Chief Electoral Officer of Canada

Issues Arising from
Improper Telecommunications with Electors

Discussion Paper

Table of Contents

Introduction

- The purpose of this discussion paper is to foster discussion on the issues arising from alleged improper communications received by electors in the days leading up to polling day and on polling day, May 2, 2011.

- The paper reviews briefly the allegations and complaints received and steps taken to deal with these complaints. It sets out the operational and legal framework of a general election and identifies other rules applicable outside the strict context of the *Canada Elections Act* (CEA). It enumerates a number of challenges that investigators faced and examines potential legislative or regulatory changes that could assist in preventing similar conduct or facilitate enforcement. The changes identified in this paper are set out strictly for discussion purposes at this time. More work is required before the Chief Electoral Officer (CEO) is in a position to make any recommendations on this issue to Parliament. The comments and suggestions received will assist in the development of balanced and better-informed recommendations to Parliament.

- While communication technologies have a potential for abuse, their benefits to the democratic process should not be ignored.

- Values and principles that should guide the discussion on this issue are the fundamental right of all electors to vote in a federal election, the right and need for political parties and candidates to communicate with electors, the privacy rights of electors, and the need for all stakeholders to preserve the integrity of the electoral process.

- Means must be found to prevent practices such as those discussed in this paper from being repeated. These practices undermine the electoral process to the detriment of all participants. In this regard, 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.

1. Alleged Improper Communications with Electors: What Happened in the May 2, 2011, General Election

This part of the paper summarizes the events that took place in the May 2, 2011, general election and reiterates steps that were taken in the following months by Elections Canada to investigate the matter.

- **Initial calls and complaints (Guelph and elsewhere)**
  - In the days leading up to polling day, on polling day, and in the days that followed, complaints were received 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).
  - Other complaints alleged 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, purportedly from candidates whose campaigns have subsequently often denied making the calls.
  - In a few cases, professional call centres have subsequently acknowledged that some electors were given erroneous information concerning their polling location based on inaccurate or outdated data.

- **Investigation of the Guelph complaints**[1]
  - Numerous complaints about telephone calls were received 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.
  - The calling number that appeared on the call display of recipients' phones was the same. This number was assigned to a pay-as-you-go cell phone, and it 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.
  - 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 a campaign 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 phone 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 obtained from that party's database.

[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. At the time of writing, the investigation is ongoing.

- The individual used a false name and address in his communications with the voice broadcasting vendor (Pierre Jones of 54 Lajoie Street in Joliette). There is no such address.
- The individual used PayPal to pay for the services rendered and gave PayPal the 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 with the same IP address,[2] through a proxy server, intentionally designed 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 a campaign office. 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 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 would have nothing to do with the actual call made by the vendor.

- **Discovery by the media in February 2012 of court documents related to the investigation and subsequent influx of complaints and reactions**
  - More than 40,000 communications were received from electors following the disclosure of this information in articles first published in the *Ottawa Citizen* on February 23, 2012, and on following days.
  - Most communications expressed outrage that individuals would try to weaken the electoral process by making false and misleading calls to electors.

- **Appearance of the Chief Electoral Officer before the Standing Committee on Procedure and House Affairs**
  - As a result of the media reports and public debate that followed, the CEO 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 CEO reported that the number of complaints alleging specific occurrences of improper or fraudulent calls was near 800.[3]
  - The CEO 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.

[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.
[3] This number reflects instances of alleged improper phone calls reported by electors, as opposed to expressions of outrage or calls for action.

- **Current status**
  - The Commissioner of Canada Elections reported that, as of August 16, 2012, the number of complaints from electors who received such calls totalled 1,394. These complaints came from electors in 234 electoral districts, including Guelph.

2. Legal Context

This part of the paper sets out the rules that apply – or do not apply, as the case may be – to the improper calls made during the last general election. It 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 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*.

