the future.

This report is the first of two thematic recommendations reports following the 41st general election. Given the importance of the matters at stake and the need to implement measures in time for the next general election, it was necessary to deal immediately with the issue of deceptive communications. A subsequent report will more broadly address the need to review and modernize the compliance and enforcement mechanisms in the *Canada Elections Act* with a view to making them more effective and better tailored to the regulatory nature of the regime. We plan to present this second report in the spring of 2014.

As indicated to the Standing Committee on Procedure and House Affairs on March 29, 2012, the purpose of this first report is to examine preventive and enforcement measures that should be taken to deal with deceptive communications. While some of the measures proposed in the report are administrative, the majority require legislative changes.

The report builds on a discussion paper released in early November 2012. In preparing the report, Elections Canada consulted Canadian electors and used the discussion paper to engage political parties as well as experts on the matters at play. The aim was to capture their concerns and insights with respect to communications with electors by Elections Canada and political entities, in the context of the electoral process.

A firm was retained to conduct a telephone survey with 1,011 electors within the general population. The purpose of the survey was to evaluate the opinions and attitudes of electors on a number of questions related to communications with electors. That survey was conducted from November 21 to December 2, 2012. The full report on the survey may be found on Elections Canada's website at www.elections.ca.

As well, Elections Canada entered into a contract with the Institute for Research on Public Policy (IRPP), a think tank based in Montréal, to convene and facilitate a day-long roundtable discussion with experts and practitioners from a range of disciplines. The purpose of this roundtable was to provide information and advice to the Chief Electoral Officer on how the Canadian electoral process could be improved in the future. A link to the report of the IRPP may also be found on Elections Canada's website at www.elections.ca.

In responding to the events that took place at the last election, it is important to achieve a proper balance between competing values and interests. New technology offers tremendous opportunities for political parties and candidates to gather information, in order to target and

reach out to electors. More importantly, for electors, communications from and with candidates and parties are fundamental to their effective participation in the electoral process, which is the very essence of the right to vote. In both the survey of electors and the roundtable discussion, it was broadly recognized that the ability to effectively communicate with electors is critical. At the same time, however, Canadians and experts strongly endorse the view that respect for the privacy of electors and the preservation of trust in the integrity of the electoral process are essential.

In this regard, our regime needs to be improved. While political parties and candidates must continue to be able to communicate with electors effectively, measures are required to provide basic privacy protections and help prevent deceptive communications.

As well, the challenges experienced in investigating the deceptive calls that were made during the 41st general election have demonstrated the need for better tools to assist the Commissioner in conducting investigations. Recommendations are made in this report for tools that are already available in the federal context for other regulatory regimes and that are available to a number of electoral management bodies in other jurisdictions.

Of course, legislative measures alone cannot prevent improper conduct from taking place. All participants in the electoral process have a responsibility to act in a manner that respects and promotes democratic values and the rule of law.

For electors, the revelation of various scandals, at both the federal and provincial levels, involving illicit fundraising methods, abuse of spending limits and deceptive communications tactics, raises disturbing questions. The issue is not simply one of compliance with legal requirements, but also respect for values of fair play. The line separating conduct that is a normal part of a healthy and vigorous electoral competition from conduct that undermines the legitimacy of the election is at risk of becoming increasingly blurred and uncertain.

In this regard, the fact that, in the context of the survey referred to above, electors are more likely to indicate that they have not very much confidence (46%) or no confidence (10%) in federal political parties should be of concern to all. For this reason, the report goes beyond strict concerns over legal requirements and recommends that consideration be given to the adoption of codes of conduct by political parties that would set out rules of behaviour for political parties and their supporters.

But codes of conduct are not enough. The electoral legislation must be sufficiently robust, not only in terms of the penalties but also of the tools available to effectively uncover acts of wrongdoing. If it is not, there is a real danger that participants will increasingly take the position that it is more advantageous to ignore the rules than to respect them, particularly if they are under the impression that their opponents are not abiding by these rules. While trust in the electoral process remains high (85% as per the survey of electors), it should not be taken for granted. Ultimately, what is at stake is the ability of the electoral process to play its fundamental role of legitimizing political power.

1. Chronology of Events

The recommendations contained in this report aim to address various forms of deceptive communications with electors and are not restricted to the specific acts that took place in the 41st general election. Nonetheless, it is important to provide the context that gave rise to this report and the recommendations it puts forward. This part of the report reviews what the investigation has so far publicly disclosed about what happened in Guelph and in other electoral districts, as well as various actions taken in Parliament and through the courts as a result.

Initial calls and complaints (Guelph and elsewhere)

In the days leading up to polling day, on polling day, May 2, 2011, and in the days that followed, Elections Canada received a number of complaints regarding automated calls, purportedly from Elections Canada, falsely informing recipients of a change in polling locations (primarily in Guelph, but complaints came in from other electoral districts as well).

The agency also received other complaints alleging numerous, repetitive, annoying or sometimes aggressive live or automated calls, as well as calls made late at night, on a religious holiday or from American area codes. These calls were purportedly made on behalf of candidates whose campaigns have subsequently often denied making the calls.

In one case, a professional call centre has since acknowledged that some electors were given erroneous information concerning their polling location based on inaccurate or outdated data.

Investigation of the Guelph complaints

The information that follows is already publicly known.[1] It is summarized here to the extent necessary to provide context for the report, and not to suggest or prejudge the result of the investigation.

Numerous complaints were received about telephone calls made to electors in the electoral district of Guelph, around 10 a.m. on May 2, 2011. The caller was described as a recorded female voice claiming to call on behalf of Elections Canada. The message was that due to a projected increase in poll turnout, the elector's voting location had been changed to another address. There was no truth to these calls. The caller was not representing Elections Canada, and no polling locations had been moved in that district.

The calling number that appeared on the call display of recipients' phones was the same for all recipients. Through the investigation, it was later found out that this number was assigned to a pay-as-you-go cell phone that was activated on April 30, 2011. The subscriber's name in Bell Canada's records is Pierre Poutine of Separatist Street in Joliette, Quebec. There is no such name or street in Joliette.

[1] The following is based on information that was made publicly available through court records in the course of the Commissioner of Canada Elections' investigation.

The investigation established that Pierre Poutine's phone only ever called two phone numbers, both of which are assigned to a voice broadcasting vendor in Edmonton that also provided services to the campaign of a candidate in Guelph.

The individual initiating the calls was accepted by the voice broadcasting vendor as a client. Records from the vendor show that 7,676 calls were made to Guelph telephone numbers between 10:03 and 10:15 a.m. (Eastern Daylight Saving Time) on May 2, 2011, bearing the calling number assigned to this individual. The list of numbers that were called is consistent with a list of non-supporters of a political party that could have been obtained from that party's database.

The individual used a different false name and address in his communications with the voice broadcasting vendor (Pierre Jones of 54 Lajoie Street in Joliette, Quebec). There is no such address in that city.

The individual used PayPal to pay for the services rendered by the voice broadcasting vendor and gave PayPal that same false name and address. Payments (totalling $162.10) were made using three separate prepaid Visa cards purchased from two different Shoppers Drug Mart stores located in Guelph. All were made from a computer through a proxy server using the same IP address,[2] which allows the originating sender to disguise the location of the computer. The individual also used the proxy server to communicate with the voice broadcasting vendor on some occasions.

On other occasions, the individual communicated with the voice broadcasting vendor using an IP address associated with the campaign office of a candidate running in the electoral district of Guelph. Personnel at the campaign office used the same IP address to communicate legitimately with the voice broadcasting vendor, and also with a political party to access its database.

The calls made to electors were transmitted from the voice broadcasting vendor using VoIP (voice over Internet Protocol) calling technology. VoIP calling is computer-generated calling over the Internet to recipients' telephones. This technology allows a voice broadcasting vendor to program into the call process any calling number its client wishes to be displayed on a recipient's call display. That number could have nothing to do with the actual call made by the vendor.

Disclosure by the media in February 2012 of court documents related to the investigation

Following the disclosure of the above information in articles first published in the media on February 23, 2012, and on following days, more than 40,000 communications were received from electors. Most of these communications expressed outrage that individuals would try to weaken the electoral process by making false and misleading calls to electors. However, a significant number of individuals from electoral districts across Canada made specific complaints regarding improper calls.

[2] An Internet Protocol (IP) address is a numerical address assigned to each computer device that uses the Internet Protocol for communication on the Internet. The IP address can provide the physical address of a computer connected to the Internet through access to records of the Internet service provider.

Investigation of complaints received from individuals in other electoral districts

Complaints with respect to inappropriate calls outside Guelph were received over a longer period of time than was the case in Guelph. While some complaints were received during the 41st general election and in the months following the election, the Commissioner of Canada Elections[3] received over a thousand reports from complainants outside Guelph following the February 23, 2012, story in the media.

Some complainants reported having received either live or recorded telephone calls on or around polling day, which many recall as claiming to be from officials calling on behalf of Elections Canada, advising the call recipients that their polling station had been changed. In almost all cases, the purported polling station was farther away from the elector's place of residence and less convenient for the elector to reach.

Some complainants also reported having received annoying calls during the weeks leading up to polling day, typically at inopportune times of day or made in a series of calls to the same complainant, purportedly seeking support for a particular candidate or federal political party. Representatives of political parties and of candidates in whose names the calls were ostensibly made were subsequently contacted by Elections Canada investigators, and in most cases, the persons contacted denied making or being a party to such calls.

Appearance of the Chief Electoral Officer before the House of Commons Standing Committee on Procedure and House Affairs

As a result of the media reports of February 2012 and of the public debate that followed, the Chief Electoral Officer asked to appear before the Standing Committee on Procedure and House Affairs to explain key aspects of Elections Canada's administrative and investigative processes. This appearance took place on March 29, 2012.

On that date, the Chief Electoral Officer reported that the number of complaints alleging specific occurrences of improper or fraudulent calls was near 800.[4] He also committed to submitting a report, no later than March 31, 2013, that would examine the challenges posed by such calls and recommend improvements to the legislative framework.

