Elections Ontario's Unprecedented Privacy Breach:

A Special Investigation Report

July 31, 2012

Information & Privacy Commissioner,
Ontario, Canada

Ann Cavoukian, Ph.D.
Commissioner

Table of Contents

Executive Summary

One of the fundamental rights in a democratic society is our right to vote. Those who choose to exercise their right to vote do so because they have faith in the electoral process. Elections Ontario is entrusted with the responsibility to protect the integrity of the electoral process, including the privacy and security of the personal information of eligible voters. The protection of privacy is hardly a novel idea – we have had privacy legislation in place in Ontario for approximately 25 years. Ontarians have rightfully come to rely on their provincial government and its agencies to responsibly manage and securely store their personal information. On its website, Elections Ontario says that its "vision is to set the standard for electoral process excellence." Unfortunately, this investigation has found that this standard was not met when it came to protecting the privacy and security of electors' personal information. Despite having privacy policies in place, Elections Ontario failed to translate these policies into meaningful business practices.

On July 5, 2012, the Chief Electoral Officer for Ontario notified me that Elections Ontario had lost two USB keys containing the unencrypted personal information of 1.4 million to 2.4 million Ontarians, including full names, home addresses, dates of birth, gender, and whether or not individual electors had voted in the October 2011 provincial election. The Chief Electoral Officer asked for my office's assistance in investigating the matter and advising how to prevent a similar breach from occurring in the future. I immediately launched an investigation to determine how the breach could have occurred and reviewed the privacy policies and procedures in place at Elections Ontario.

As the October 2011 provincial election resulted in a minority government, Elections Ontario was required to prepare for the possibility that another election might be called on very short notice. Elections Ontario's main office did not have the capacity to both store materials for a potential future election and to conduct the post-election updating project. As a result, the decision was made to conduct the "Strike-off Project" at a leased, off-site warehouse. In order to facilitate the transfer of voter information required by the project, two USB keys were used. Regrettably, contrary to agency policy, the personal information of electors contained on the USB keys was not encrypted.

On April 26, 2012, a project coordinator realized that both USB keys were missing. The incident was reported to senior management and an extensive internal investigation was launched. When an extended search did not reveal the USB keys, Elections Ontario retained external legal counsel to advise in this matter, and to initiate an independent investigation, supported by a forensic security specialist firm. Elections Ontario subsequently reported this matter to the Speaker of the Legislative Assembly of Ontario and the Ontario Provincial Police (OPP), who are conducting their own independent investigation.

Upon completion of my investigation, I concluded that Elections Ontario had failed to implement reasonable measures to protect the privacy and security of electors' personal information. I found the organization's policies and procedures to be deficient, with policies rarely reflected in actual practice.

As a result of our investigation, I have made the following recommendations.

Elections Ontario

I recommend that Elections Ontario take the following steps to enhance the protection of personal information in its custody and control. Specifically, Elections Ontario should:

1. Retain the services of an independent third party to conduct a thorough and comprehensive audit of all of the personal information management policies, practices and procedures at Elections Ontario.
2. In conjunction with the independent third party audit, develop an overarching privacy policy that applies to all aspects of Elections Ontario information management processes. At a minimum, this privacy policy must include specific direction on the appropriate use of mobile devices, including a requirement that any personal information stored on such devices be encrypted – identifying exactly what that means and who should be responsible for performing the encryption.
3. Establish Technology Services as the centre of responsibility and accountability at Elections Ontario for the implementation of strong measures to protect the privacy and security of personal information on all electronic devices, and for ensuring that staff are fully trained and supported regarding the use of these devices.
4. Appoint a senior manager within the organization as the Chief Privacy Officer to be responsible and accountable for all privacy-related matters, with the authority to approve any proposal or program impacting electors' privacy or their personal information.
5. Develop a comprehensive, mandatory privacy training program for:
    a. all temporary and full time newly hired staff;
    b. all staff, on an annual basis.
6. Develop an ongoing communications plan to ensure that all staff are made aware and reminded of the organization's privacy and security protocols and policies.
7. Provide my office with a copy of the audit report, and any new or revised policies and procedures, for review and comment within six months of the date of this Report.

Government of Ontario

I recommend that the government of Ontario:

1. Ask the Office of the Auditor General of Ontario to conduct privacy audits of the information management practices of selected public sector agencies in the province.
2. Conduct a complete review and modernization of the *Election Act* to ensure that the privacy and security of personal information in the custody and control of Elections Ontario is strongly protected and used prudently, as prescribed.

Background

On July 5, 2012, the Chief Electoral Officer for Ontario advised my office that two unencrypted USB keys, containing the unencrypted personal information of up to 2.4 million Ontarians, had been lost by or stolen from his organization, Elections Ontario. The personal information stored on the USB keys included full names, home addresses, dates of birth, and gender, as well as whether or not an individual elector had voted in the October 2011 provincial election.

Upon learning of this privacy breach, I immediately launched an investigation to examine how it could have occurred, and began to review the relevant privacy and security policies and procedures in place at the province's election agency. I also urged the Chief Electoral Officer to notify affected members of the public about the breach as soon as possible. The results of my investigation form the basis of this Report.

Elections Ontario

Elections Ontario is a non-partisan, independent agency of the Legislative Assembly of Ontario that is responsible for the conduct of provincial elections and byelections. Elections Ontario operates under the direction of the Chief Electoral Officer, an officer of the Legislative Assembly, and employs 97 permanent staff, and temporary workers, as needed. At the time of this investigation, my staff were advised that there were approximately 50 temporary workers employed at Elections Ontario. For the 2010/2011 fiscal year, Elections Ontario had a budget under the *Election Act* of $16 million. Elections Ontario is responsible for the day-to-day operations necessary to assist the Chief Electoral Officer in performing his duties.

The Chief Electoral Officer's mandate, which is set out in the *Election Act*, is to establish and maintain a permanent register of electors for Ontario, to implement measures to verify the accuracy of the permanent register, and to ensure that the permanent register is updated at least once per year. Following an election, he or she is responsible for the management and storage of documents and lists containing the personal information of eligible electors in Ontario, of which there are currently approximately 8.9 million.

Ontarians entrust their personal information to Elections Ontario so that they may exercise their democratic right to vote. It is this personal information that is the currency in which Elections Ontario trades. The sensitivity of the personal information in the organization's custody and control is recognized in guidelines developed for authorized users of the data, referred to as the *Permanent Register of Electors for Ontario and List of Electors Guidelines* (the *Guidelines*) which can be found on Elections Ontario's website. The *Guidelines* state that there is a need to ensure that all authorized users of this data understand the importance of protecting the privacy of electors' information. In the *Guidelines*, Elections Ontario also states that it "places high importance on respecting the privacy of personal information" and that "authorized users of the List of Electors must take appropriate measures to keep private the personal information in the List of Electors and to preserve the reputation of Ontario's electoral system and its participants." The importance of maintaining the privacy and integrity of electors' personal information underscores the seriousness of this breach.

The *Election Act*

Before I turn to the issues under consideration in this investigation, I would first like to set out the statutory framework for provincial elections in Ontario and the work of Elections Ontario. Ontario provincial elections are governed by the *Election Act,* which provides a broad framework that covers both the organization and the conduct of provincial elections. Under this statute, the Lieutenant Governor-in-Council appoints a Chief Electoral Officer who is responsible for the administration of the *Election Act*.[1]

In addition, for each of Ontario's 107 electoral districts, the Lieutenant Governor-in-Council appoints a Returning Officer, based on the recommendation of the Chief Electoral Officer.[2] Each Returning Officer is responsible, under the direction of the Chief Electoral Officer, for running the election within that district.

Massive amounts of personal information are collected, used, and disclosed as part of the election process. Pursuant to section 17.1 of the *Election Act*, the Chief Electoral Officer is required to establish, maintain and update Ontario's permanent list of electors, known as the Permanent Register of Electors for Ontario (PREO). PREO contains the following fields of personal information for individual electors:

- Full Name;
- Home Address;
- Date of Birth; and
- Gender.