- **Communications with electors by political entities under the *Canada Elections Act***
  - Communications with electors by political entities are essential to the democratic process. The main purpose of an election is to convince electors to vote and to vote for a particular candidate. This is done through a number of means but for many, the direct contact between candidates or their team and the elector remains an important strategy, if not the most important.
  - To facilitate these communications, Parliament has included a number of provisions in the CEA requiring the transmittal of elector information to parties, candidates or MPs through lists of electors (ss. 93, 104.1, 107, 109 and 45).
  - These lists contain the name, addresses (mailing and civic) and numerical identifier of each elector. They do not contain elector phone numbers.
  - 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 MPs for their respective districts. MPs also receive an annual copy of the lists of electors for their respective districts, as do parties that so request, provided they endorsed a candidate in that district in the last election.
  - The Act imposes no obligations on the recipients of the lists with respect to protecting and controlling access to the personal information they contain. 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 personal information is managed by political parties, and does not know whether there are measures put in place by the parties to control or limit the use made of this information.

- The agency understands that political parties merge the information contained on the lists of electors with their own information on electors. These databases may contain a significant amount of additional information, including phone number and vote preference, if known.[4] 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 and to facilitate communication with the electors.
- 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 some of these tools present to hide the true source of the communication, also make them key instruments for those who want to deceive electors.
- Deceptive practices[5] involving the use of "robocalls" or websites have emerged in the US 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.[6]
- 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.

---

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

[5] The expression "deceptive practices" is used in this document 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 understands "deceptive practices" more broadly as including misinformation about political opponents.

[6] 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).

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

- Under the CEA (ss. 110, 111(*f*)), the primary constraint on the use of personal information contained on the lists of electors by parties, candidates and MPs 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 only the misuse must be demonstrated but also the individual's knowledge of the source of the information and its use.[7]
- Election advertising is allowed – that is, promoting or opposing a candidate or party (CEA, s. 319ff). This may and is done through many means, including door-to-door canvassing and other forms of voter contact.
- Get-out-the-vote calls are also allowed.
- However, wilfully preventing or trying to prevent an elector from voting is prohibited (CEA, s. 281(*g*); offence at s. 491(3)(*d*)).
- Similarly, inducing a person to refrain from voting (or to vote for or against a particular candidate) by "any pretence or contrivance" is prohibited (CEA, s. 482(*b*)).
- 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 (CEA, s. 91; offence at s. 486(3)(*c*)).
- On the positive side, these prohibitions are drafted fairly broadly. The prohibitions found in ss. 281(*g*) and 482(*b*) are not tied to a particular technology or means of interference. Section 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, it is also important to note that these prohibitions are backed with criminal sanctions and not administrative penalties. As a result, non-compliance is dealt with through criminal investigations. This limits the tools available to obtain information and translates into relatively lengthy and cumbersome procedures. There is also a significant imbalance between these lengthy and cumbersome procedures and the small fines that may be imposed as a result of a guilty finding, 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.

[7] The CEA does not address the collection of personal information by political entities or its disclosure. The need for the prosecutor to prove that the individual who used the information knew that it came from the lists of electors (as opposed to another source) reduces the chance of a successful prosecution and as such reduces accountability with regard to the protection and use of the personal information contained on the lists.

- 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, grouping 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 should meet specific accessibility standards both inside and outside the building.[8] 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 CEO, usually not before the election is imminent.
- A voter information card (VIC) is then sent to all 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.
- At the start of each election, Elections Canada asks political parties and candidates not to communicate with electors regarding polling locations or poll changes to avoid the risk of confusion or potentially erroneous information being given.
- 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, electors are informed through media broadcasts and personally by an election worker posted at the entrance of the closed or changed polling station.
- 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 phone numbers of electors.[9] Even in the few cases where electors provide their phone 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.

- ***Privacy Act* and *Personal Information Protection and Electronic Documents Act***
  - The general principles governing the collection, use, disclosure and retention of personal information are found in the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and they reflect internationally recognized standards.[10]
  - However, neither the *Privacy Act* nor PIPEDA generally applies to political entities. The *Privacy Act* applies only to federal institutions – that is, generally, 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.[11]

[8] 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.
[9] 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.
[10] These principles are set out in Schedule 1 of PIPEDA and have been reproduced in the Annex to this paper.
[11] The Bennett and Bailey report mentioned *supra* indicates that British Columbia's *Personal Information Protection Act* defines an organization to include "a person, an unincorporated association, a trade union, a trust or a not for profit 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 http://www.priv.gc.ca/information/pub/pp_201203_e.pdf, p.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 use of devices such as robocalls to deceive targeted segments of the electorate is not possible without the kind of intelligence on the composition of the electorate compiled and accessed by political parties.