Other related events

On March 12, 2012, the House of Commons unanimously passed a motion that reads as follows:

> That, in the opinion of the House, the government should, within six months, table amendments to the Elections Canada Act [sic] and other legislation as required that would ensure that: (a) Elections Canada investigation capabilities be strengthened, to include giving the Chief Electoral Officer the power to request all necessary documents from political parties to ensure compliance with the Elections Act; (b) all telecommunication companies that provide voter

[3] The Commissioner of Canada Elections is a statutory officer responsible for the enforcement of the *Canada Elections Act* as well as the *Referendum Act*. He is appointed by the Chief Electoral Officer pursuant to section 509 of the *Canada Elections Act*.

[4] This number reflects instances of alleged improper phone calls reported by electors, as opposed to expressions of outrage or calls for action. In his appearance of May 29, 2012, before the Committee, the Chief Electoral Officer indicated that the number of complaints regarding alleged fraudulent calls then exceeded 1,100. It now stands at just over 1,400.

> contact services during a general election must register with Elections Canada; and (c) all clients of telecommunication companies during a general election have their identity registered and verified. [5]

From March to December 2012, 19 petitions were presented in the House of Commons regarding the events that took place in the 41st general election. Most of these petitions asked for a full and independent inquiry into these events while one called upon members of Parliament "to immediately enact legislation that would give Elections Canada the ability to restore public confidence in Canada's electoral process."[6] The Government responded to these petitions by first stating its agreement with the importance of maintaining Canadians' confidence in the integrity of the electoral system. It indicated its intention to conduct a broad review of the *Canada Elections Act*, taking into account, among other things, forthcoming recommendations of the Chief Electoral Officer as well as those from the Standing Committee on Procedure and House Affairs.

On March 23, 2012, seven individuals made distinct applications to the Federal Court to have the results of the 41st general election in each of their respective electoral districts declared null and void, pursuant to paragraph 524(1)(*b*) of the Act. The grounds of the applications were that calls were purposefully made to electors who supported the candidates of specific parties to provide them with incorrect information about their polling site and that these were fraudulent calls that affected the results of the elections. The electoral districts involved were Don Valley East (Ontario), Nipissing–Timiskaming (Ontario), Winnipeg South Centre (Manitoba), Elmwood–Transcona (Manitoba), Saskatoon–Rosetown–Biggar (Saskatchewan), Vancouver Island North (British Columbia) and Yukon. The application contesting the election in Don Valley East was subsequently withdrawn. The case was heard by a judge of the Federal Court in December 2012, but, as of March 15, 2013, a decision had not yet been rendered.

Another application was filed in June 2012 by the Marijuana Party candidate in Guelph, contesting the election in that electoral district. The applicant alleges that the results of the election – that is, the number of votes cast for him – were affected by improper calls, purportedly from Elections Canada, directing voters to non-existent polling stations. The applicant is not alleging, however, that the respondent member of Parliament – whose supporters were also targeted by these calls – would not have been elected. The respondent member of Parliament filed a motion to strike the application on a number of grounds, including that the application was filed out of time. The motion to strike was heard by a judge of the Ontario Superior Court of Justice on October 29, 2012. As of March 15, 2013, a decision had not yet been rendered.

Finally, on October 12, 2012, Bill C-453, a private member's bill entitled *An Act to amend the Canada Elections Act (preventing and prosecuting fraudulent voice messages during election periods)* was tabled and read for the first time in the House of Commons. The proposed enactment would amend the *Canada Elections Act* to make it an offence, during an election period, to knowingly transmit false information, to falsely represent oneself as an election officer in voice messages related to an election, or to assist such fraudulent transmissions. As well, it would require that any registered party, candidate, third party engaging in election advertising or electoral district association provide certain information related to voice messaging to the Chief

[5] Canada, House of Commons, *Journals*, 41st Parliament, 1st session, no. 94, March 12, 2012.

[6] See the June 12, 2012, petition tabled by Mr. Kevin Lamoureux (Winnipeg North).

Electoral Officer or the Commissioner of Canada Elections upon request. It would further require that a company or other persons contracted to transmit voice messages provide certain information to the Chief Electoral Officer. The proposed enactment also makes it an offence to contravene these provisions. The bill has not yet received second reading.

Current status

The Commissioner has received complaints from more than 1,400 electors in 247 electoral districts, who report having received calls misdirecting or misinforming them with respect to their correct polling station, or calls they described as rude, harassing or annoying, received at an inopportune time of day or on multiple occasions. This includes 252 complainants from the electoral district of Guelph. The investigation is ongoing, and at the time the report went to press, no charges had been laid.

2. Legal Context

In order to understand the implications of the deceptive calls made during the 41st general election and the need for legislative reform, it is necessary to provide, in summary fashion, an overview of the rules that currently apply – or do not apply, as the case may be – to such conduct. This part of the report sets out relevant parts of the *Canada Elections Act*, indicates that the main pieces of federal privacy legislation do not apply to political parties, and explains how provisions of the *Telecommunications Act* and a number of the Unsolicited Telecommunications Rules of the Canadian Radio-television and Telecommunications Commission (CRTC) dealing with telemarketing or automated calls do apply to political entities. Finally, it refers to certain offences set out in the *Criminal Code*.

A. *Canada Elections Act*

Communications with electors by political entities are essential to the democratic process. For political parties and candidates, the purpose of an election campaign is to convince electors to vote and to vote for a particular candidate. This is done through a number of means, and for many, the direct contact between candidates or their team and the elector remains an essential component of the campaign.

To facilitate these communications, Parliament has included a number of provisions in the Act requiring the transmittal of elector information to parties, candidates or members of Parliament through lists of electors (sections 93, 104.1, 107, 109 and 45). These lists contain the name, addresses (mailing and civic) and numerical identifier of each elector.[7] They do not contain elector telephone numbers.

The Act imposes no obligations on the recipients of the lists with respect to protecting and controlling access to the personal information they contain. Nevertheless, Elections Canada provides administrative guidelines that include best practices to protect the personal information found on the lists. However, these guidelines are not enforceable.

Elections Canada has limited information on how this and other personal information is managed by political parties. There is little public knowledge about the manner in which the information is collected, the sources of the information, whether the information is shared and with whom, the purposes for which it is used, and whether there are measures put in place by the parties to control or limit the use made of this information. The agency understands that there are a number of commercial software packages on the market that allow political parties to more easily merge

[7] Four of these lists are given to candidates and parties during the election period (the preliminary lists, the updated preliminary lists, the revised lists and the official lists). The final lists, produced after the election, are given to registered parties that endorsed candidates in the electoral districts and to members of Parliament for their respective districts. Members of Parliament also receive an annual copy of the lists of electors for their respective districts, as do parties that request one, provided they endorsed a candidate in that district in the last election.

information contained on the lists of electors with their own information on electors. These databases may contain a significant amount of additional information, including telephone number and vote preference, if known.[8] Elections Canada also understands that, in certain cases, local campaigns and the parties to which they are affiliated share the elector information in the party's database to increase the information available to both entities for that electoral district. The primary purpose of parties' use of these databases is to build a record of their supporters (and of their non-supporters) to facilitate communication with electors during campaigns, for example, to get the vote out.[9]

The evolution of new technologies and their increased use by participants in the electoral process have allowed participants to target segments of the electorate and reach out to electors more easily and more efficiently. This is done through an expanding range of mechanisms, including live or automated calls and interactive telephone town halls, all of which allow parties and candidates to pass on their message and foster participation.

The tools to do so are not expensive and are relatively easy to use. For this reason, they present significant benefits to the electoral process. However, these very qualities, combined with the capability of some of these tools to hide the true source of the communication, also make them key instruments for those who want to deceive electors.

Deceptive practices[10] involving the use of "robocalls" or websites have emerged in the United States over the last decade. For example, in 2006, in Kansas City and Virginia, electors received automated phone calls falsely informing them of changes in polling location.[11] Apart from interfering with the constitutional rights of electors, such practices potentially erode the trust of electors as well as the capacity of political parties and candidates to effectively communicate with electors and stimulate voter participation.

What can and cannot be done by parties and candidates in communications with individual electors

Under the Act (section 110, paragraph 111(*f*)), the primary constraint on the use of personal information contained on the lists of electors by parties, candidates and members of Parliament is that the personal information they contain not be *knowingly* used for a purpose other than: (a) communicating with electors, or (b) a federal election or referendum. Under this prohibition, not

[8] See Colin J. Bennett and Robin M. Bayley, *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis* (Ottawa: Office of the Privacy Commissioner of Canada, 2012), pp. 16, 34ff. www.priv.gc.ca/information/pub/pp_201203_e.asp.

[9] Id., p. 16.

[10] The expression "deceptive practices" is used in this report rather than the (in some respects) narrower concept of "voter suppression" commonly found in the literature. Voter suppression is defined in the US Department of Justice manual for the prosecution of election offences as follows: "Voter suppression schemes are designed to ensure the election of a favored candidate by blocking or impeding voters believed to oppose that candidate from getting to the polls to cast their ballots. Examples include providing false information to the public – or a particular segment of the public – regarding the qualifications to vote, the consequences of voting in connection with citizenship status, the dates or qualifications for absentee voting, the date of an election, the hours for voting, or the correct voting precinct.... Currently there is no federal criminal statute that expressly prohibits this sort of voter suppression activity." See Craig C. Donsanto, *Federal Prosecution of Election Offenses*, 7th ed. (Dept. of Justice, 2007), p. 61. Elections Canada prefers the use of the term "deceptive practices", which is broader and also includes impersonation of political opponents that is not aimed at suppressing the vote but which distorts the electoral process.

[11] See Common Cause, Lawyers' Committee for Civil Rights Under Law and Century Foundation, *Deceptive Practices 2.0: Legal and Policy Responses* (Washington: Common Cause, 2008).

only must the misuse be demonstrated, but also the person's knowledge of the source of the information and its use.[12]

Communications with electors may be and are done through many means, including door-to-door canvassing and other forms of voter contact. Election advertising – that is, the transmission to the public during an election period of an advertising message promoting or opposing a candidate or party, or a position with which they are associated[13] – is permitted, subject to the requirement that it include a mention in or on the message that its transmission was authorized by the official agent of the candidate or by the registered agent of the party.[14] Get-out-the-vote calls are also authorized communications.