Under the *Election Act*, the Chief Electoral Officer may provide the personal information contained in PREO to (a) the Chief Electoral Officer of Canada; and (b) any municipality in Ontario and its local boards.[3] Registered political parties and Members of Provincial Parliament (MPPs) are also entitled to request a copy of PREO (or in the case of an MPP, a copy of part of PREO that relates to his/her district).[4]

It is, however, important to note that section 17.4 of the *Election Act* dictates that any information obtained from PREO, whether directly or indirectly, is to be used for electoral purposes only.[5] The use of information from PREO for non-electoral (including commercial) purposes is considered to be an offence under the *Election Act*, punishable by a fine of up to $5,000.[6]

To protect against the potential for misuse of information in PREO, the Chief Electoral Officer can publish guidelines to inform political parties, MPPs and others about the use and access requirements in the *Election Act* and additional best practices for maintaining the privacy of the

1 *Election Act*, s. 4(1)
2 *Election Act*, s. 7(1)
3 *Election Act*, s. 17.2
4 *Election Act*, s. 17.3
5 *Election Act*, s. 17.4
6 *Election Act*, s. 97

information contained in PREO.[7] Each registered political party is also required to develop and implement a policy to ensure that its candidates, MPPs, employees and agents do not misuse information obtained from PREO and that they comply with any related guidelines issued by the Chief Electoral Officer.[8]

Further privacy protection is provided to Ontarians through section 17.1.2, which allows individuals to opt out of PREO by having their names removed from the electoral list, upon showing proof of identity and place of residence. During an election period, an elector can apply at the district's returning office to have his or her name removed from PREO.[9] An elector can also apply to have his or her name removed from PREO by: (a) submitting an application form and copies of supporting documents to the office of the Chief Electoral Officer; or (b) appearing in person to the municipal clerk in the electoral district.[10]

After an election is announced and a formal writ of election has been issued, PREO is used by the Chief Electoral Officer to prepare a list of electors for each Returning Officer.[11] The list of electors is to be maintained at each returning office and made available for public inspection.[12] In addition, the list of electors is to be disclosed by the Returning Officer to:

- the clerk of each municipality with territorial jurisdiction in the polling division; and
- each candidate in the electoral district.[13]

The list of electors contains the full names and home addresses of individual electors.

For election day, the Returning Officer for each electoral district prepares official polling lists for every poll within that district. Each official polling list is a compilation of the list of electors plus any updates made by the Returning Officer and contains the information of the specific electors assigned to that poll (typically a few hundred electors). On election day, polling officials record which electors voted on the official polling list. Eligible voters who do not appear on the official polling list are still permitted to vote and are added to the record of electors for the poll where they vote. The official polling lists and records of electors include Ontarians' names and addresses (but not their dates of birth or gender).

Following each provincial election, the *Election Act* directs the Returning Officer for each electoral district to send all election documents, papers and materials (including copies of all official polling lists) to the Chief Electoral Officer. Section 84(1) states:

> Forthwith after making his or her return, the returning officer shall arrange for shipment in the prescribed manner to the Chief Electoral Officer of all envelopes

7 *Election Act*, s. 17.5. A copy of the most recent guidelines can be found in the Ontario Gazette, Saturday January 8, 2011, Volume 144-02, ISSN0030-2937, pp. 175 to 205.
8 *Election Act*, s. 17.6
9 *Election Act,* s. 17.1.2(2)
10 *Election Act,* s. 17.1.2(3)
11 *Election Act*, s. 19(1)
12 *Election Act*, s. 19(3)(a)
13 *Election Act*, s. 19(3)(b) and (c)

> returned to the returning officer by the deputy returning officers, and all documents, papers, and materials in his or her possession relating to the conduct of the election.

The Chief Electoral Officer is then required to retain this documentation for at least one year following an election (and a longer period if the election is contested).[14]

Section 86(1) of the *Election Act* allows any member of the public to inspect these election related documents (with the exception of the ballots):

> All documents forwarded by a returning officer in pursuance of this *Act* to the Chief Electoral Officer, other than ballots, shall be open to public inspection at such time and under such conditions and rules as are made by the Chief Electoral Officer, and he or she shall supply copies of or extracts from the documents to any person demanding them on payment of the prescribed fee, and in computing the number of words a figure shall be counted as a word.

Reading these sections of the *Election Act* together, I conclude that the Chief Electoral Officer has the statutory authority to:

- collect and retain (for one year) elector information arising from the election process;
- collect and use elector information for the purpose of establishing and updating PREO;
- disclose to political parties and MPPs copies of PREO (which includes an elector's name and address); and
- disclose to the general public elector information arising from the election process (except ballots from the election) including full names, home addresses and whether someone has voted in the previous election.

The Strike-off Project

Because the October 2011 provincial election resulted in a minority government, Elections Ontario was required to prepare for the possibility that another election might be called on very short notice. This included the requirement to update PREO based on information obtained during the October election. At the same time, Elections Ontario was involved with processing the 2011 general election documentation that had to be returned to Elections Ontario by the Returning Officers for each of the electoral districts.

This significant post-election project is called the "Strike-off Project" which involves updating PREO using the information obtained by elections officials during the previous election, including information with respect to which individuals should be deleted, transferred or added to the list of electors for each of the 107 electoral districts. The project team also updated Elections Ontario's records by indicating whether individuals had voted in the election of October 2011.

14 *Election Act*, s. 85

This information was taken from the list of electors used by polling officials at each poll on election day. (As voters present themselves to obtain a ballot and vote, their names are crossed off the list of electors by polling officials. These "strike-offs" are then scanned by project staff into an electronic database with a separate file for each electoral district that is used to update PREO.) The Strike-off Project team set up following the 2011 election consisted of 15 data entry clerks who were hired as temporary employees, as well as two team leaders, who were also temporary employees. The project was primarily overseen by permanent staff members of Elections Ontario's Electoral Events Services (EES) division. This included two coordinators and a manager who reported to the Director of EES.

Previous iterations of the Strike-off Project had been completed at Elections Ontario's permanent facilities on Rolark Drive. The Rolark Drive facility provides offices and work stations for Elections Ontario employees, as well as storage for election-related documentation and forms.

Following the October 2011 election, Elections Ontario realized that the Rolark Drive facility did not have adequate space to provide storage for both the new forms and the documentation that had been ordered in preparation for a possible election in the near future, as well as the documentation that had been returned by the province's electoral districts to Elections Ontario following the 2011 election. As a result, the decision was made to store the returned elections material at a leased warehouse on Birchmount Avenue (the Birchmount warehouse), close to Elections Ontario's Rolark location. Since the material required by the Strike-off Project would be stored at the Birchmount warehouse, a further decision was made to locate the Strike-off Project's work in the same warehouse. This decision was confirmed by Elections Ontario's Strategic Leadership Team in February 2012.

Following this decision, a Manager from the EES Division who was responsible for the Strike-off Project arranged for the approval and acquisition of the necessary equipment and staffing for the Birchmount warehouse and assigned two staff to coordinate and oversee the project. The Technology Services department was involved in the setup of the computer hardware and software required for the project, and the Human Resources department assisted with staffing needs.

The start date for the Strike-off Project was March 5, 2012. The update of PREO involved each of the province's 107 electoral districts. The 15 data entry clerks were each given a laptop computer and would have electoral district files downloaded by one of the team leaders onto their designated laptop. The team leaders had all 107 electoral district files transferred to their laptops, also using USB keys. Each of the 15 data entry clerks would then update an electoral district file on their laptop by inputting data contained in written records sent to Elections Ontario by the Returning Officer for that electoral district. This included scanning the list of electors, using a hand-held barcode scanning device, from each poll within the electoral district to capture which individuals had voted in the election. Updating a single electoral district in this manner could take upwards of two weeks. Using a commercial software application, the data from each updated electoral district was then copied into the PREO database.

The challenge of locating the Strike-off Project at a remote location soon became apparent. Previous Strike-off Projects, having been located in Elections Ontario's Rolark headquarters, were able to make use of the information technology resources available at that location.