- **The Canadian Radio-television and Telecommunications Commission's Unsolicited Telecommunications Rules**[12]

  Authority

  - Section 41 of the *Telecommunications Act* states: "The Commission may, by order, prohibit or regulate the use by any person of the telecommunications facilities of a Canadian carrier for the provision of unsolicited telecommunications to the extent that the Commission considers it necessary to prevent undue inconvenience or nuisance, giving due regard to freedom of expression."
  - While the rules adopted by the CRTC are in many ways quite comprehensive, it is important to keep in mind that they do not apply to the Internet or e-mail communications.[13]

  National Do Not Call List Rules

  - The National Do Not Call List (DNCL) allows consumers to register a telephone number to avoid receiving telemarketing communications at that number. Pursuant to s. 41.7(1)(*c*) to (*e*) of the *Telecommunications Act*, the National DNCL Rules do not apply to a telecommunication made by or on behalf of political entities governed by the CEA, that is, registered parties, candidates, nomination contestants, leadership contestants and electoral district associations.
  - That said, it is important to note that s. 41.7(4) requires exempted individuals and organizations, such as political parties and candidates, to maintain their own internal DNCL. Political parties and candidates must ensure that no telecommunication is made on their behalf to any person who has requested to be on their DNCL. However, this provision does not apply in respect of a person making a telecommunication for the sole purpose of collecting information for a survey of members of the public.

  Telemarketing Rules

  - The Telemarketing Rules apply whether or not the telemarketing telecommunication is exempt from the National DNCL Rules. Therefore, the rules apply to political entities.

[12] 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 one-pager 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.

[13] 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.

- However, “telemarketing” is defined 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 would probably not be found to apply when they are asking for the electors’ support at the polls, as such a call does not involve a commercial activity. Nor would the rules apply to get-out-the-vote calls or calls advising of changes in polling locations.
  - The Telemarketing Rules include:
    - Prior registration of a telemarketer acting on its own behalf or of a client of a telemarketer
    - 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[14]
    - 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
    - Telemarketing telecommunications restricted 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)[15]
    - The telemarketer must display the originating phone number or an alternate number where the telemarketer can be reached

The Automatic Dialing-Announcing Device Rules

- These rules apply whether or not the telemarketing telecommunication is exempt from the National DNCL Rules. Therefore, they apply to political entities.
- An “automatic dialing-announcing device” (ADAD) is defined 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.

[14] This issue is dealt with in the CRTC fact sheet entitled “Key facts on the telemarketing rules for political candidates, parties and organizations.” 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.” See http://crtc.gc.ca/eng/info_sht/t1041.htm.

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

- 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 discussion paper are the following:
  - Restriction 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)[16]
  - 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.
  - 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 ss. 72.01 to 72.15 of the *Telecommunications Act*). Because such penalties are not part of the criminal law process, and therefore are not accompanied by the full panoply of rights and protections granted to suspects and those accused of criminal offences, they can be imposed with much greater speed and efficiency by the agency.
- The CRTC's investigative powers regarding a violation of the provisions on unsolicited telecommunications are found at ss. 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, etc.

- ***Criminal Code* restrictions on fraudulent communications**

  Current provisions of the *Criminal Code* may be of limited assistance in dealing with inappropriate communications with electors.

  Harassing or misleading phone calls (s. 372(1), (3))

  - It is an offence to convey, by telephone, information known to be false "with intent to injure or alarm any person" (s. 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 (s. 372(3)).

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

Personation (s. 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.[17]

Mischief (s. 430, 430(1.1))

- Section 430 lists activities in relation to "property" (as defined) that constitute the offence of "mischief". Section 430(1.1) creates mischief offences for destroying, altering or interfering with the use of "data" as defined in s. 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.

[17] The automated message sent to Guelph voters identified the originator as follows: "This is an automated message from Elections Canada."

3. Investigation Challenges

This part of the paper describes 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.