However, wilfully preventing or trying to prevent an elector from voting is prohibited.[15] Similarly, inducing a person to refrain from voting (or to vote for or against a particular candidate) by "any pretence or contrivance" is prohibited.[16] Finally, knowingly making or publishing a false statement of fact in relation to the personal character or conduct of a candidate or prospective candidate with the intention of affecting the result of the election is also prohibited.[17]

These prohibitions are drafted fairly broadly. The prohibitions found in paragraphs 281(*g*) and 482(*b*) are not tied to a particular technology or means of interference. Paragraph 482(*b*) would capture both tricks used to deceive electors in their vote preference (e.g. by falsely pretending to call on behalf of another candidate) as well as tricks to suppress the vote (e.g. by falsely informing electors that their polling location has changed).

However, these prohibitions are backed with sanctions enforceable in the criminal courts and not administrative penalties. As a result, non-compliance can only be dealt with through investigations for which the outcome may be a penal process. As discussed further in this report, the limited tools available to obtain information translate into usually lengthy and stringent procedures. There is also a significant imbalance between these lengthy and stringent procedures and the small fines that may currently be imposed by the courts following a conviction, thus limiting the deterrent effect of such a finding.

Communications with electors regarding polling locations

Each electoral district is divided into a number of geographic parcels called polling divisions, with a division comprising at least 250 electors. Generally, there is one polling station for every polling division. The basic rule is that a polling station should be located in the polling division. However, if the returning officer considers it advisable, several polling stations may be placed together in a central polling place. In practice, most polling stations are grouped in this manner.

---

[12] The *Canada Elections Act* does not address the collection or disclosure of personal information by political entities. The need to prove that the person who used the information knew that it came from the lists of electors (as opposed to another source) reduces the likelihood of a successful enforcement action. This may limit mechanisms to reinforce accountability with regard to the protection and use of the personal information contained on the lists.

[13] *Canada Elections Act*, s. 319.

[14] Id., s. 320.

[15] Id., para. 281(*g*); offence at para. 491(3)(*d*).

[16] Id., para. 482(*b*).

[17] Id., s. 91; offence at para. 486(3)(*c*).

Before each election, returning officers are tasked with identifying polling sites in the polling divisions, or sites in which a central polling place may be established. Central polling places may group together a maximum of 15 polling stations. Where feasible, polls should be in a public building that is centrally located in proximity to the electors they serve, and that meets specific accessibility standards both inside and outside the building.[18] While returning officers may have preliminary discussions with landlords for the rental of the premises, they may not enter into a lease prior to the issue of the writs unless authorized to do so by the Chief Electoral Officer, usually not before the election is imminent.

A voter information card (VIC) is sent by the returning officer to all registered electors in the electoral district. The VIC indicates the address of the elector's polling station as well as voting dates, voting hours and a telephone number to call for further information.[19] If it is necessary to change the location of a polling station – for example, because of the sudden unavailability of a polling site – the returning officer prints and sends amended VICs to affected electors. If the change occurs too late in the election calendar to proceed in this fashion,[20] electors are informed through media broadcasts and personally by an election worker posted at the entrance of the closed or changed polling station.

Candidates are directly informed of the location of polling sites and of any changes to these locations because the Act authorizes them or their representatives to be present at polling stations and at the counting of the votes.[21] This information is also posted on the Elections Canada website. Following the request of a party during the 41st general election, polling site information was shared with all political parties as well, with the specific instruction that it not be used by parties to inform voters of their voting location.[22] Given the static nature of the information provided to parties and the risk of confusion, in the future, Elections Canada will resume its practice of providing this information directly to candidates only, and not to political parties.

Elections Canada does not call electors to advise them of changes in polling sites. Subject to a few exceptions, the agency does not have the telephone numbers of electors.[23] Even in the few cases where electors provide their telephone number voluntarily, this personal information is not captured in the National Register of Electors or on the lists of electors and it is not available to returning officers.

---

[18] On polling day, May 2, 2011, there were 64,477 polling stations located in 15,260 polling sites. In addition, 1,669 mobile polls were set up in 4,865 establishments.

[19] *Canada Elections Act*, s. 95.

[20] Id., s. 102. The *Report on the Evaluations of the 41st General Election of May 2, 2011*, published by Elections Canada, indicates that in total, 326 ordinary polling stations (0.5%) and 38 advance polling stations (0.8%) were reassigned to another site. Of the 326 ordinary polling stations reassigned to a new polling site after the VICs were mailed, there was enough time to mail a revised VIC to electors for 274 of them. The remaining 52 polling stations, representing approximately 19,000 electors, were reassigned less than six days before election day. This situation occurred in 26 electoral districts.

[21] *Canada Elections Act*, ss. 135–140, 283–291.

[22] In April 2011, following a request received from a party, Elections Canada sent a dataset of all polling sites to be used for the 41st general election to all political parties. The message covering the dataset indicated that polling locations may change. As a result, it asked parties to ensure that users of the dataset respect the following restrictions: that the dataset be used for internal purposes only; that it not be used to inform voters of their voting location, via mail-outs or other forms of communications; and that it not be shared with any other organization.

[23] For example, electors have the option of providing their telephone number when they apply for special ballots in order for Elections Canada to contact them if their faxed documents are illegible.

Other Elections Canada communications with electors during the election period

While Elections Canada does not communicate with electors individually except through the VIC, it does launch an extensive multi-platform campaign to provide electors with all the information they need on registration, the various voting options, and voter identification requirements so they can vote during an election.

The campaign includes a number of communication vehicles, such as advertisements on television, in newspapers, on the radio, on billboards in public places and on popular social media websites. Advertising is complemented with the mailing of VICs to all registered electors and a reminder brochure to all Canadian households, a comprehensive website and public enquiries services, as well as a network of community relations officers across the country who work with specific target groups of electors – namely, youth, Aboriginal and ethnocultural communities, homeless electors and seniors – to raise awareness about the electoral process.

Contested elections

The fact that the election was contested in a number of electoral districts as a result of alleged fraudulent communications warrants a few explanations about the legislative framework for contesting elections under Part 20 of the Act. Unlike a judicial recount – which merely serves to verify that the results that were validated by the returning officer properly reflect the preferences expressed on the ballots – a contested election puts into question the validity of the election. An election may be contested on the basis that the winning candidate was not eligible to be a candidate, or that there were irregularities, fraud or corrupt or illegal practices that affected the result of the election (section 524).

Where it has been established that the winning candidate was ineligible to be a candidate, the court hearing the application must declare the election null and void. However, where it has been established that the result of the election was affected by irregularities, fraud or corrupt or illegal practices, the court may annul the election, but is not bound to do so (section 531). In exercising its discretion under subsection 531(2) to annul or not annul an election, a court must consider whether the irregularities (or fraud, or corrupt or illegal practices) raised doubts about the winner *or* whether the integrity of the electoral process would be called into question.[24]

B. Other relevant legislation

Privacy Act and *Personal Information Protection and Electronic Documents Act*

The *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) set out the general principles governing the collection, use, disclosure and retention of personal information. These principles reflect internationally recognized standards.[25]

[24] *Opitz v. Wrzesnewskyj*, [2012] S.C.C. 55, para. 23.

[25] These principles are set out in Schedule 1 of PIPEDA and have been reproduced in the annex to this report.

However, neither the *Privacy Act* nor PIPEDA generally applies to political entities. The *Privacy Act* applies only to federal institutions – that is, departments and agencies of the federal government. With respect to PIPEDA, its scope is limited to personal information collected, used or disclosed in the course of commercial activities.[26]

The absence of a legal framework governing how personal information is managed and protected by political parties and candidates is a matter of significance, considering that the intelligence compiled and accessed by political parties on the composition of the electorate is likely a key factor in the attraction to the use of devices such as robocalls to deceive targeted segments of the electorate.

The recent report sponsored by the Privacy Commissioner on federal political parties and the protection of personal information points out that the information collected by political parties concerns many individuals, including party volunteers and employees, donors to the parties, as well as registered electors whose personal information they receive from Elections Canada and from a variety of other sources.[27]

The authors hold the view that there are privacy risks associated with these databases. Parties not only handle large amounts of personal information, but also share this information with a small army of volunteers and local campaign workers. As indicated in the report:

> 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.[28]

As the authors point out, "[b]eyond 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."[29]

The report describes various incidents occurring over the last few years that put the personal information of certain electors at risk, including a reference to "potential vote suppression in key ridings through the practice of 'robocalling'" in the last federal election.[30]

In that context, a survey of 1,011 electors conducted by Phoenix Strategic Perspectives Inc. for Elections Canada in November and December 2012 indicates that nearly two thirds (65%) of those surveyed were of the view that political parties and candidates should be regulated by privacy laws when interacting with electors during an election period.[31] Canadians are receptive to political parties and candidates contacting them during a federal election to encourage them to vote or to inform them of their policies. It is worth noting that many of them think it is

---

[26] The Bennett and Bayley report, mentioned *supra* at footnote 8, indicates that British Columbia's *Personal Information Protection Act* has a broad definition of "organization" and does not limit its application to commercial activities. It has been held to cover British Columbia's political parties and may also cover the activities of federal political parties in that province. See www.priv.gc.ca/information/pub/pp_201203_e.pdf, p. 26.

[27] Id., p. 19.

[28] Id., p. 22.

[29] Id., p. 24.

[30] Id.

[31] Phoenix Strategic Perspectives, *Survey of Electors on Communications with Electors*, March 2013, p. 10.

appropriate for parties or candidates to provide them with information on where and when to vote.[32] However, the majority of electors do not believe that it is important for political parties to collect personal information on electors.[33]

The panel of experts consulted by Elections Canada also recognized the need for parties to be able to engage individual Canadians, and while they agreed that the use of and control over the personal information held by political parties should be regulated, some suggested that the approach to doing this should not be as restrictive as that applicable to commercial activities.[34]

Canadian Radio-television and Telecommunications Commission's Unsolicited Telecommunications Rules[35]

Section 41 of the *Telecommunications Act* allows the CRTC to regulate unsolicited telecommunications "to the extent that the Commission considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression."[36] Relying on the authority of the *Telecommunications Act*, the CRTC has adopted the National Do Not Call List (DNCL) which allows consumers to register a telephone number to avoid receiving telemarketing communications at that number.