The projects could rely on secure, interconnected systems which protected electors' personal information. This meant that electoral districts could be updated and that electors' personal information would reside only on the secure servers at the Rolark headquarters. In contrast, the Birchmount warehouse was not electronically connected to the Rolark headquarters and did not have a secure server.

As a result, the Strike-off Project was left with the challenge of transferring the information from the updated electoral districts onto the main server at the Rolark facility. This lead the Manager to make a request to Technology Services on March 15, 2012 for two USB keys. The keys would have a number of functions. Once a data entry clerk had completed updating an electoral district, a team leader would transfer the completed district to the key. The completed district would then be downloaded onto the team leader's laptop. A new electoral district would be loaded by the team leader onto the USB key and downloaded on to the data entry clerk's laptop to allow the updating of that district to commence. Finally, given some concerns regarding the age and reliability of the laptops provided to the data entry clerks, it was contemplated that the USB keys could be used to back up incompleted electoral districts to guard against loss.

It appears that little or no thought had been given as to how the updated electoral districts would then be transferred from the team leaders' laptops at the warehouse to the Elections Ontario's main servers. This lead to one coordinator, who assumed the responsibility for this task, visiting the warehouse periodically and transferring the updated electoral data back to Elections Ontario's main servers by using a third personal USB key.

While the circumstances surrounding the decision to provide the USB keys to the Strike-off Project team are set out in detail below, it is sufficient to note here that although the Technology Services division advised against using USB keys as part of the Strike-off Project, the decision was nonetheless made to use the USB keys.

One of the Strike-off Project coordinators purchased two USB keys with a corporate credit card. After the keys were purchased, they were provided to staff in Technology Services who made a record of the serial numbers of the keys.

The Strike-off Project coordinators received verbal direction from their Manager to encrypt the data contained on the USB keys, without any instructions as to how to do so. These two USB keys were then given to the two team leaders – they were told to lock the keys in their desks overnight and not take them off-site. The coordinators and team leaders were not provided with any training or instruction on the meaning of encryption or how to enable the encryption function of the keys.

When interviewed by my staff, it became clear that the Strike-off Project staff were of the opinion that encryption meant compressing ("zipping") and password-protecting files. They had no understanding of the meaning of "encryption." Acting on this information, the two team leaders were told to ensure that any electoral districts uploaded onto the USB keys were "zipped" (not encrypted) and password protected, with instructions provided on how to accomplish this task. The team leaders were also provided desks with locks and were directed to lock the USB keys in their desks. The team leaders had been instructed to delete the files of the completed electoral

districts from the USB keys once the data had been successfully uploaded onto their laptops. The team leaders were responsible for regularly uploading the data inputted by the 15 data entry clerks on to the two USB keys, and using the USB keys to transfer that data to their laptops.

The Privacy Breach

In the late afternoon of April 23, 2012, the Strike-off Project team was advised not to report to work on April 24, 2012 as mould had been detected in the Birchmount warehouse. The project remained shut down through April 27, 2012. On April 25, 2012, the two coordinators attended at the Birchmount warehouse to perform some quality control work while the Strike-off Project team was absent. One coordinator checked the two team leaders' USB keys. At that time, it became apparent that the two USB keys used by the team leaders were not being securely stored. The USB keys were either left on the team leaders' desks or, if locked in the desk drawer, the desk drawer key was readily available. One of the coordinators was able to easily obtain the USB keys and perform the quality control work. The coordinator also noted that electoral district data had not been deleted from the keys, nor had it been zipped or password protected, but took no steps to do so. After finishing with the two USB keys, the coordinator placed them back on the team leaders' desks; one in a pencil holder on the desk and the other in a roll of masking tape – neither key was securely locked away.

On April 26, 2012, the two coordinators returned to the Birchmount warehouse to continue working on the quality control task. At approximately 3:00 p.m. that day, the coordinator who had used the USB keys on the previous day realized that they were missing. The coordinators searched for the USB keys the rest of that day, and the following morning, but to no avail.

The breach was reported to senior management at Elections Ontario on April 27, 2012 and an extensive internal investigation was launched. When an extended search did not reveal the keys, Elections Ontario retained the law firm of Gowling Lafleur Henderson LLP to advise it in this matter, and to initiate and guide an independent investigation, supported by INKSTER Incorporated, a forensic security specialist firm. Elections Ontario subsequently reported this matter to the Ontario Provincial Police (OPP), and it is currently conducting its own independent investigation.

The Strike-off Project resumed its work on April 30, 2012. Although a number of measures were implemented over the next month to address security deficiencies, the project resumed using a replacement set of USB keys. Remarkably, despite the experience of the previous week and the resulting anxiety over lost data, the replacement USB keys were unencrypted, and no thought was given to encrypting the laptops which contained portions of PREO.

As noted above, my office was only notified of the privacy breach on July 5, 2012 by Ontario's Chief Electoral Officer. Following this, the Chief Electoral Officer held a media conference on July 17, 2012 to publicly announce the loss of the USB keys. Elections Ontario also initiated an extensive outreach program to notify Ontarians about the loss.

This was a massive breach. There were 49 electoral districts being worked on by the Strike-off Project at the time of the breach, involving information relating to just over 4 million electors. Despite significant forensic investigation, Elections Ontario has not been able to specifically identify the number of electoral districts contained on the USB keys at the time of their disappearance. However, it is estimated that between 20 and 25 electoral districts were involved, potentially impacting between 1.4 and 2.4 million electors. Based on the interviews conducted with my staff, I accept Elections Ontario's estimate of the scope of the breach as being reasonably accurate. Given that Elections Ontario was unable to specifically identify which electoral districts were involved, the public notification alerted all 49 districts.

The USB keys included the following elector information:

- Full Name;
- Home Address;
- Date of Birth;
- Gender;
- Whether the elector had voted in the last election; and
- Administrative codes used solely for election purposes.

The scope of this breach makes it by far the largest in Ontario, and possibly, Canadian history.

The Investigative Process

While Elections Ontario is not subject to the *Freedom of Information and Protection of Privacy Act* (the *Act),* the Chief Electoral Officer approached me to assist Elections Ontario by conducting a full review of this matter and to provide advice on containment of the breach, and notification of the affected parties. My office provided immediate advice on the method of notification and urged that it take place at the earliest opportunity. In addition, I immediately launched an investigation, with the full cooperation of Elections Ontario, mindful of the privacy protection provisions set out in Part III of the *Act*, applicable to provincial government institutions.

As part of this investigation, my office conducted a review of the policies, practices and procedures in place at the agency. My staff also interviewed senior management at Elections Ontario and members of the Strike-off Project team. All interviews were conducted at Elections Ontario's head office on Rolark Drive. On July 9, 2012, my staff also conducted a physical inspection of the Birchmount warehouse. We reviewed a number of internal documents including:

- *Permanent Register and List of Electors Privacy Policy*;
- *Permanent Register of Electors for Ontario and List of Elector Guidelines*;
- *Elections Ontario Computer and Technology Acceptable Use Policy*;

- *Elections Ontario: Internet Acceptable Use Policy*;
- written employee statements of the incident; and
- relevant emails and other correspondence.

Throughout the entire investigation, my office received the full and complete cooperation of Elections Ontario staff – I would like to commend the Chief Electoral Officer and his staff for providing my office with timely and thorough responses.

Issues Arising from the Investigation

The issues arising from this investigation are:

1. Is the information on the USB keys "personal information" as defined in section 2(1) of the *Act*?
2. Did Elections Ontario put in place reasonable measures to protect the privacy and security of the personal information of Ontario voters?
3. Did Elections Ontario have appropriate policies and procedures in place to protect the privacy and security of the personal information?
4. Did Elections Ontario adequately train its staff to ensure that they implemented and understood the measures to be taken to protect the privacy and security of the personal information?
5. Did Elections Ontario respond adequately to the privacy breach?
6. What actions, if any, should the government of Ontario take in response to this breach?