- **No written contracts for telemarketing or other communications with electors**

  The cases Elections Canada investigated seem to indicate that major parties deal with their own stable of telemarketing firms. Contacts within these firms appear to be shared with candidates' campaigns. While there are invoices, there is generally no evidence of written contracts between campaigns and telemarketing firms for what services are to be provided by the firms, when and at what cost.

- **Current limits to the degree of compelled reporting to Elections Canada**

  The data contained in the returns filed by political parties is currently too limited for any relevant information to be gleaned from them. Indeed, party returns only include details on the contributions received. Parties' election expenses are regrouped in broad categories, and the return provides no or little breakdown about how these expenses were incurred. Under current legislation, political parties at the federal level are not required to submit any evidence in support of their expenses.

  While candidates' returns and accompanying documentation are more complete and may show that a telemarketing firm was retained for making live or automated calls to electors, 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 CEA.[18]

  Furthermore, if a return does not indicate that the campaign retained the services of a telemarketing or telecommunications firm to communicate with electors, or if the expense was not for election advertising (e.g. calls to get out the vote) and is reported in the less-detailed return of the electoral district association, the agency would not know that expenses have been incurred for that purpose except through other channels: complaints, denunciations, etc.

  Finally, any information contained in the returns regarding arrangements with service providers may arrive too late to be of any significant assistance to an investigation.

- **Technological means of anonymity**

  Current technology offers several ways by which individuals 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.

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

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.
- That being said, 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.

Proxy servers

- Anonymity can also be facilitated through the use of proxy servers that function as an intermediary for computers and servers communicating over the Internet. Proxy servers provide anonymity by automatically cleansing their records of originating communications.
- In the investigation of the Guelph matter, Court documents filed by the Commissioner of Canada Elections indicate that proxy servers were used to communicate with the voice broadcasting vendor under a false identity.

Disposable cell phones

- Disposable cell phones can be used to hide the origin of a communication. There are also applications that allow iPhone users to create disposable telephone numbers that can be used, both for calls and text messaging, without a trace.
- In the same investigation, Court documents filed by the Commissioner specify that a disposable cell phone was used to communicate with a voice broadcasting vendor under a false identity.

- **The 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 phone number). Some keep this information for only a few days, others for three months. The length of time for which data is retained directly impacts the ability to investigate.

  The *Criminal Code* allows investigators to obtain a production order from a judge to compel individuals or entities to provide or produce certain documents in their possession to the investigator. Production orders are used as a less intrusive alternative to search warrants, under appropriate circumstances. Under s. 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 or is suspected to have been committed.

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. The chain of events and of communications may be very difficult, if not impossible, to establish where a company retains telecommunications records only for a very short period.

- **The threshold to be met to obtain a production order**

  As stated above, for a production order to be issued, investigators must show that they have reasonable grounds to believe that an offence was committed or is suspected to have been committed. They 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. Where complaints are based on the memory of witnesses or after-the-fact suspicion, the information may be insufficient as a basis for a production order to obtain evidence from a telecommunications firm.

- **The public nature of an Information to Obtain**

  Once a judge grants a production order, a document is subsequently filed with the judge reporting on the information obtained. At that point, the ITO (that is, the document drafted by investigators to explain why they need the information and why they believe it is in the possession of the specified person or entity) becomes a public document.

  It is the discovery of one of these ITOs by *Ottawa Citizen* reporters that led to the influx of complaints and reactions in February 2012. However, through the publication of the contents of the ITOs, the reputation of individuals and entities may have been negatively impacted even though the ITOs did not suggest that these persons or entities were a party to any wrongdoing.