While the National DNCL Rules do not apply to a telecommunication made by or on behalf of political entities governed by the *Canada Elections Act*[37] – that is, registered parties, candidates, nomination contestants, leadership contestants and electoral district associations – the *Telecommunications Act* requires exempted individuals and organizations, such as political parties and candidates, to maintain their own internal DNCL.[38] Political parties and candidates must ensure that no telecommunication is made on their behalf to any person who has requested to be on their internal DNCL.[39]

Political entities governed by the *Canada Elections Act* are also bound by the CRTC's Telemarketing Rules, as well as the Automatic Dialing-Announcing Device (ADAD) Rules.

Telemarketing Rules

The Telemarketing Rules made pursuant to section 41 of the *Telecommunications Act* apply whether or not the telemarketing telecommunication is exempt from the National DNCL Rules. Therefore, the rules apply to political entities.

---

[32] Id., p. 5.

[33] Id., p. 7.

[34] IRPP, *Issues Arising from Improper Communications with Electors – Roundtable Report*, March 2013, p. 7.

[35] This section is Elections Canada's attempt to summarize the CRTC rules. The rules themselves can be found on the CRTC's website at http://crtc.gc.ca/eng/trules-reglest.htm. Also of interest is a fact sheet entitled "Key facts on the telemarketing rules for political candidates, parties and organizations," found at http://crtc.gc.ca/eng/info_sht/t1041.htm. For further information regarding the Unsolicited Telecommunications Rules, please contact the CRTC.

[36] While the rules adopted by the CRTC are in many ways quite comprehensive, they do not apply to the Internet or e-mail communications. In December 2010, Parliament adopted anti-spam legislation (see S.C. 2010, c. 23). As a result, once the legislation comes into force, the mandate of the CRTC will be expanded to include commercial electronic messages.

[37] See paragraphs 41.7(1)(*c*) to (*e*) of the *Telecommunications Act*.

[38] Id., s. 41.7(4).

[39] However, one may call a person who has asked to be put on the internal do not call list of an organization if the telecommunication is for the sole purpose of collecting information for a survey of members of the public.

"Telemarketing" is defined in the Rules as the use of telecommunications facilities to make unsolicited telecommunications for the purpose of solicitation; and "solicitation" means the selling or promoting of a product or service or the soliciting of money or money's worth. Therefore, the Telemarketing Rules apply to political entities when soliciting donations, but not when they are asking for the electors' support at the polls. Nor would the rules apply to get-out-the-vote calls.

The Telemarketing Rules provide for:

- Prior registration of a telemarketer making calls on its own behalf and of a telemarketer's client on whose behalf the calls are made.
- Maintenance of an internal DNCL by a telemarketer acting on its own behalf or by a client of a telemarketer.
- Adding a consumer's name and number to the internal DNCL within 31 days of the consumer's do not call request.[40]
- At the beginning of a voice telemarketing telecommunication, providing the name or fictitious name of the individual making the call, the name of the telemarketer and the name of the client.
- Upon request during a voice telemarketing telecommunication, providing a voice telecommunications number that allows access to an employee or other representative of the telemarketer and of the client. The name and address of an employee or other representative must also be given upon request.
- Restricting telemarketing telecommunications to certain hours of the day (9 a.m. to 9:30 p.m. on weekdays and 10 a.m. to 6 p.m. on weekends).[41]
- The telemarketer displaying the originating phone number or an alternate number where the telemarketer can be reached.

Automatic Dialing-Announcing Device Rules

It is important to note that the ADAD Rules, also made pursuant to section 41 of the *Telecommunications Act*, apply whether or not the telemarketing telecommunication is exempt from the National DNCL Rules. Therefore, they apply to political entities.

An ADAD is defined in the Unsolicited Telecommunications Rules as "any automatic equipment incorporating the capability of storing or producing telecommunications numbers used alone or in conjunction with other equipment to convey a pre-recorded or synthesized voice message to a telecommunications number". It produces what are sometimes referred to as robocalls.

[40] This issue is dealt with in the CRTC fact sheet mentioned *supra* at footnote 35. It indicates that "[a] constituent's request to have their name and phone number added to the internal do not call list of a party or candidate, or those making calls on their behalf, must be honoured at the time of the call. Callers must update their internal do not call list within 31 days."

[41] These hours are subject to provincial legislation governing this type of activity. The Phoenix survey of electors referred to *supra* at footnote 31 indicates that 40% of electors prefer to be contacted between 5 p.m. and 9 p.m. (p. 3).

A person using an ADAD to make unsolicited communications where there is no solicitation must nevertheless comply with a number of conditions. The most relevant conditions for the purposes of this report are the following:

- There are restrictions on the hours during which such telecommunications can be made (9 a.m. to 9:30 p.m. on weekdays and 10 a.m. to 6 p.m. on weekends).[42]
- The call must begin with a clear message identifying the person on whose behalf the telecommunication is made. This message must include a mailing address and a local or toll-free telecommunications number at which a representative of that person can be reached. If the actual message relayed is longer than 60 seconds, the identification message must be repeated at the end of the telecommunication.
- The telecommunication must display the originating telecommunications number or an alternate telecommunications number where the telecommunication originator can be reached.

Enforcement of the Unsolicited Telecommunications Provisions by the Canadian Radio-television and Telecommunications Commission

The regime provides for administrative monetary penalties as the main enforcement tool (see sections 72.01 to 72.15 of the *Telecommunications Act*). Because such penalties are imposed directly by the CRTC and not under a criminal court process, and therefore are not accompanied by the full panoply of rights and protections granted to suspects and those accused of offences prosecuted in criminal court, they can be imposed with speed and efficiency by the CRTC.

The CRTC's investigative powers regarding a violation of the provisions on unsolicited telecommunications are found at sections 72.05 and 72.06 of the statute. A person designated by the Commission to issue notices of violation may enter and inspect, at any reasonable time, any place in which he or she believes on reasonable grounds there is any document or information relevant to the enforcement of the rules. That individual may also use or cause to be made use of any data processing system at that place to examine any data contained in or available to the system, and the records contained in the system may be copied or reproduced.

A person authorized to issue notices of violation may also require that anyone whom he or she believes is in possession of information necessary for the administration of the Unsolicited Telecommunications Rules submit information to him or her in the manner that he or she specifies.

It is worth noting that in recent amendments to its *Election Act*,[43] the Alberta legislature has imposed its own requirements on advertisements transmitted to a telephone, whether in the form of a live call or an automated pre-recorded call. It requires that the telephone number of the sponsor be capable of being displayed on the call display of persons called; that the name of the sponsor and the sponsor's party affiliation be stated at the beginning of the advertisement; that the advertisement state whether the sponsor has authorized the advertisement; and that the

[42] These hours are subject to provincial legislation governing this type of activity.

[43] *Election Accountability Amendment Act, 2012*, S.A. 2012, c. 5, assented to December 10, 2012. Section 46 of that Act amends section 134 of the Alberta *Election Act*.

telephone number of the sponsor or the sponsor's campaign office at which the sponsor may be contacted be stated at the end of the advertisement. As a result of other amendments to the *Election Act*, Alberta's Chief Electoral Officer may impose an administrative penalty or serve a letter of reprimand on any person that has contravened a provision of the Act, including those above.[44]

Criminal Code restrictions on fraudulent communications

Current provisions of the *Criminal Code* appear to be of limited assistance in dealing with deceptive communications with electors.

Harassing or misleading phone calls (subsections 372(1), (3))

It is an offence to convey, by telephone, information known to be false "with intent to injure or alarm any person" (subsection 372(1)). It is unclear whether a court would consider that affecting an opponent's chances of success in the election (as opposed to injuring the opponent himself or herself) constitutes an injury under this section.

It is also an offence to "mak[e] or caus[e] to be made repeated telephone calls" with "intent to harass" the person receiving the calls (subsection 372(3)).

Personation (section 403)

It is an offence to fraudulently personate another person, living or dead, with intent to achieve any of four specified purposes, including "to cause disadvantage to ... another person". The jurisprudence confirms that the personation must be of a real person. The offence would not be applicable to a call or caller represented as "Elections Canada", nor to a fictitious character such as Pierre Poutine.

Mischief (section 430, subsection 430(1.1))

Section 430 lists activities in relation to "property" (as defined) that constitute the offence of "mischief". Subsection 430(1.1) creates mischief offences for destroying, altering or interfering with the use of "data" as defined in section 342.1 (that is, "representations of information ... suitable for use in a computer system"). These provisions do not appear to apply to the calls per se.

[44] Id., section 54 adding new section 153.1 to the Alberta *Election Act*. Under this new authority, Alberta's Chief Electoral Officer must be of the opinion that a person has contravened a provision of the Act before serving on the person a notice of administrative penalty or a letter of reprimand. The notice of penalty must set out, among other things, the particulars of the contravention, the amount of the penalty and the date by which it must be paid, and a statement of the right to appeal the imposition or the amount of the penalty to the Court of Queen's Bench. The following factors must be considered by Alberta's Chief Electoral Officer in determining the amount of the penalty to be paid or whether to issue a letter of reprimand: the severity of the contravention, the degree of wilfulness or negligence, whether there are mitigating factors, whether steps have been taken to prevent reoccurrence of the contravention, whether the person has a history of non-compliance, whether the person reported the contravention on discovering it had occurred, and any other relevant factor. The amount of the penalty may not exceed the maximum fine that could be imposed for the corresponding offence. If the penalty is not paid within the time frame set out in the notice, Alberta's Chief Electoral Officer may file a copy of the notice with the Court of Queen's Bench and on being filed, the notice has the same force and effect as a judgment of that court and may be enforced as if it were a judgment of the court.

3. Investigation Challenges

In order to understand the rationale for the recommendations made in this report, particularly those involving legislative changes, it is essential to provide an overview of some of the challenges faced by Elections Canada's investigators in their search for the source of the improper calls made during the last general election. Some of these challenges are unavoidable, especially as regards the current state of the technology. Others are reported more to give an idea of the complexity of the investigation and the inherent delays in obtaining the evidence required to take enforcement measures than for the purpose of changing the regime. Still, a number of improvements to the legislative framework could be made to facilitate the investigative process.