Issue 1: Is the information on the USB keys "personal information" as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* states, in part, that "personal information" means recorded information about an identifiable individual including:

> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> …
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> …

> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

As noted above, the lost USB keys contained the full name, home address, date of birth and gender of Ontario voters. They also included information about whether or not the individual had voted in the last election and "administrative codes" that were used solely for election purposes.

I am satisfied that the USB keys did not include any information that would reveal how an individual voted. However, I am also satisfied that the information on the keys meets the requirements of the definition of "personal information" contained in one or more of paragraphs (a), (d) or (h) of section 2(1) of the *Act*.

Issue 2: Did Elections Ontario put in place reasonable measures to protect the privacy and security of the personal information of Ontario voters?

Section 4 of Ontario Regulation 460, made pursuant to the *Act*, establishes the obligation to ensure that organizations have reasonable measures in place to protect the privacy and security of the records of personal information in their custody and control. Section 4 states:

> (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.
>
> (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
>
> (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

As mentioned above, Elections Ontario is not an institution under the *Act*. However, for the purposes of evaluating the steps taken by the organization to protect the privacy and security of the personal information in its custody and control, and advising the Chief Electoral Officer on additional steps that may be required, Section 4 of Regulation 460 is a useful reference point.

In the discussion that follows, I will therefore consider whether Elections Ontario had reasonable measures in place to protect the privacy and security of the personal information entrusted to it for the purposes of the management of elections in this province, taking into account the nature of the records to be protected.

The Workplace

As noted above, following the 2011 election, senior management decided that the Strike-off Project needed to be completed on an expedited basis. Given that the government was in a minority position, Elections Ontario staff were required to be ready in case an early election was called. This lead to the decision to house the Strike-off Project at the Birchmount warehouse.

A *Project Change Request* form was completed in order to get the necessary approvals to move the project to the warehouse. This form was sponsored by the EES division and approved by a number of senior managers at Elections Ontario. The form documented the need to move the project and identified the costs associated with the rental of furniture, janitorial services, laptop computers, and staffing.

It is notable that the *Project Change Request* form did not include an analysis of the privacy and security issues associated with the establishment of the project off-site at the Birchmount warehouse. The only comment contained in the form that indicates any consideration of the challenges posed by the off-site location is the following:

> Having no connectivity between [Elections Ontario Headquarters] and the off-site location could provide communication problems and slow the project down.

The senior managers interviewed by my staff could not recall any specific discussions about the privacy and security issues associated with working in the warehouse. As reflected in the *Project Change Request* form, it appears that any discussion revolved around identifying the materials and support required to get the job done, and getting staff in place to undertake the project.

This oversight is very significant – its importance cannot be overstated. The eventual loss of the USB keys can be traced back to the failure to systematically identify the privacy and security issues, both physical and technological, that the Strike-off Project would face at the off-site location. Given that the project would have access to the PREO database – a massive database containing electors' personal information – it is somewhat shocking that obvious security measures were not addressed.

For example, with regard to the physical layout of the off-site location, I note the following:

- The Birchmount warehouse was equipped with a lock and an alarm system. However, 16 different staff had the code to activate and deactivate the alarm, and had a key or access to a key to the premises. Among those who had keys or access to keys were warehouse staff who were not working on the Strike-off Project.

- The project staff and their laptops were located on the warehouse floor, without any partition or separation from the other warehouse activities. The laptops were therefore accessible to anyone entering the warehouse.

- While desks with locking drawers were made available to the two team leaders, as I will discuss in detail below, at times the locked drawers of the desks were not used by staff, nor were the drawer keys stored in a secure manner.

- The primary work space for the Project Manager and the two permanent coordinators was at the Rolark headquarters – thus they were not in the warehouse overseeing the work of the Project team on a regular or permanent basis.

Of greater concern was the failure to consider any of the crucial technology challenges posed by the decision to locate the Strike-off Project at the off-site location. This is of grave concern considering the vast amount of elector information involved in the project, and the stewardship role that Elections Ontario has been entrusted with in relationship to this information.

For example, although senior management understood that the Project team would be using laptops to carry out their work and that at any given time, the laptops would be loaded with portions of PREO, virtually no thought was given to the risks posed by the use of these portable devices in an open concept warehouse. The hard drives were not encrypted, nor were the laptops secured in any fashion to prevent them from being stolen. Insufficient attention was devoted to the threats to privacy and security that might arise from external sources or other staff already working inside the warehouse, who were not directly involved in the Strike-off Project.

Senior staff should have taken the time to evaluate the risks associated with the move of this project to the Birchmount warehouse. This evaluation should have involved the relevant divisions including EES, Technology Services and Corporate Services. Failing to do so, the result was that staff who did not require access to personal information for the purposes of their positions, were in possession of the keys and the alarm code to get in to the building. Once inside the building, laptop devices containing unencrypted data, protected by very weak passwords (which I will discuss in detail below) were accessible in the facility's open concept environment. Other than the password protection on each laptop and the ability to lock USB keys into desks, no efforts were made nor was thought given to the privacy and security of the personal information that was accessible to the project team.

Privacy and Security of Electronic Devices

The failure to plan for the privacy and security risks posed by locating the Strike-off Project at the Birchmount warehouse is most egregious when considering the privacy and security flaws that resulted.

The simplest security precautions were overlooked. For example, laptop computers were assigned to data entry clerks, along with a user name and password. The user names were Elmsuser01, Elmsuser02, and Elmsuser03, etc. At the outset, all Project staff shared the exact same password which was 1234abcd. My staff learned during interviews that this was the default password assigned to all computers that had "stand-alone applications." While staff were prompted by the computer to change their password, we learned that most did not do so. In fact, some staff who changed their passwords wrote the new password on yellow stickers that were stuck to the front of their computer screens. It appears that there was no direction given to staff to change or protect their user names and passwords.

Most important, insufficient thought was given to how electoral data would be securely transferred between the data entry clerks and the team leaders, and then between the team leaders and the

Rolark headquarters. The process that lead up to the use of unencrypted USB keys was indicative of a significant failure in the planning process.

The potential use of USB keys as part of the Strike-off Project was originally raised on February 29, 2012. In reviewing the technology equipment requirements identified by EES, a Technology Services staff member sent an email to EES saying:

> …USB keys are not acceptable to use they are a security concern, if you want to use them please have [the EES director] sign off that she accepts the risk.

On March 5, EES responded with the following:

> There is no longer a requirement for a printer, or USB keys, we will develop a workaround.

However, by March 15, 2012, the need for the USB keys to transfer data during the Strike-off Project had again been raised. Part of the reason for this may have been because of difficulties experienced with the reliability of the laptops assigned to the project. On March 8 and 14, 2012, emails were sent by one of the project coordinators requesting that Technology Services assist with laptops that had "crashed." In an email sent on March 15, 2012 by the Manager, EES to the Technology Services division and the Acting Director, EES, there was no reference to the need for the USB keys to transfer the data. Rather, the email stated:

> We have a need for 2 USB keys for the Strike-off Project. The keys will be used to back up the data on a nightly basis. We had a bit of a scare yesterday when there was an incident with one of the laptops. Fortunately we were able to recover the data, however, having a way to back up the data will avoid possible loss of work.
>
> […] – can you please respond to this email giving your authorization to use the keys?
>
> Thanks very much

The response from the Acting Director, EES was as follows:

> I have signing authority for [the director] while she is away. Please accept this as approval for the USB keys to mitigate potential data loss.
>
> We understand that this is a temporary solution that will not be continued at the end of the project.
>
> **…I would imagine a concern is what will be on the USB key and how we will protect that data from being lost/stolen. Can you confirm that the USB keys will be securely stored and data erased/protected when the data is backed up in a more conventional way?**

The Manager of Technology Services responded to this email as follows:

> I will send over the link to the form, understand that voter data on a USB key is a concern and is in no way recommended, if the person(s) involved forget it in their pocket and take it home overnight and *if it is lost or stolen, it is wide open*.
>
> *Your signature on the form is required to remove our responsibility as this is not a recommended security practice for private data*. [Emphasis added.]