4. What More Can Be Done to Promote Compliance and Enforcement in the Future

This part of the paper lists a number of potential remedies that *could* be considered to avoid the problems that gave rise to the complaints received regarding the 2011 general election and to promote greater compliance and enforcement in the future. It is important, however, to keep in mind that legal prohibitions and disclosure requirements are of little impact on those determined to operate outside of the law. In this regard, it is critical that potential remedies have a deterrent value and be accompanied by effective enforcement tools.

a. Public information on the electoral process

- As indicated earlier, Elections Canada is responsible for managing polling locations and ensuring changes are communicated to electors.
- In preparing for the next election, the agency will have to consider means to promote public awareness of its procedures (in particular, the fact that the agency does not communicate with electors by phone), as well as means to warn electors about misleading calls and inform them of available remedies.
- This may involve collaboration with other agencies, such as the CRTC.

b. Prohibition against impersonating an election official or knowingly providing false information on the electoral process

- Ontario's *An Act to amend the Election Act with respect to certain electoral practices,* S.O. 2011, c. 17, 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 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 s. 482(*b*) of the CEA of inducing a person to refrain from voting 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 considered 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.[19]

[19] However, at least in the case of a person falsely representing himself or herself as a candidate, 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.
- Consideration should also be given to including a prohibition on falsely representing oneself as a registered "third party" (or an agent or employee thereof). In the US, there are examples of messages sent purportedly from minority rights associations giving false information about the voting process.

c. Expansion of the Unsolicited Telecommunications Rules or creation of a similar regime in the *Canada Elections Act* to cover "voter contacts" in order to better protect the privacy of electors

- Both the CRTC's Telemarketing Rules and ADAD Rules, to which this paper previously referred, already apply to political entities with respect to some types of calls: live and automated calls for the purpose of solicitation. Some rules also apply when an automated call is made for a purpose other than solicitation. This includes the obligation for the caller to identify the person on whose behalf the call is made as well as a mailing address and phone number for reaching this person.
- There are, however, some limitations: the regime rests on telemarketers identifying themselves. If originators do not identify themselves and the automated calls are made using anonymizing technology to avoid detection, there is currently little that can be done by agencies involved in compliance and enforcement activities.
- In this context, the following issues need to be discussed.
- Should the Telemarketing Rules be expanded, or a separate but similar regime created, to cover voter contacts (that is, the gamut of calls made by or on behalf of political entities during an election campaign)? These rules would cover – as do the Telemarketing Rules – obligations such as the prior registration of the telemarketer or client, the maintenance of a DNCL by telemarketers and clients with respect to voter contacts, providing the names of the caller, telemarketer and client at the beginning of a voice telecommunication, and restrictions as to the hours during which the calls can be made.
- The Telemarketing Rules currently apply to provincial and municipal elections. Would potential rules on voter contacts also apply to them?
- Should these rules be applicable only during the election period or should they continue to apply outside electoral events?
- The benefits associated with expanding the CRTC's Unsolicited Telecommunications Rules are that the regime already exists and that the CRTC has gained some experience in its administration. The CRTC also has the authority to impose administrative penalties when the rules are violated and sufficient evidence of the violation exists. It has established contacts with the industry, which gives it access to better intelligence with respect to technological developments.
- Would it be better that a similar regime be authorized under the CEA and be administered and enforced by the Office of the Chief Electoral Officer?

- As a separate but important issue, should the CEA be amended to allow electors to opt out of receiving these calls from political entities by indicating this preference when registering or updating their information in the National Register of Electors? This information, made valid for a defined and renewable period of time (e.g. five years), could then be added beside the names on the lists of electors transmitted to parties and candidates. Political entities would be required to respect the expressed preference of electors by including them on their internal DNCLs. An advantage of this option would be that the CRTC or Elections Canada could monitor complaints and intervene with the political entity.
- However, such an approach may have perverse effects: individuals or organizations could make deceptive calls to targeted electors (supporters of their political opponents) in the hope that they would ask not to receive calls in the future, thereby interfering with another party's or candidate's ability to reach out to supporters or potential supporters (e.g. to raise funds, get out the vote).

d. Extension of the application of privacy protection principles to political parties

- The Privacy Commissioner recently sponsored a report on federal political parties and the protection of personal information.[20] This report 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.
- 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. (22)

- 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" (24).
- They describe 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 (ibid.).
- It may be time to require and ensure that political entities respect broadly accepted privacy principles similar to those set out in Schedule 1 of PIPEDA (reproduced in the Annex to this paper) regarding the collection, use, disclosure and retention of records; and the need for accountability, for the consent of the person whose personal information is collected, used or disclosed, and for safeguards.