A. Lack of contractual information on local and national campaigns

Current limits to the degree of mandatory reporting to Elections Canada

The data contained in the election expenses returns filed by political parties is currently very limited and does not include specific information, such as contracted communications or telemarketing services, that could provide guidance to an investigation. While party returns include details on the contributions received, parties' election expenses are grouped into broad categories, and the return provides no or little breakdown about how these expenses were incurred. This is something Elections Canada intends to remedy before the next general election. More importantly, however, under current legislation, federal political parties are not required to submit any supporting document in relation to their expenses, nor can such documentation be requested of them.[45]

By comparison, candidates' returns and accompanying documentation are more complete and may show that a telemarketing firm was retained for making calls to electors. However, the purpose for which the firm was retained and the text of the messages communicated to electors is not available as part of the return since the reporting of this information is not required under the *Canada Elections Act*.[46] Moreover, as candidates' campaign returns need not be filed until four months after polling day (section 451), any information contained in the returns regarding arrangements with service providers may arrive too late to be of any significant assistance to an investigation.

[45] In the 2010 recommendations report, the Chief Electoral Officer recommended that he or she be able to request that registered political parties provide any documents and information that may, in the Chief Electoral Officer's opinion, be necessary for verifying that the party and its chief agent have complied with the requirements of the Act with respect to the election expenses return. See *Responding to Changing Needs – Recommendations from the Chief Electoral Officer of Canada Following the 40th General Election*, recommendation II.1.

[46] The Act allows the Chief Electoral Officer to request additional documentation in support of the expense. As a general rule, the contents of an advertisement are not relevant for that purpose.

The cases Elections Canada has investigated seem to indicate that major parties deal with their own stable of telemarketing firms. Candidates' campaigns gain access to these firms through referrals by the party. However, while invoices from the party may be submitted with the candidates' campaign returns, the Act does not require that these returns also include the original contracts entered into with telemarketing firms regarding the services to be provided by the firms, when and at what cost. As such, little if anything is known from the returns about the specific services rendered by telemarketing firms, to either political parties or candidates.

B. Technological means to prevent traceability or identification

Current technology offers several ways by which persons who do not want to comply with the rules can escape detection. This means that, even where there are applicable legislative or regulatory requirements such as the CRTC's Unsolicited Telecommunications Rules, these requirements can in practice be evaded using various technological means of anonymity. The solution to these problems may be more in the advancement of technology than in the introduction of new rules.

Voice over Internet Protocol technology

The current state of the technology allows callers to hide the origin of a call by causing a fake number to appear on the recipient's call display ("spoofing"). This limits the ability for VoIP calls to be traced back to the caller. The technology has so evolved that it is possible to set up a VoIP call centre from almost anywhere, including a home, with a newer computer, some servers and access to call lists.[47]

Proxy servers

Anonymity can also be facilitated through the use of proxy servers that function as an intermediary between the originator of a message and its intended destination when communicating over the Internet. Proxy servers are websites that provide anonymity by appearing as the originating communicator when communicating with the intended destination. In the investigation of the Guelph matter, court documents filed by the Commissioner of Canada Elections indicate that the information regarding the true originator was kept by the proxy server for only a short period of time, thus allowing the originator to communicate anonymously with the voice broadcasting vendor.

Disposable cell phones

Disposable cell phones can be used to prevent the identification of a caller. There are also applications that allow cell phone users to create temporary telephone numbers that can be used, both for calls and text messaging, without leaving a trace. In the Guelph investigation, court documents filed by the Commissioner indicate that a disposable cell phone was used to communicate with a voice broadcasting vendor under a false identity.

[47] However, it should be noted that the system used in the case of Guelph was that of an existing, known voice broadcasting vendor that kept its own records of calls made and has co-operated with investigators.

C. Limitations with *Criminal Code* means of obtaining information

Threshold to be met to obtain a production order

The *Criminal Code* allows investigators to obtain a search warrant or a production order from a judge to compel individuals or entities to provide or produce certain documents or data in their possession to the investigator. Production orders are used as a less intrusive alternative to search warrants, under appropriate circumstances. Under subsection 487.012(3), the order will not be granted unless the informant (in Elections Canada's case, the investigator) can show that he or she has reasonable grounds to believe that an offence has been committed. The informant must also have reasonable grounds to believe that the documents or data sought will provide evidence respecting the commission of the offence, and that the person who is the subject of the order has possession or control of the documents or data. Thus, an investigation must have made significant progress and solid evidence must exist before a production order can be sought from the courts.

Lack of industry standards in the data retention policies of telecommunications companies

There are no industry standards on the type of telecommunications records to be kept, nor on their retention time. Some companies keep no records on telecommunications unless billing is required. Others keep records on all telecommunications made by users (e.g. date the call was made, duration, recipient's telephone number). Some keep this information for only a few days, others for three months or longer. The length of time for which data is retained directly impacts the ability to obtain information during the investigation.

The drafting of the supporting information (called an Information to Obtain, or "ITO") required to convince a judge to issue a production order, the issuance of the requested order by the judge and the waiting for the actual production of the documents by their holder may take weeks or months, depending on the progress of the investigation and the complexity of the matter. As well, it is often necessary to go through the process of drafting an ITO, obtaining an order and receiving documents in response a number of times to pursue a given trail. That said, the chain of events and communications leading to a robocall may be very difficult, if not impossible, to establish where a company retains telecommunications records only for a very short period.

Inability to compel testimony

Individuals who are not suspected of wrongdoing often have relevant information that could assist in determining whether the *Canada Elections Act* has been contravened and shed light on the circumstances of the contravention. Often, their collaboration is critical at the early stages of an investigation. However, experience demonstrates that, for a number of reasons, these individuals may refuse to collaborate with investigators, or they may only agree to do so after considerable efforts and delays that may result in the loss of key evidence.

For example, in the case of the Guelph investigation into misleading robocalls, the publicly available court records show that at least three individuals believed to have key information refused to speak with investigators. The inability to compel testimony has been one of the most significant obstacles to effective enforcement of the Act.

4. Recommendations

The following measures and recommendations are aimed at better addressing the risks posed by deceptive tactics to Canada's electoral democracy. Some of the measures proposed here are administrative in nature and can be implemented by Elections Canada. Most recommendations, however, require legislative changes.

Both the measures and the recommendations are based on the view that, first and foremost, the focus must be on preventing this kind of conduct from occurring. In making the recommendations, Elections Canada is also mindful of the importance of limiting, to the extent possible, the regulatory burden imposed on political entities. At the same time, however, Canadians, political parties and candidates expect Elections Canada to be able to intervene promptly and effectively in investigating potential abuses of the electoral process. The ability to do so is essential to preserving confidence in electoral democracy and can only be achieved with the appropriate legislative tools.

A. Prevention measures and recommendations

Public information on the electoral process

> In order to better inform the public, Elections Canada will ensure that advertising campaigns in the next election include clear messaging on its procedures when polling sites are changed very late in the election period.

As indicated earlier, Elections Canada is responsible for managing polling locations and ensuring that changes are communicated to electors. This communication is done through the mailing of new voter information cards or, if it is too late for such a mailing, through public announcements in the media and the posting of an election worker at the door of the old polling site.

Evidence suggests that Canadians do not understand the respective roles of Elections Canada and political parties in providing information about where and how they can vote. Indeed, 64% of electors thought it appropriate for political parties and candidates to provide them with this information.[48] The responsibility of Elections Canada as regards the voting process needs to be clarified. Means must also be taken to reduce the risk of electors being given inaccurate information by candidates or parties, or worse, being deceived by callers impersonating Elections Canada officials. In preparing for the next election, the agency will therefore foster greater public awareness of its procedures (in particular, the fact that the agency does not communicate with electors by telephone), as well as develop means to warn electors about misleading calls and inform them of available remedies, including how to file a complaint with Elections Canada or with the CRTC, depending on the nature of the call.

[48] Phoenix, Survey of Electors, p. 5.

In order to better inform political entities, Elections Canada will collaborate with other government agencies, such as the Canadian Radio-television and Telecommunications Commission, to draw attention to certain rules applicable during election campaigns.

In discussions with members of the Advisory Committee of Political Parties, many have told Elections Canada that they were not sufficiently informed of or did not fully understand the CRTC rules governing unsolicited telecommunications. Officials within the CRTC have already informally indicated a willingness to better communicate and explain these rules to political entities. Elections Canada will work with the CRTC in this endeavour.

A code of conduct for political entities

In order to increase electors' confidence in the electoral process and in political parties, consideration should be given to the development of codes of conduct applicable to political parties, their officials, candidates, other affiliated entities such as electoral district associations, and active supporters. These codes would be developed by the parties, with Elections Canada's assistance if required.

Another means of increasing Canadian electors' confidence in the political process and political parties (particularly as regards political entities' use of their personal information), which garnered a broad consensus from the panel of experts consulted by Elections Canada, is the development of a code of ethics or code of conduct[49] for political parties – one to which they would either voluntarily adhere or that could be mandated through legislation.

In its 1991 report, the Royal Commission on Electoral Reform and Party Financing ("the Lortie Commission") strongly recommended that parties adopt codes of ethics as a remedy to the concern that "where incidents or allegations of misbehaviour arise, parties have been reluctant to assume responsibility for reviewing and revising the practices that gave rise to the allegations."[50] As stated by the Lortie Commission, "[a] code of ethics would establish an important organizational instrument of party governance, giving party executives and leadership a tool to manage and give coherence to the behaviour, practices and standards of the party."[51] It also expressed the view that

> [c]rystallizing the party's basic values and principles in a code of ethics would be particularly valuable to party members who make difficult decisions in the competitive environment of electoral campaigns. It would enhance the incentive and inclination of party members to put the party's long-term interest in protecting its integrity and public respect ahead of potential and illusive short-term gains.[52]

[49] While in certain fields distinctions are made between a code of ethics and a code of conduct, for the purpose of this report, the two terms are used interchangeably unless referring to specific codes.