This email elicited a response from the Director of Technology Services, directed to the Acting Director, EES:

> Please ensure that [Manager, EES] encrypts the data before storing it on a key. Also – can you please elaborate on the storage protocol that will be in place for the keys?

The Manager EES indicated that the keys "will be put in a protected area each night and not transported off-site. There is also a security (alarm system) at the Birchmount warehouse. When the project is complete, the data will be returned to EO HQ, the data will then be erased from the keys and returned to [Technology Services]."

Finally, the Director, Technology Services responded by noting the danger inherent in the use of USB keys:

> **My point is what is a 'protected area' – is that a safe? An office? Someone's car? My concern is not with outside people getting in, but with the contract staff helping themselves to a key. That is why the data needs to be encrypted and stored in a place that they do not have access to.**

Despite the clear dangers of using USB keys having been identified, the Acting Director, EES signed a *Hardware Request Form* on March 15, 2012, requesting two keys for the Strike-off Project.

Our interviews determined that the project coordinators then approached Technology Services staff about acquiring the USB keys. They were directed to purchase the keys themselves directly from an office supply store, since requisitioning the keys through Technology Services would take some time. The project coordinators were given directions as to which keys to purchase. The devices that were recommended by Technology Services possessed built-in encryption software. Despite the fact that the correct keys were purchased, the encryption needed to be "turned on" or enabled in order to be activated. It was not, nor were the coordinators instructed to do so by Technology Services.

One of the project coordinators returned to Technology Services to have the serial number of the two keys recorded. However, at that time, Technology Services staff made no inquires as to whether the project coordinator understood the need for encryption, how to deploy the encryption function on the key, or even whether the coordinator understood what encryption was. They did not even instruct the coordinators to activate encryption functionality.

This proved to be a crucial oversight. As I noted above, the Project Manager told my staff that he thought the direction to encrypt the data meant that the data should be "zipped" and password protected. He asked his two coordinators if they could encrypt the data and they said they could.

The coordinator who was interviewed corroborated this version of events. It was her understanding that zipping a file and adding a password was the equivalent of encryption. She conducted a Google search to find out how to do that, and once satisfied that she knew how, she instructed the team leaders how to zip and password protect files loaded on the USB keys. The coordinator stated that it was not part of her routine to check to see whether the team leaders were following the protocol of zipping and password protecting the files, although she subsequently discovered on April 24, 2012 that this was not being done. This begs the question – who was responsible for ensuring the encryption took place?

It is important to note that the act of zipping a file does not result in the data being encrypted. To zip a data file is to compress the data so that more data can be stored on a device. Therefore, once zipped, the data is easier to transmit, and takes up less computer memory and bandwidth. Once the file is zipped, it can be password protected. However, password protection and zipping do not offer the strong security features of encryption. The difference between these two processes was not well known at Elections Ontario, if understood at all, particularly among front-line staff who were expected to ensure the security of the data.

While Elections Ontario acknowledged that the data on the two missing USB keys were not encrypted, in a number of public statements regarding this privacy breach, they stated that the data on the lost USB keys could only be accessed in an intelligible form using "internal Elections Ontario proprietary software" or "specialized commercial software applications." The implication of this statement was that the data could not be read and that the loss of the USB keys represented only a minimal privacy risk to electors whose information was contained on the key. With due respect, this is simply not accurate.

During the course of our interviews with senior staff, we learned that to query (or read) the data on the USB keys, an individual must first install a commercial software application, which can be downloaded for a fee from the Internet. Therefore, the data that is stored on the USB keys can be easily queried or read using this readily available software program. This language and associated software are also available for free download online. To suggest that the information is unintelligible is simply not the case. Nor is it accurate to suggest that because this commercial software application is required to read the data, the risk of the data being accessed is low. That is not the case. It is not the same as encryption – far from it. The easiest and most straightforward way to render data unreadable to unauthorized parties is to encrypt it.

My office has issued a number of papers[15] and Orders[16] that address the need to ensure that mobile devices are encrypted. For example, in March of 2007, I conducted an investigation following the theft of a laptop computer from a physician's automobile. The laptop computer

15 *Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes* (September 2011); Fact Sheet 16: *Health-Care Requirement for Strong Encryption*, (July 2010); Fact Sheet 14: *Wireless Communication Technologies: Safeguarding Privacy & Security* (August 2007); Fact Sheet 12: *Encrypting Personal Health Information on Mobile Devices* (May 2007)

16 Order HO-004, Order HO-007, Order HO-008

contained the personal health information of a large number of patients of a large hospital. In Order HO-004, issued under the *Personal Health Information Protection Act* (*PHIPA*), I stated:

> A written and enforced corporate policy prohibiting the removal of identifiable patient information from the hospital might have prevented this incident. Similarly, a clear corporate policy requiring the encryption of [personal health information] on desktop and laptop computers would have provided an essential level of protection. Finally, the enabling of all computing devices with the appropriate security protections by the hospital's IT department would not have left this important function to be decided by an individual staff member.
>
> Corporate responsibility for security recognizes that technical safeguards may become outdated over time as technology evolves. Password protection, which is extensively canvassed in [the health custodian's] policies, can no longer be considered to provide adequate security. Password "crackers" are easily available and may well be part of a network administrator's tool kit in order to help staff who have forgotten or lost their passwords. [Personal health information] of this very sensitive nature must be either de-identified or encrypted if on disk, e-mailed or stored on a laptop computer.
>
> Encryption is a common and potentially effective mitigation to the risks associated with having [personal health information] accessed outside of normal network protections. Encryption is the practice of encoding a message or data in such a manner as to render it into a meaningless array of letters, numbers and symbols. Such encoding, or encryption, is accomplished by the use of a computer algorithm and encryption keys. If relatively current encryption tools are used, [personal health information] is effectively rendered meaningless. This significantly reduces the risk of a privacy breach to a truly negligible level, provided that the encryption keys are not included with, or in the lost or stolen laptop. While encryption may have an impact on system performance, it so clearly addresses the risk of a privacy breach that the onus must be placed on the organization to justify not using it. For health information custodians, the encryption of [personal health information] on vulnerable computing devices, particularly laptops, should now be viewed as the rule, not the exception.

In Order HO-007, issued under *PHIPA* in January 2010, I investigated the circumstances surrounding the loss of a USB key which contained the personal health information of individuals who had attended immunization clinics. In that Order, I reminded health information custodians of the benefits of encrypting personal health information stored on mobile devices. I stated:

> If an encrypted USB memory stick was lost, there would be no cause for alarm on the part of the organization, which would have a high degree of confidence that the stored data would not be compromised. There would be no need to invoke the time-consuming and expensive breach management process involving notification, investigation, and remediation.

As other immunization clinics using unencrypted mobile devices were in progress at the time of my investigation, I wanted to alleviate any ongoing concern regarding the ability of these clinics to proceed with this important work. I introduced the public health unit's senior staff to CryptoMill Technologies, a private Ontario company which has developed encryption software solutions. CryptoMill offers one of a number of encryption software solutions that are widely available, many of which are built right into the portable electronic storage devices. The requirement to encrypt sensitive data is not a novel idea – it should be fundamental to the policies and practices of any organization whose bread and butter is the personal information that has been entrusted to its care. The existence of products from companies such as CryptoMill demonstrates that, with a modicum of thought ahead of time, Elections Ontario could have put into place a comprehensive solution for the security needs of the Strike-off Project.

The failure to ensure that encryption was properly deployed on the USB keys simply highlights the failure of Elections Ontario to put in place reasonable measures to protect the personal information of Ontario voters. Much-needed, essential planning did not take place to mitigate the privacy risks inherent in the Strike-off Project. Some specifics:

- I am not satisfied that the Strike-off Project required the use of USB keys at all. One of the basic tenets of privacy protection is that personal information should not be placed on mobile electronic devices, if other alternatives exist. Here, at least two alternatives should have been considered by Elections Ontario. Given the sensitivity of the information that was the subject of the Strike-off Project, the project should have been conducted at the Rolark headquarters and other pre-election functions, which did not involve personal information, relocated to the Birchmount warehouse. Alternatively, a server could have been installed at the Birchmount location in order to negate the need for USB keys. While there may have been some discussion about installing a server at the warehouse prior to the Strike-off Project start, it appears that the time required for this to happen lead to the decision to use the USB keys.