---

[20] Colin J. Bennett and Robin M. Bayley, *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis* (Ottawa: Privacy Commissioner, 2012). http://www.priv.gc.ca/information/pub/pp_201203_e.asp.

- One way of regulating the practices of parties while reducing what could be perceived as intrusion by the state in their internal business may be to require parties to obtain a certification from an external management auditor. This certification would be to the effect that the party has systems in place to protect the personal information of electors and that these systems respect the principles set out in PIPEDA. A party would need this certification to continue to receive lists of electors from Elections Canada.
- This certification would not necessarily be a panacea – among other things, it may not be practical to apply it to candidates – but it could act as a preventive measure and possibly limit the damage that can be done by negligent people or people who do not wish to respect the rules. It would also preserve the reputation of political parties that have the certification 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. This is critical in preserving the ability of parties and candidates to communicate with electors.

e. Increased reporting requirements

The following options for increased reporting may be considered as means to facilitate investigations when complaints are received regarding improper calls.

All clients of telecommunications companies during a general election must have their identity registered and verified

- This recommendation, which was included in the motion unanimously passed by the House of Commons on March 12, 2012,[21] following media disclosure of the robocalls investigation, casts a very broad net by requiring all clients of telecommunications companies to register (with the telecommunications company or Elections Canada?) and be verified (by the telecommunications company or Elections Canada?), whether or not the purpose of their telecommunications are related directly or indirectly to the election. However, if all clients have their identity registered and verified during the election period (normally 36 days), it may be easier after the fact to trace back the originator of phone calls that may be legally challenged. The outstanding issue is one of who would administer such a regime.

  This proposal was clarified and simplified in Bill C-453, a private member's bill introduced in the House of Commons on October 17, 2012, which sets out requirements for the registered parties, candidates, third parties engaging in election advertising and electoral district associations that, during an election period, use telephone or other telecommunications devices or systems for the purpose of transmitting voice messages related to the election to electors. They would be required to keep records of the method of delivery, timing and destination of the voice messages and the name of the company with whom they entered into a contract for the purpose of transmitting the messages. This information would be retained for at least two years by the political entity, but would have to be provided to the CEO or to the Commissioner of Canada Elections within four months of either official requesting the information.[22]

[21] House of Commons, 41st Parliament, 1st Session, *Journals*, No. 94, March 12, 2012.
[22] See s. 328.4 of Bill C-453, *An Act to amend the Canada Elections Act (preventing and prosecuting fraudulent voice messages during election periods).*

- A slightly different approach, which would facilitate a more rapid investigation of allegations of improper calls, would be to require at least parties and candidates to advise the CEO 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 decision has been made regarding the means of voter contacts or an arrangement has been made with an outside organization (rather than possibly several months after the election).

Telecommunications companies that provide voter contact services during a general election must register with Elections Canada

- This recommendation, also included in the House of Commons motion, assumes that the telecommunications companies (or telemarketing companies, as may be the case) are told by their clients not only what phone numbers are to be targeted using the company's telecommunication facilities but also the common characteristic of the intended call recipients, that is, that they are all potential voters. Enforcement of such a provision could be difficult, but would make these companies more aware of the ultimate recipients of calls by parties and campaigns. That said, telecommunications companies are not otherwise regulated by Elections Canada.

- Bill C-453 proposes a different approach, which mirrors the obligation it seeks to impose on political entities to keep records. In this case, the obligation to keep the same records would be on the telephone or other telecommunications company, person or other entity that has entered into a contract with the registered party, candidate, third party or electoral district association to provide devices or systems, during an election period, for the purpose of transmitting voice messages related to the election to electors. The information would then be transmitted to the CEO within four months after polling day. The obligations would apply to any such company, person or entity, whether they are located in Canada or elsewhere.

- As noted above with regard to political entities, the investigation could proceed much more rapidly and efficiently if this information was forwarded to Elections Canada on a more timely basis (i.e. as soon as an arrangement has been concluded). This would also facilitate the tracking of alleged improper calls before records are erased in the companies' normal course of business.

f. Increase in the Chief Electoral Officer's audit tools

The number of improper calls may be reduced significantly by means of legislated administrative deterrents. The following possible audit mechanisms may be considered.