[50] Canada, Royal Commission on Electoral Reform and Party Financing, *Reforming Electoral Democracy*, vol. 1 (Ottawa: Communication Group, 1991) (Chair: Pierre Lortie), p. 285.

[51] Id., p. 286.

[52] Id., p. 287.

For the Commission, "[a] code of ethics would help reconcile public demands for greater regulation with the legitimate desire of parties to manage their internal affairs."[53] It also insisted on the need for parties to enforce their own codes and suggested the setting up of an ethics committee to ensure compliance.[54]

While the Lortie Commission suggested that each party have and administer its own code of ethics, Elections Canada's research also provided examples of codes of ethics or conduct to which all parties within a particular jurisdiction adhere (or by which they are bound).

The organization International IDEA, the International Institute for Democracy and Electoral Assistance,[55] proposes a model voluntary code of conduct setting out "rules of behaviour for political parties and their supporters relating to their participation in an election process".[56]

Even though authors generally see voluntary codes as the best solution,[57] codes of conduct may be developed in a number of ways and may be quite different in nature. They may be agreed on by the parties, or agreed on by the parties and then given legal status; they may be legislated, or they may be determined by the electoral management body pursuant to a regulatory authority.[58]

It is a common view among authors and in the codes reviewed that a code should be applicable to the party itself and, through the control of each party, to its leader, officials, candidates and members. To the extent possible, a party should be responsible for the activities of its supporters. It should also be responsible for violations of the code by its supporters.[59]

While codes of conduct for political parties have been adopted mainly in emerging democracies,[60] an example of such a code has existed in Manitoba for the last decade.[61]

---

[53] Id., p. 288.

[54] Id., p. 289.

[55] International IDEA is an intergovernmental organization. Its programs aim to provide knowledge to democracy builders, provide policy development and analysis, and support democratic reform.

[56] International IDEA, *Code of Conduct for Political Parties – Campaigning in Democratic Elections*, www.idea.int/publications/coc_campaigning/loader.cfm?csmodule=security/getfile&pageid=2401, 1999, p. 7. A study prepared for the Inter-Parliamentary Union (of which Canada is a member) by Guy S. Goodwin-Gill also proposes a model code directed at political entities. See *Codes of Conduct for Elections: A Study Prepared for the Inter-Parliamentary Union*, www.ipu.org/PDF/publications/CODES_E.pdf, 1998, at p. 59ff.

[57] International IDEA, *Code of Conduct for Political Parties – Campaigning in Democratic Elections*, pp. 8–9.

[58] Id., p. 6.

[59] Id., p. 10. See also Goodwin-Gill's study at pp. 64 and 67.

[60] See the launch of Ghana's *Political Parties Code of Conduct* for the 2012 elections, www.modernghana.com/news/366561/1/political-parties-code-of-conduct-for-2012-launche.html; see also Zambia's code of conduct issued and administered by the Electoral Commission, www.elections.org.zm/media/electoral_code_of_conduct_2011.pdf. Political parties in a number of countries in Africa have adopted similar codes, with the support and encouragement of the Electoral Institute for Sustainable Democracy in Africa (EISA). See www.eisa.org.za/WEP/comcode.htm. India's Election Commission has also published a model code of conduct for the guidance of political parties. See http://eci.nic.in/eci_main/faq/faq_mcc.pdf.

[61] See Manitoba's *Shared Code of Ethical Conduct* at www.electionsmanitoba.ca/en/Political_Participation/Shared_Ethical_Code_of_Conduct.html. It was developed as a result of a recommendation contained in the 1999 report of a commission of inquiry that looked into allegations of offences under the province's *Elections Act* and *Elections Finances Act* during Manitoba's 1995 general election. The code, which applies to all political parties and candidates, provides guiding principles and rules of conduct. Respect for the law by all those to which the code applies is emphasized, as well as the need for political entities to uphold the integrity of the political process. The code is administered by each political party.

In the federal sphere, this code (or codes) could be developed in collaboration with parties and, as is the case in all jurisdictions where such codes exist, bind not only the parties but also their officials, candidates, other entities and active supporters.

B. Recommendations to improve compliance

Extension of the application of privacy protection principles to political parties

In order to preserve the confidence of Canadians in the political entities with whom they deal, and in order to better protect the privacy of Canadian electors dealing with political entities, it is recommended that the *Canada Elections Act* be amended to provide a mechanism by which the application of privacy protection principles governing most Canadian institutions and organizations would be extended to political parties.

The Act should also be amended to require that political parties demonstrate due diligence when giving access to their voter databases.

The survey of electors referred to in part 2 of this report reflects the concerns of the individuals canvassed with respect to the collection and use of their personal information by political parties. More than 75% of the electors surveyed felt that they should have the right to "opt out" of communications from political entities. As well, 69% of electors disagreed with the view that it is important for political parties to be able to collect personal information on electors.[62] When asked what is more important, the right of political entities to communicate with electors or the right of electors to protect their privacy, two thirds expressed the view that preserving their privacy is of greater importance.[63]

The group of experts consulted by Elections Canada through the Institute for Research on Public Policy (IRPP) were of the view that "data gathering by the parties is a good thing, as it allows them to better reach their supporter base." They also agreed that it may be time to consider extending privacy regimes to political entities. They were particularly concerned about data breaches and the lack of recourse that those affected by such breaches would have.[64]

The Chief Electoral Officer shares these views and recommends that political entities become subject to the broadly accepted privacy principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, also enumerated in Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and reproduced in the annex to this report. These general principles govern the collection, use, disclosure and retention of records. They include requirements for accountability mechanisms; for the consent, where appropriate, of the person whose personal information is collected, used or disclosed; and for proper safeguards. This change would go a long way to reassuring electors as to the use of their personal information by political entities and to increasing the level of trust in those entities.

[62] Phoenix, Survey of Electors, p. 7.

[63] Id., p. 9.

[64] IRPP, Roundtable Report, pp. 5–6.

One way of regulating the privacy practices of parties while reducing what could be perceived as intrusion by the state in their internal affairs would be to require parties to obtain an assurance from an external management auditor, attesting that the party has systems in place to protect the personal information of electors and that these systems respect the principles listed in the annex to this report. A party would need this assurance to continue to receive lists of electors from Elections Canada.

This assurance would also preserve the reputation of the political party and reassure electors as to the protection given to their personal information, particularly in the wake of events that took place in the last election. However, such a regime would be impracticable for political entities who are by nature temporary: candidates, leadership contestants and nomination contestants.

In order to mitigate the risk of voter information being misused by candidates or persons involved in candidates' campaigns, additional measures are required. It is recommended that the Act be amended so that parties that provide voter information to candidates are required to (a) take all reasonable means to restrict access to data, (b) inform the persons to whom the data is made accessible of the proper use of the data in accordance with instructions provided by the Chief Electoral Officer, and (c) demand that these persons not use or disclose the data for any other purpose, except as required by law. In case of misuse or loss by local campaigns of voter information obtained from the party, the party that provided access to the data would be liable unless it can show that it exercised due diligence in providing access to the voter information. This would be done by respecting the above requirements.

In the discussion paper published in November 2012, Elections Canada considered whether the Act should be amended to allow electors to opt out of receiving unsolicited calls from political entities by indicating this preference when registering or updating their information in the National Register of Electors.

While it is recognized that most Canadians (78%) would like to have this option,[65] the panel of experts were strongly of the view that parties should continue to be allowed to contact voters.[66] It is also noted that the *Telecommunications Act* already provides a mechanism to deal with this issue by having one's name added to the internal do not call list of a political entity. At this time, therefore, Elections Canada does not recommend such an amendment to the Act.

New requirements governing telecommunications with electors

As a measure to reduce the risk of telecommunication devices being used to misinform electors or to mislead them as to the caller, it is recommended that the *Canada Elections Act* be amended to include certain rules regarding all telecommunications with electors.

Both the CRTC's Telemarketing Rules and Automatic Dialing-Announcing Device Rules, to which this report has previously referred, already apply to political entities with respect to some types of calls: live and automated calls for the purpose of solicitation. However, not all direct voter contacts are governed by the CRTC's Unsolicited Telecommunications Rules. For example, live calls that are not made for solicitation purposes are excluded. Moreover, under the

[65] Phoenix, Survey of Electors, p. 7.

[66] IRPP, Roundtable Report, p. 12.

Canada Elections Act, only those communications from political parties and candidates that constitute "advertising" require a statement regarding the authorization of the party's registered agent or the candidate's official agent.

The Act should provide that in the case of all messages from a political entity transmitted to a telephone, whether in the form of a live call or an automated pre-recorded call, the telephone number of the sponsor should be displayed on the call display of persons called, and should not be blocked from being displayed; the name of the sponsor of the call and the sponsor's party affiliation, if any, should be stated at the beginning of the message; the message should state whether the sponsor has authorized it; and the telephone number of the sponsor or the sponsor's campaign office at which the sponsor can be contacted should be stated at the end of the message.[67] The Act should also provide for limitations similar to those contained in the CRTC's Unsolicited Telecommunications Rules regarding the time of day during which calls may be made. These rules should apply during as well as outside of election periods.

Increased reporting requirements

The following recommendation dealing with increased reporting is made to ensure that the recommended identification requirements are met and to further prevent the recurrence of deceptive communications.

In order to assist in ensuring compliance, it is recommended that the *Canada Elections Act* be amended to require that political entities provide additional information regarding telemarketing services on a timely basis.

The Act should be amended to provide for increased reporting requirements, not only for political parties but for all entities (i.e. electoral district associations, candidates, third parties), regarding the use of telemarketing communication services. This change would assist in ensuring compliance with the previous recommendation regarding telecommunications with electors. Additional information should include the text of messages, dates on which they were communicated to electors, and, if requested by the Chief Electoral Officer, the telephone numbers that were contacted. A strong majority of the participants convened by the IRPP to provide their advice to Elections Canada supported increasing the disclosure requirements of political entities, "in a push for more transparency."[68]

Building on a recommendation contained in a motion passed unanimously by the House of Commons on March 12, 2012,[69] and on a proposal contained in Bill C-453 (a private member's bill introduced in the House of Commons on October 17, 2012), the agency recommends that parties and candidates also be required to advise the Chief Electoral Officer of the names and contact information of any person or entity they retain to provide voter contact services before or during an election, as soon as a contractual arrangement has been made with an outside organization (rather than possibly several months after the election). Such a requirement would also facilitate a more rapid investigation of allegations of improper calls.