- The purpose to which the USB keys were to be put was not well defined. For example, the interviews conducted by my staff suggested that information should have been deleted from the keys once a completed electoral district was uploaded onto a team leader's laptop. This would have meant that the loss of the keys would not have been as serious. However, deletion of stored information would seem to be contradictory to the stated purpose of using the keys "to back up data on a nightly basis." (As evidenced by the email from the Manager, EES, dated March 15, 2012, which is referred to above.) We were not successful in obtaining any clarity on this matter.

- It appears that little or no thought was given as to how the completed electoral districts would be transferred from the Birchmount warehouse to the Rolark headquarters. As a result, a project coordinator used a personal, unencrypted USB key to perform this function. Given the lack of planning in initiating the project, this should not be surprising. In the absence of any useful guidance from management, she was left to her own devices, albeit her actions resulted in a breach of existing policies, which was not surprising, given the lack of training (see below).

- There was a general failure of senior staff to take responsibility to ensure that the USB keys, once deployed, were encrypted. Technology Services noted the need for encryption, but failed to follow up with EES to ensure that this requirement was understood, and that the devices deployed were, in fact, encrypted.

- EES accepted the risk of using USB keys, but did not take any steps to ensure that front-line staff engaged in the Strike-off Project understood what encryption actually meant, and that the information on the keys was encrypted.

- The thought that one particular department could "accept" the responsibility for taking a privacy risk is unacceptable. Privacy is a corporate responsibility, especially for Elections Ontario. In this case, the failure to appreciate that a privacy breach affected not just one division, but the entire organization, was an inherent organizational weakness.

In summary, I have found that Elections Ontario did not have reasonable measures in place to protect the privacy and security of the personal information of Ontario voters. Elections Ontario must develop and implement a comprehensive corporate privacy policy. At a minimum, the privacy policy must provide that personally identifiable information will not be stored on USB keys, laptops or other mobile electronic devices unless absolutely necessary. If it is absolutely necessary to transfer personal information to a mobile device, personal information stored on that device must be encrypted. The need to then explain what that means and how it can be achieved is critical.

In addition, Elections Ontario must develop an organization-wide endpoint electronic devices policy, applicable to portable devices (laptops, PDAs and mobile storage devices like USB keys and CDs) which mandates that any personal information not stored on secure servers must be encrypted.

The development of these policies should only occur following a thorough review of Elections Ontario's privacy, security and technology requirements. This investigation has focused on a single incident – the loss of two USB keys containing significant portions of the PREO database. However, this breach points to the need for a full review of Elections Ontario's information management practices. Only by following a comprehensive review of Elections Ontario's practices and procedures will its privacy and security vulnerabilities be identified so that the corresponding policies and procedures can be developed.

I am not satisfied that Elections Ontario has sufficient privacy expertise to undertake this work internally. I will, therefore, be recommending that the organization seek outside assistance to review current practices, and to develop strong, agency-wide privacy policies and appropriate information technology policies and procedures.

Issue 3: Did Elections Ontario have appropriate policies and procedures in place to protect the privacy and security of the personal information of Ontarians?

Two documents were provided by Elections Ontario in response to a request from my staff for any policies and procedures relevant to this breach – the *Permanent Register and List of Electors Privacy Policy* (PREO Privacy Policy) and the *Elections Ontario Computer and Technology Acceptable Use Policy* (the Acceptable Use Policy.) As discussed below, taken together, these policies provided inadequate direction to Elections Ontario staff regarding the need to protect the privacy and security of personal information entrusted to their custody and the appropriate means to be taken to ensure that the information is protected.

PREO Privacy Policy

The PREO Privacy Policy in effect at the time of the breach was finalized prior to the 2011 election. It was authorized by the Chief Electoral Officer and the Deputy Chief Electoral Officer on August 24, 2011. Of relevance is the fact that the EES Manager responsible for the Strike-off Project is listed as the "Contact Officer" on the document. The policy was circulated to Elections Ontario staff by way of an all-staff email on September 12, 2011 and is available for reference by Elections Ontario staff on the office's intranet site. However, as the preceding review of events leading up to the loss of the USB keys demonstrates, a policy is not enough. If policies are not reflected in practice, they have little value. Policies must be translated into procedures which are then implemented by way of visible actions, in order to be effective. This fact appears to have been completely overlooked in the present case.

Section 1 of the document notes that the PREO Privacy Policy:

> …establishes standards for the protection of personal information of electors. The policy is guided by the overarching privacy protection principles reflected in the legislative framework that applies to governmental agencies in Ontario and is in conformity with the standards and expectations of Elections Ontario's data partners.

Section 10 contains numerous provisions that are relevant to the incident involving the lost USB keys. That section is entitled, "*Securing Privacy in a Mobile Work Environment*." Under the heading *Electronic Records*, the following requirement is set out:

> 9. Electronic records containing personal information should be stored and encrypted on a password protected disk, CD, or removable drive rather than on the hard drive of a laptop or home computer.

Under the heading *Laptops and home computers*, direction is given that access to laptops and home computers should be password controlled, and any data on the hard drive must be encrypted. Employees are also directed to only use software that has been approved by Elections Ontario's Technology Services Division.

Finally, under the heading *Wireless Technology*, the following relevant provision is set out:

> 15. Employees must protect the privacy and confidentiality of personal information stored on wireless devices such as personal digital assistants and cellphones. Access to such devices must be password controlled, and any stored data should be encrypted.

At first glance, the PREO Privacy Policy may appear to be adequate. However, on further examination, serious deficiencies become apparent. The first relates to the scope and purpose of the policy – it relates only to the Permanent Register and List of Electors. It was confirmed by Elections Ontario staff that no agency-wide privacy policy exists. Given that personal information may be handled by Elections Ontario staff who are not directly involved with the Permanent Register and List of Electors, a comprehensive privacy policy is an absolute necessity.

The primary focus of the PREO Privacy Policy is on the use of the Permanent Register and List of Electors by external stakeholders, resulting in insufficient attention being given to the obligations of Elections Ontario staff. For example, section 2 sets out the purpose of the policy. That section notes that the Permanent Register and/or the List of Electors will be provided to a range of stakeholders, including political parties, Returning Officers, municipal clerks, local candidates and the Chief Electoral Officer of Canada. However, only passing mention is made of Elections Ontario staff themselves who are involved in the preparation and distribution of the Permanent Register.

I am not confident that an Elections Ontario staff member, in search of the privacy requirements applicable to their position, would readily turn to the PREO Privacy Policy. As mentioned, the policy seems to focus primarily on the external recipients of the Permanent Register, such as political parties, candidates and Returning Officers. I will, therefore, be making a recommendation regarding the need for a comprehensive, agency-wide privacy policy to guide the work of all Elections Ontario staff members.

I further note that there are substantive deficiencies in the PREO Privacy Policy that need to be addressed. For example, while the need to encrypt data stored on mobile devices is noted, by stating that personal information "should" be encrypted, doubt may exist in the minds of staff as to whether this is an absolute requirement. Further, this provides insufficient guidance to staff. Mobile devices must only be used as a last resort for storing personal information, and only when other more secure alternatives are unavailable. Should it be necessary to transfer personal information onto a mobile device, such a transfer should be limited to only that which is absolutely necessary. The PREO Privacy Policy does not contain this required level of granularity. Nor does it provide any indication of how one would go about encrypting the data involved, or what type of encryption was contemplated.

In addition, the suggestion in section 10 of the policy that the use of password protected disks, CDs or removable drives should be preferred over the hard drive of a laptop or home computer makes little sense. Encrypted data stored on a laptop or home computer is as secure as encrypted data stored on these other devices. In the case of a laptop or home computer, it is arguable that these devices are less likely to be lost or misplaced because of their size.