Authority to request that political entities produce all documents necessary to ensure compliance with the Act

- The first element of the motion passed unanimously by the House of Commons was that Elections Canada's investigation capabilities be strengthened to include giving the CEO the power to request all necessary documents from political parties to ensure compliance with the CEA. This is similar to the proposal contained in the CEO's 2010 recommendations report, whereby he or she would be authorized to request that registered parties provide any documents and information that may, in the CEO'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.

Authority to make any audit or examination required for and in the exercise of the Chief Electoral Officer's mandate

- As with legislation in a number of other jurisdictions, the CEA could also authorize the CEO to make any audit, examination or inquiry that the CEO considers necessary for and in the exercise of his or her mandate. This power would be available to the CEO for administrative purposes, not for conducting penal investigations.

Authority to require additional information from political entities regarding telemarketing or promotional services

- Finally, increased reporting requirements (for example, providing the text of telecommunications messages transmitted to electors during the election period), not only for parties but for all entities (i.e. electoral district associations, candidates) regarding the use of telemarketing or promotional communication services would both facilitate verification and discourage their use for unlawful purposes.

g. Increase in the Commissioner of Canada Elections' investigation tools

The following mechanisms should be considered to assist the Commissioner in the gathering of evidence when there are allegations of improper calls having been made to electors.

Requirement for telemarketing companies to preserve records of all telecommunications made during an election period

- To facilitate investigations of improper calls, companies that provide telemarketing services could be required to keep records of all communications made in Canada during the election (including client information, payment information, scripts, outgoing and incoming calls). These records would be kept for a period of at least one year after the election but would be made available to the Commissioner only after judicial authorization, through a traditional search warrant or production order.

Authority to require telecommunications companies to preserve specified records pending the obtaining of a production order

- It would also be useful to grant the Commissioner (or individuals acting on the Commissioner's behalf) 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 telemarketing companies as part of their normal business practices.
- Investigators could only make such demands if they had reasonable grounds to suspect a) that an offence 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, 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. As indicated above, the same obligation should extend to telemarketing services.

Authority of the Commissioner of Canada Elections to compel testimony, subject to prior judicial authorization

- Another mechanism, which already exists in the *Competition Act*,[23] would be to authorize the Commissioner 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 on 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.
- Prior to obtaining such an order, the Commissioner would have to establish, 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 the information sought.
- No testimony given by an individual pursuant to such an order could be used or received against that individual in a criminal proceeding.
- It is worth noting that Quebec's chief electoral officer has the power to require the attendance before him or her, *without prior judicial authorization*, of any person whose evidence may be material to the subject of inquiry, and may order any person to bring before him or her such books, papers, deeds and writings as appear necessary for arriving at the truth.[24]

[23] See s. 11 of the *Competition Act*, R.S.C. 1985, c. C-34.

[24] 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.

Annex

Principles Set Out in the National Standard of Canada Entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96[25]

4.1 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.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(*a*) implementing procedures to protect personal information;

(*b*) establishing procedures to receive and respond to complaints and inquiries;

(*c*) training staff and communicating to staff information about the organization's policies and practices; and

(*d*) developing information to explain the organization's policies and procedures.

4.2 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.

4.2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

---

[25] *Personal Information Protection and Electronic Documents Act*, Schedule 1.

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(*c*) consent may be given orally when information is collected over the telephone; or

(*d*) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 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.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 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.

4.5.1

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 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.

4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2

An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 – Safeguards

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

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

(*a*) physical measures, for example, locked filing cabinets and restricted access to offices;

(*b*) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and

(*c*) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 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.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization’s policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

(*a*) the name or title, and the address, of the person who is accountable for the organization’s policies and practices and to whom complaints or inquiries can be forwarded;

(*b*) the means of gaining access to personal information held by the organization;

(*c*) a description of the type of personal information held by the organization, including a general account of its use;

(*d*) a copy of any brochures or other information that explain the organization’s policies, standards, or codes; and

(*e*) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 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.
Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

An organization shall respond to an individual’s request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 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.

4.10.1

The individual accountable for an organization's compliance is discussed in Clause 4.1.1.

4.10.2

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.