[67] These rules now exist for advertisements in the Alberta *Election Act* at subsection 134(3) as amended by the *Election Accountability Amendment Act, 2012*. It is proposed that they apply to all telecommunications from political entities.

[68] IRPP, Roundtable Report, p. 8.

[69] Canada, House of Commons, *Journals*, 41st Parliament, 1st session, no. 94, March 12, 2012.

Increase in the Chief Electoral Officer's audit tools

The following audit mechanism is recommended to better ensure compliance with the requirements of the Act and to ensure transparency.

> In order to increase transparency, it is recommended that, upon request from the Chief Electoral Officer, political parties be required to produce all documents necessary to ensure compliance with the *Canada Elections Act*.

The first element of the motion passed unanimously by the House of Commons was that Elections Canada's investigation capabilities be strengthened to give the Chief Electoral Officer the power to request all necessary documents from political parties and thus ensure compliance with the Act. This is similar to the proposal contained in the 2010 recommendations report, whereby the Chief Electoral Officer would be authorized to request that registered parties provide any documents and information that may, in the Chief Electoral Officer's opinion, be necessary to verify that the party and its chief agent have complied with the requirements of the Act with respect to election expenses returns. This tool could be used, for example, to obtain specific documents related to voter contacts from parties, as they are not required to submit any supporting documents with their return. As discussed in the recommendations report, this authority already exists in all provincial jurisdictions.[70] This power would be available to the Chief Electoral Officer for administrative purposes, not for conducting penal investigations.

C. Recommendations to improve enforcement

Prohibition against impersonating an election official

> To facilitate the prosecution of individuals who deceive voters by pretending to be election officials, it is recommended that a provision be added to the *Canada Elections Act* prohibiting anyone from impersonating an election officer or an employee or agent of the Chief Electoral Officer. The prohibition could also extend to impersonating a candidate, a party, or representatives of such entities.
>
> To indicate the seriousness of this transgression, it is recommended that a person found guilty of the corresponding new offence, as well as the existing offence under paragraph 482(*b*) of inducing a person to refrain from voting, be liable on summary conviction to a fine of a maximum of $50,000 or imprisonment for a maximum of two years, or both; and on conviction on indictment, to a fine of a maximum of $250,000 or imprisonment for a maximum of five years, or both.

[70] *Election Act*, R.S.B.C. 1996, c. 106, s. 276; *Election Finances and Contributions Disclosure Act*, R.S.A. 2000, c. E-2, s. 5; *Election Act, 1996*, S.S. 1996, c. E-6.01, s. 280; *Election Financing Act*, C.C.S.M., c. E27, s. 67; *Election Finances Act*, R.S.O. 1990, c. E.7, s. 7; *Election Act*, R.S.Q., c. E-3.3, s. 118; *Elections Act*, S.N.S. 2011, c. 5, s. 221; *Political Process Financing Act*, S.N.B. 1978, c. P-9.3, s. 16; *Election Expenses Act*, R.S.P.E.I. 1988, c. E-2.01, s. 6; *Elections Act, 1991*, S.N.L. 1992, c. E-3.1, s. 275.

Legislation adopted by Ontario in 2011[71] creates a new offence for a person who, inside or outside Ontario, falsely represents himself or herself to be an employee or agent of the Ontario Office of the Chief Electoral Officer, a person appointed under the *Election Act*, a candidate or candidate's representative, or an authorized representative of a registered party or registered constituency association.

In the Ontario legislation, if a judge finds that the offence has been committed knowingly, the person is guilty of a corrupt practice and is liable to a fine of a maximum of $25,000, imprisonment for a maximum of two years less a day, or both.

While the offence in the Ontario statute applies to the person making the calls, the offence set out in paragraph 482(*b*) of the *Canada Elections Act* of inducing a person to vote or to refrain from voting by any pretence or contrivance would also apply to the originator of the scheme (that is, the person who directed the calls to be made).

That said, an offence similar to that of Ontario should be included in the Act not only for someone representing himself or herself as an employee or agent of Elections Canada, but also for a person falsely representing himself or herself as a candidate or candidate's representative, or as an authorized representative of a registered party or registered electoral district association. In both cases, proving the offence would not require evidence that the offender's conduct was aimed at interfering with the right to vote or at inducing electors not to vote for a particular candidate. It would be sufficient to show that the person falsely represented himself or herself. However, such an offence would need to be crafted so as to exclude bona fide political satire. This could be achieved by indicating that the false representation must be such that a person could reasonably be confused as to the impersonator's true identity.

Such an offence should be crafted broadly enough to include deceptive practices on the Internet, such as the abuse of campaign domain names and false campaign websites.

The recommended maximum amount of the fine ($250,000) or of imprisonment (five years) for both this new offence and for that set out in paragraph 482(*b*)[72] is significantly higher than for most other offences in the Act. While this could create a discrepancy, Elections Canada is of the view that many offences under the Act should provide for higher sanctions than is currently the case, in order to have a more significant deterrent effect on offenders. Higher fines would send a message to all Canadians about the importance given by Parliament to maintaining the integrity of the electoral process. Elections Canada intends to submit a report in the spring of 2014 addressing these matters and making specific recommendations to Parliament.

Increase in the Commissioner of Canada Elections' investigation tools

Elections Canada strongly believes that the Act should be amended to provide additional mechanisms to assist the Commissioner in the gathering of evidence when there are allegations of offences contrary to the Act and, more particularly, allegations of improper calls having been made to electors.

[71] *An Act to amend the Election Act with respect to certain electoral practices*, S.O. 2011, c. 17.

[72] A person currently found guilty of the offence set out in paragraph 482(*b*) is liable on summary conviction to a fine of not more than $2,000 or to imprisonment for a term of not more than one year, or to both; or, on conviction on indictment, to a fine of not more than $5,000 or to imprisonment for a term of not more than five years, or to both (see subsection 500(5)).

In order to make the enforcement of the *Canada Elections Act* more effective, it is recommended that the Commissioner of Canada Elections be given the power to apply to a judge for an order to compel any person to provide information that is relevant to an investigation.

As indicated earlier in the report, the inability to compel testimony is one of the most significant obstacles to effective enforcement of the Act. The Chief Electoral Officer strongly recommends that this power be given to the Commissioner to facilitate and accelerate the manner in which allegations are investigated.

While compliance with the Act is primarily ensured by way of offences, it is important to keep in mind that the Act is fundamentally of a regulatory nature. It sets out a number of rules, such as spending limits and reporting requirements, designed to establish a fair electoral process. The offences in the Act merely serve to better ensure compliance with those rules, and not to sanction conduct that is inherently reprehensible, as is the case with true criminal offences.

In other regulatory schemes, such as provincial securities legislation or the federal *Competition Act*, it is not uncommon for agencies responsible for ensuring compliance and conducting investigations to have the ability to require persons to provide information by way of testimony or records. Consistent with the *Canadian Charter of Rights and Freedoms*, information obtained in this manner cannot be used against those who are compelled to testify. The information may nevertheless be essential in determining whether a contravention has occurred and allowing for timely and effective enforcement or corrective action.

In the electoral context, several provincial statutes grant the chief electoral officer or commissioner, as the case may be, the power to compel persons to appear before them and provide testimonial evidence or produce records. This includes New Brunswick, Nova Scotia, Quebec, Ontario, Manitoba, Alberta and Yukon.[73] Internationally, other electoral management bodies have this power. These include the Australian Electoral Commission[74] and the Federal Election Commission of the United States.[75]

The role of the Commissioner with respect to compliance and enforcement of the *Canada Elections Act* is essential to ensuring a fair electoral process and preserving the democratic rights of Canadians under the Charter. Where the legitimacy of an election is questioned by allegations of breaches under the Act, it is in the public interest to uncover what took place in a manner that is as timely and effective as possible, in accordance with the rights of those that may be involved as well as the democratic rights of Canadians.

---

[73] Section 494 of Quebec's *Election Act*, R.S.Q, c. E-3.3, vests Quebec's chief electoral officer, with respect to his or her own investigations, with the powers and immunities of a commissioner appointed under Quebec's statute respecting public inquiry commissions (c. C-37). This includes the power described above (section 9). The same goes for the chief electoral officers of Nova Scotia (*Elections Act*, S.N.S. 2011, c. 5, s. 286; *Public Inquiries Act*, R.S., c. 372, s. 5), New Brunswick (*Political Process Financing Act*, S.N.B. 1978, c. P-9.3, s. 16), Ontario (*Election Act*, R.S.O. 1990, c. E.6, s. 4.0.1; *Election Finances Act*, R.S.O. 1990, c. E.7, s. 3; *Public Inquiries Act*, S.O. 2009, c. 33, Schedule 6, s. 33), Manitoba (*Elections Act*, C.C.S.M., c. E30, s. 186(5)), Yukon (*Elections Act*, R.S.Y. 2002, c. 63, s. 351; *Public Inquiries Act*, R.S.Y. 2002, c. 177, ss. 4 and 5) and Alberta (*Election Act*, R.S.A. 2000, c. E-1, s. 4.2 and *Election Finances and Contributions Disclosure Act*, R.S.A. 2000, c. E-2, s. 5, both as amended by the *Election Accountability Amendment Act, 2012*; *Public Inquiries Act*, R.S.A. 2000, c. P-39, s. 4).

[74] See *Commonwealth Electoral Act 1918*, s. 316.

[75] These powers of the Commission are set out at sections 437d (a)(3) and (4) of Chapter 14 of Title 2 of the United States code. See www.fec.gov/law/feca/feca.pdf.

In order to achieve this balance, it is recommended that the Commissioner be granted powers similar to those found under section 11 of the *Competition Act*.[76] The Commissioner would be authorized to make an *ex parte* application to a judge to obtain an order providing that a person who has or is likely to have information regarding an investigation be examined under oath by the Commissioner or one of his or her representatives on any matter relevant to the investigation. The order could also require the person to produce documents. The examination would be conducted in private and any person required to be examined would have the right to be represented by counsel.