The policy also appears to contemplate the storage of personal information on home computers. Allowing the use of personal devices over which the agency has no control presents serious privacy and security risks. It is clear that Elections Ontario must undertake a thorough review of the direction being provided to staff and stakeholders in the management of electoral information in order to ensure that such information is being handled securely and in accordance with relevant privacy and security requirements.

During our interviews, we also found that knowledge of this privacy policy was inconsistent. Several front-line staff were, in fact, completely unaware of its existence. Also, the privacy policy was not included in the orientation package provided to new employees. This may not come as a surprise since, as noted, it is not an agency-wide policy, but rather focuses on only a portion of the work done by Elections Ontario. I am not satisfied that there is sufficient agency-wide awareness of the PREO policy and its relevance to the work being conducted across the organization. It is clear that, although a policy was in existence, albeit with many deficiencies, the requirements of the policy had not permeated the organization.

I would like to make some final observations regarding the PREO Privacy Policy. The policy does set out some specific responsibilities for senior Elections Ontario staff that, in my view, were not met in the circumstances of this breach.

For example, the Director of EES is responsible for:

- developing business practices to ensure compliance with the guidelines to ensure that the privacy protection measures outlined in the policy are met; and
- advising the CEO of any policy gaps that need to be addressed and developing appropriate procedures and operational guidelines to address these gaps.

Further, managers responsible for the Permanent Register of Electors are responsible for ensuring the implementation of the PREO Privacy Policy, providing resources to ensure that staff are equipped to implement the guidelines, and training and mentoring staff to ensure that their roles are well defined in relation to the implementation of the privacy policy and its guidelines.

As related above, the events leading up to the loss of the USB keys lead me to conclude that none of these responsibilities were met. The Strike-off Project was initiated without any consideration being given to the privacy and security implications raised by the use of a remote location and the use of portable electronic devices. Business practices were not put into place to ensure that privacy protective measures were implemented and that privacy responsibilities were met. Certainly, none of the privacy and security gaps (that could have been easily identified with a modicum of effort) were identified or addressed. As has also been identified, front-line staff were not provided with appropriate direction or resources to meet their obligations.

Similarly, relevant responsibilities of the Director of Technology Services included:

- Developing and implementing an information security framework and information technology services to meet the requirements of established privacy guidelines, including the appropriate use of passwords and encryption methods to ensure the protection of data;
- Guiding Elections Ontario management and staff in conducting risk/needs assessments related to the security of information on the Permanent Register;
- Ensuring that the procedural guidelines related to the security of information are translated into normal business practices throughout the organization; and
- Providing guidance to management and staff in the implementation of information security standards and procedural guidelines.

In my view, none of these responsibilities appear to have been met. The Strike-off Project was allowed to proceed at an off-site location without due consideration being given to the information technology implications. For example, the data on laptops was not encrypted or secured, and user IDs and passwords were rudimentary, left unchanged or, in some cases, appeared in full public view. Although encryption was identified as a requirement for USB keys, if they were used, front-line EES staff were directed by Technology Services to purchase their own keys! More egregiously, Technology Services staff allowed those keys to be put into service without first ensuring that the project staff knew what "encryption" meant and had specific instructions on how to properly use the USB keys (i.e. activating the encryption function) to ensure that electoral information stored on the keys was, in fact, encrypted. Clearly, Technology Services did not ensure that the guidelines were translated into normal business practices, nor did it provide staff with any guidance on the implementation of information security standards.

In my view, the failure of senior managers to meet their obligations under the PREO Privacy Policy directly led to the privacy breach experienced by the Strike-off Project – the policy was simply not reflected in practice. The actions of the front-line staff bore no resemblance to the privacy policy.

Acceptable Use Policy

The Acceptable Use Policy was issued on May 12, 2005. I understand that it is also available on the Elections Ontario intranet site. In general, the policy sets out guidelines regarding access to and disclosure of data on any electronic communications system belonging to Elections Ontario. A significant portion of the policy deals with the ability of Elections Ontario to ensure the security of their information technology systems and to set standards for the personal use of equipment and the Internet. There are a number of provisions relevant to this investigation:

- Initial passwords are assigned by Technology Services; employees should change this password as soon as possible using the instructions *provided by the IT staff*.
- Passwords should not be displayed openly at any workstation.

- Computers with sensitive information installed on the local disk drive should be secured in a locked room or office during non-business hours.

- The use of and storage on premises of USB data storage keys or any other external storage devices is restricted to those provided and supplied by Technology Services through the proper request and authorization. [Emphasis added.]

As with the PREO Privacy Policy, there appeared to be little awareness of the Acceptable Use Policy and even less adherence to it. While initial passwords may have been provided by Technology Services, it is clear that employees were not directed by Technology Services staff to change those passwords as soon as possible, although they may have been prompted to do so by the laptop computers assigned to them. My staff were informed that passwords were displayed openly at workstations, at least by some staff. Given the broad access allowed to the warehouse, it simply cannot be said that the laptops in use by the Strike-off Project staff were securely stored. Indeed, it was not until several weeks after the USB keys went missing that the decision was made to secure the laptops to the Strike-off Project staff's desks. Finally, the USB keys in use by the Strike-off Project staff were not supplied by Technology Services. In fact, Technology Services had directed Strike-off Project staff to purchase the two missing keys themselves.

I note that, as part of the orientation process, new staff are required to read and sign the *Internet Acceptable Use Policy*. As the name suggests, this document is not the same as the *Computer and Technology Acceptable Use Policy*. The document, signed by staff, sets out the organization's rules designed to "promote the responsible use of Internet functions by specifying acceptable conduct for accessing information on the Internet." It does not refer to issues such as the physical security of computers nor the requirement to only use devices provided and supplied by Technology Services.

Given the breaches of the Acceptable Use Policy that occurred while the Strike-off Project was operating, the need for greater staff education relating to the policy is readily apparent. This is an issue that I will address below.

Privacy Breach Protocol

While the privacy policy includes a requirement that staff must report to managers any omission or discrepancy affecting privacy protection, and any potential or actual violation or breach of privacy, this is not sufficient. Organizations must have in place a privacy breach protocol that all staff are familiar with and are trained on to ensure that staff know what steps need to be taken in response to a privacy breach. It was clear from the outset that senior management were not able to determine whether or not a privacy breach had occurred. Yet it should have been abundantly clear that the missing USB keys posed a serious threat to the privacy of the individuals whose information they contained.

Elections Ontario should develop a comprehensive privacy breach protocol and ensure that all staff are trained on the appropriate steps to be taken in the event of a privacy breach or suspected privacy breach.

No Chief Privacy Officer

The shortcomings of the policies, and their failure to have any meaningful impact on the daily activities of staff, points to the importance of not only having robust privacy policies in place, but also the need to ensure that the import of those policies permeates the daily activities of all staff. It is also indicative of a lack of understanding by Elections Ontario of the requirement to protect the privacy and security of personal information and the way in which that should be done.

In staff interviews, it was clear that there was no "go-to person" at the agency should staff have a question about privacy requirements or the implications of particular practices on privacy. It is commonplace for organizations that deal with sensitive personal information to have, at a minimum, a senior staff person with the designated responsibility for privacy such as a Chief Privacy Officer. The involvement of such a person in the planning stages of the Strike-off Project would have been invaluable.

During our interviews at Elections Ontario, my staff were left with the impression that Elections Ontario staff gave priority to getting the Strike-off Project up and running, at the expense of any privacy and security concerns. A Chief Privacy Officer with the authority to delay the project until such concerns had been addressed would likely have prevented such a privacy breach. No such person existed. Focus could have been placed on the critical privacy issues raised by conducting such a project off-site. For example, greater scrutiny could have been given to the physical security of the warehouse and the need to closely regulate access to the facility. An employee with privacy authority could have delayed the project until a server was installed at the warehouse, thus avoiding the serious risks inherent in the use of USB keys and unencrypted laptops. By turning their minds to how the transfer of voters' personal information was to be made from the warehouse to the main Rolark facility, alternatives to the use of USB keys would have been considered.