Prior to obtaining such an order, the Commissioner would have to satisfy a judge, on the basis of affidavit evidence, that an investigation is taking place and that the person to be examined has or is likely to have information that is directly relevant to the investigation. In all cases, information so obtained could not be used in support of a prosecution against the person who was required to provide it, except where the person has intentionally provided misleading evidence.

In this regard, to ensure that this power is effective, the *Canada Elections Act* should also include an offence for providing false information to the Commissioner or for obstructing an investigation. Similar offences exist in various provincial electoral statutes.[77]

The Commissioner of Canada Elections strongly supports this recommendation.

To facilitate the timely investigation of improper calls, the *Canada Elections Act* should be amended to require companies that provide telemarketing services to keep records of all communications made in Canada during the election (including client information, payment information, scripts, incoming and outgoing calls, as well as phone numbers displayed). These records would be kept for a period of at least one year after the election but would be made available to the Commissioner of Canada Elections only following judicial authorization.

This recommendation is a variation of a provision contained in Bill C-453 for companies that provide telemarketing services to transmit documents to the Chief Electoral Officer within four months after the election. It is the agency's view that requiring all providers of telecommunication services to transmit this information to Elections Canada is not necessary. The purpose of this recommendation is to ensure that companies that provide telemarketing services keep records for a period long enough for the information to remain available to investigators for a reasonable period of time (in this case, a minimum of one year).

The records to be kept cover all communications made in Canada, and not just those made for election purposes. For this reason, these records should not be forwarded to Elections Canada, but only retained by the companies. They would only be shared with the Commissioner following judicial authorization through a production order issued pursuant to the authority described in the previous recommendation (that is, if a judge is satisfied, on the basis of affidavit evidence, that an investigation is taking place and that the person to be examined has or is likely to have information that is directly related to the investigation).

[76] *Competition Act*, R.S.C. 1985, c. C-34.

[77] Saskatchewan *Election Act, 1996*, S.S. 1996, c. E-6.01, s. 283; Manitoba *Elections Act*, C.C.S.M., c. E30, s. 183(7); Nova Scotia *Elections Act*, S.N.S. 2011, c. 5, s. 334; Prince Edward Island *Election Expenses Act*, R.S.P.E.I. 1988, c. E-2.01, s. 28; Newfoundland and Labrador *Elections Act, 1991*, S.N.L. 1992, c. E-3.1, s. 323.

The privacy of Canadians is only minimally affected by the production of records held by telemarketers. Indeed, in most cases, the only personal information that would be disclosed is the fact that they received a call from a telemarketing firm as well as the message used by the firm.

To facilitate the enforcement of its provisions, the *Canada Elections Act* should authorize the Commissioner of Canada Elections to require telecommunications companies to preserve specified records pending receipt of a production order issued by a judge.

In investigations dealing with deceptive practices, the Commissioner (or individuals acting on the Commissioner's behalf) should have the authority to require telecommunications companies to preserve specified computer records in their possession or control when such a demand is made. This would protect the information from being disposed of by the telecommunications companies as part of their normal business practices.

Investigators could only make such demands if the Commissioner had reasonable grounds to suspect (a) that an offence involving deceptive communications with electors was (or will be) committed under the Act, (b) that the computer record is in the possession or under the control of the person to which the demand is made, and (c) that the record would assist in the investigation of the offence. A demand would not require judicial authorization but would only be valid for a limited duration (e.g. 90 days), until a production order has been obtained from a judge.

However, in order for such a mechanism to be useful, the Commissioner would need to know in advance details regarding the telecommunication service providers of candidates and political parties. Currently, this information is not available with respect to parties. With respect to candidates, it only becomes known to Elections Canada once the candidates file their financial returns, which are due four months after polling day. Accordingly, as discussed above, candidates and parties should be required to report information on their telecommunication service providers (including phone and Internet account numbers) as soon as a contract is signed or an arrangement concluded, during or before the election period.

D. Suggestions that were not pursued

Before concluding, it is worth addressing a few suggestions that were not pursued.

In the course of drafting this report, Elections Canada received a number of suggestions from parties or experts regarding means of preventing the type of situation that occurred in the 2011 general election or facilitating the detection of guilty individuals or groups. After reviewing them, some were set aside as out of scope, not practical, too complex to implement or simply not applicable in the context of the electoral process. In this context, two of these suggestions are worth mentioning.

Granting the Chief Electoral Officer the power to cancel an election or to apply to a court for it to cancel the election

The Chief Electoral Officer is tasked with administering the electoral process. His or her role is and must remain that of a neutral and impartial arbitrator. The suggestion that the Chief Electoral Officer should be authorized to apply to a court to have an election cancelled – or worse, have the power to cancel the election – would irremediably damage this arbitrator role. This is because

the exercise of such a power would require that the Chief Electoral Officer take sides by being for or against one of the participants in the election contest. Applying to a court to seek the cancellation of an election is the responsibility of those who fought in that election or who, as electors, had a stake in the election. This should remain the case.

Providing for the possibility of rewarding whistleblowers

It is already possible for anyone who believes that an offence has been committed under the *Canada Elections Act* to report the matter to the Commissioner of Canada Elections, for him or her to investigate the matter as he or she deems necessary in the circumstances and to take the measures he or she considers appropriate for dealing with the offence if one was committed.

It has been suggested, however, that the probability of someone providing information on an offender is much greater if there is a financial incentive for the informer to denounce the alleged illegal act. For that reason, a whistleblower regime that provides a financial reward to the person who provides information on an illegal act is seen as a more effective deterrence measure than relying strictly on informers who denounce illegal acts for purposes other than money. The agency was referred to the whistleblower program available under the United States *Securities Exchange Act of 1934*.[78] Under that program, the Securities and Exchange Commission is authorized to reward the assistance and information provided from a whistleblower who knows of possible securities law violations. The legislation underpinning the program provides that the rewards are paid from a fund in which are deposited the fines imposed on offenders.

The website of the best-known Canadian whistleblower program that provides for such payments, Crime Stoppers, indicates that rewards for information that helps the police solve crimes are funded exclusively by donations from private citizens and local businesses.[79] A source of funds over which the Chief Electoral Officer would have some control would have to be generated for the payment of rewards under the *Canada Elections Act*. Furthermore, there is no whistleblower regime in Canadian federal legislation that provides for the payment of a reward to the whistleblower.[80] The electoral process does not appear to be the best context for such a regime, as nothing indicates a lack of denunciations by participants in the electoral process or by Canadians in general.

[78] See "Securities Whistleblower Incentives and Protection" in *Securities Exchange Act of 1934*, 15 U.S.C. 78a et seq., sec. 21F.

[79] http://crimestoppers.ca/donate/.

[80] See section 66.1 of the *Competition Act* and section 27 of PIPEDA for examples of whistleblower provisions in federal law. As well, see the *Public Servants Disclosure Protection Act*, S.C. 2005, c. 46.

Conclusion

The recommendations made in this report are aimed at better addressing the risks posed by deceptive tactics to Canada's electoral democracy. While Elections Canada can take some administrative measures to prevent the kind of conduct discussed in the report from occurring again, Parliament's intervention is required to make legislative changes that will allow the agency to promptly and effectively investigate potential abuses of the electoral process.

While 80% of Canadians who gave their opinion in the Phoenix survey said they had quite a lot (48%) or a great deal (32%) of confidence in Elections Canada,[81] it can be expected that this level of confidence will decrease if significant delays in investigations (let alone a lack of results) occur following repeated perceived egregious violations of the *Canada Elections Act*. Similarly, actions must be taken to increase Canadians' level of confidence regarding the vital role played by political parties in our electoral democracy. The recommendations contained in this report aim to address these two issues.

In our view, some of these recommendations are of particular importance in this context.

The authority of the Commissioner of Canada Elections to compel witnesses to testify or to produce documents with prior judicial authorization would go a long way in accelerating the investigation process, particularly at the start, when facts need to be clarified. This is a vital tool in the application of regulatory provisions, and one that already exists in federal legislation. The Commissioner strongly supports this recommendation.

As well, we share the view of Canadians and of the experts we consulted in the preparation of this report that political parties should be required to pay greater attention to the protection of electors' personal information. There do not appear to be any public policy reasons for excluding political parties from the application of the privacy protection principles governing most Canadian institutions and organizations. These principles should be extended to political parties. This could be accomplished through an assurance provided by an external management auditor. However, regardless of the means chosen, the application of these principles should be a pre-condition to the party continuing to receive lists of electors from Elections Canada.

Other recommendations have also been made to deal with the particular issue of communications with electors. They include the addition of a new offence prohibiting anyone from impersonating an election official. As well, the Commissioner should have the authority to require telecommunications companies to preserve specified records pending receipt of a production order. Political entities should also be required to provide timely information regarding their contractual arrangements with telecommunications, Internet service and telemarketing service providers, to the extent that these arrangements are to be in effect during election periods. Finally, in line with the motion adopted by the House of Commons in March of 2012, we reiterate the recommendation made in our previous recommendations report that, upon request from the Chief Electoral Officer, political parties be required to produce all documents necessary to ensure compliance with the Act.

[81] Phoenix, Survey of Electors, p. 26.

Means must be given to Elections Canada to address deceptive practices such as those that occurred during the 41st general election. These practices undermine the electoral process, to the detriment of all participants. In this context, however, it is important to keep in mind that legislative measures alone cannot prevent improper conduct from taking place. All participants in the electoral process have a responsibility to act in a manner that respects and promotes democratic values and the rule of law.

Annex

The principles that follow are set out and further discussed in Schedule 1 to the *Personal Information Protection and Electronic Documents Act*.

Principle 1 – Accountability

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

Principle 2 – Identifying Purposes

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

Principle 3 – Consent

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

Principle 4 – Limiting Collection

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

Principle 5 – Limiting Use, Disclosure, and Retention

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

Principle 6 – Accuracy

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

Principle 7 – Safeguards

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

Principle 8 – Openness

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

Principle 9 – Individual Access

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

Principle 10 – Challenging Compliance

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