Accordingly, I will be recommending that Elections Ontario appoint a senior staff person as Chief Privacy Officer, with the authority to ensure that projects and practices do not proceed until the privacy and security implications are satisfactorily resolved.

Issue 4: Did Elections Ontario adequately train its staff to ensure that they implemented and understood the measures to be taken to protect the privacy and security of the personal information of Ontarians?

My office has repeatedly stated that the requirement to put in place reasonable measures to protect the privacy and security of personal information includes a requirement to ensure that staff are appropriately trained in the privacy and security requirements related to personal information and the protocols in place to manage that information. This means that staff and management who require access to personal information in order to perform their duties must receive training to a level commensurate with the sensitivity of the information to which they have access.

During the course of interviews conducted with managers in EES, Technology Services and Human Resources, my staff learned that:

- No training was offered to staff at Elections Ontario regarding the privacy and security of personal information.

- Some management staff who participated in the development of the *PREO Privacy Policy* did not know whether the policy was on the Elections Ontario intranet site and did not know whether any measures were in place to review the policy with staff.

- Most staff did not know who the contact person was, in the event they had any concerns relating to privacy and the security of personal information.

- The only direction that staff using the USB keys received was a verbal direction from the Manager of the Strike-off Project that the information on the USB key should be encrypted. However, neither the manager nor the staff knew what encryption was.

- No training was offered with respect to encryption. Staff responsible for the project thought that they could set up the encryption on the USB key by "zipping" a file and password protecting it. The non-management project staff who were interviewed were not aware of the privacy policy and the fact that it included a requirement to encrypt all data on mobile devices. Surprisingly, these same staff said, at the time of our investigation, that they were still confused as to what encryption entailed and how to carry it out.

- At the time of the breach, the Director of Technology Services was aware of the existence of the privacy policy but was not sure who was responsible for ensuring that encryption on mobile devices was in place. He was of the view that the responsibility for implementing the encryption lay with the "business area."

What was particularly discouraging was the discovery that the privacy and security of personal information did not form part of any of the training programs that were offered to staff. Despite the sensitive nature of the information in the custody and control of Elections Ontario, no training was offered to staff regarding the organization's obligation to protect the information in its possession from inappropriate access, loss or theft. Needless to say, this is completely unacceptable.

Even if an organization does have strong privacy policies and protocols, which I have found was not the case here, those policies and protocols are of little assistance in ensuring the privacy and security of personal information if staff have not been adequately trained. It is equally important to conduct regular training courses to ensure that privacy awareness remains embedded within an organization.

Given the nature of the personal information in the custody and the control of Elections Ontario, senior management has an obligation to put in place comprehensive privacy and security education and awareness campaigns which should include the following:

- Elections Ontario should provide training regarding privacy, the ability to identify privacy breaches, and the security of personal information upon the hiring of all full-time and temporary staff;

- Training of all staff should be refreshed on an annual basis;

- In addition to the oath of secrecy required by section 115 of the *Election Act*, a confidentiality pledge should be signed upon hiring which includes an acknowledgement by staff that failure to comply with the pledge or oath of secrecy, or their participation in a breach of privacy, may result in disciplinary action, including the termination of employment; and

- Regular communiqués should be given to all staff on the importance of privacy and security of personal information via email blasts, newsletters and posters positioned in those physical areas where staff are working with personal information.

In addition to the failure to provide any training on the obligation to protect privacy and the security of personal information, Elections Ontario failed to offer any training on the use of the USB keys and on the implementation of the encryption on those devices. As I noted, the Technology Services department requested that the staff in the Strike-off Project purchase specific USB devices because they included encryption functionality. However, these staff did not know how to use the devices, did not understand what encryption meant and assumed that if a file was "zipped," it was encrypted. Given the lack of training and support provided by Technology Services, this was not necessarily an unreasonable assumption.

In my view, the Technology Services department must function as the center of responsibility for ensuring that appropriate devices are deployed and software installed, as well as ensuring that users are provided with sufficient training. The Technology Services department should also be responsible for training on any privacy and security protocols developed in relation to the use of these devices.

In summary, Elections Ontario did not adequately train its staff to ensure that they implemented and understood the measures to be taken to protect the privacy and security of personal information. In my view, the failure to have in place a comprehensive training and communications program on privacy, security and the appropriate use of mobile devices, was a significant contributing factor to the present privacy breach.

Issue 5: Did Elections Ontario respond adequately to the privacy breach?

Investigating the breach

On April 26, 2012, when the Strike-off Project staff first learned that the USB keys were missing, a thorough search was conducted of the warehouse premises and the home of the project coordinator who had used the keys the previous day. On the morning of April 27, 2012, staff reported the loss to their Manager, who notified his superior, who, in turn, notified the Chief Electoral Officer the same day.

Another physical search of the warehouse area was conducted that day and on April 30, 2012, the Strike-off Project team was advised that there had been a security breach at the warehouse. On May 4, 2012, the Director of Election Finances, the General Counsel and the Director responsible for the Strike-off Project met with the Chief Electoral Officer. During that meeting, staff decided they did not have enough information to determine whether or not a privacy breach

had occurred. Consequently, a decision was made to provide a questionnaire to employees to gather additional information. Other internal investigations were completed, which culminated with a report that was provided to the Chief Electoral Officer on May 25, 2012.

On May 24, 2012, Elections Ontario consulted with external legal counsel who recommended that it retain the services of an investigation firm to conduct an independent review. On May 31, 2012, the Speaker of the Legislative Assembly of Ontario was notified of this breach. On June 13, 2012, Elections Ontario contacted the OPP and asked that it investigate the matter.

As noted above, on July 5, 2012, my staff and I met with the Chief Electoral Officer and senior staff members from his organization at which time the circumstances surrounding this breach were reported to my office. At that time, Elections Ontario staff advised that in responding to the privacy breach, they had reviewed the IPC's *Privacy Breach Protocol, Guidelines for Government Organizations*. We were also advised that the purpose of its report to the IPC was to request assistance on the issues of containment, notification, and privacy audits, and to coordinate communications plans and public messaging. Following this meeting, my office immediately began its investigation.

As noted previously, the Chief Electoral Officer held a media conference on July 17, 2012, at which time he publicly notified the citizens of the province about the breach. On the same date, the Chief Electoral Officer also wrote to the Speaker to formally notify him of the breach and to submit to the Speaker a preliminary report regarding the breach prepared by outside counsel retained by his office. The Chief Electoral Officer also directed the following:

- An immediate and comprehensive review of all Elections Ontario policies, processes, procedures and protocols related to the privacy, management, protection and custody of voter information, including staff orientation, training, management oversight and accountability and audits;

- An immediate and comprehensive review of Elections Ontario Technology strategic framework, infrastructure and management policies and oversight.

I am satisfied that Elections Ontario conducted a thorough search for the missing USB keys once their disappearance was discovered. I also commend the organization for retaining outside assistance to investigate the potential scope and cause of the breach. However, my concerns with the organization's response to the breach are twofold: the delay in contacting my office regarding the loss of the USB keys and the corresponding delay in notifying the public and those who may potentially be affected by the breach.

I commend Elections Ontario for reviewing the IPC's *Privacy Breach Protocol, Guidelines for Government Organizations*. However, I note that my office's guidelines on responding to a privacy breach state:

> Upon learning of a privacy breach, immediate action should be taken. Many of the following guidelines need to be carried out simultaneously or in quick succession.

In my view, Elections Ontario and the public would have been better served had they contacted my office much sooner. The delay of some 10 weeks between the USB keys going missing and my office being notified was, in my view, excessive. My office has the experience to provide focused and timely advice on containing and responding to privacy breaches, particularly breaches of significant magnitude. IPC staff are available to advise organizations about all issues surrounding a privacy breach. However, I appreciate that Elections Ontario wanted to conduct a thorough search for the keys prior to contacting my office.

I am also concerned that the delay in contacting my office lead to a delay in notifying the public of the breach. Again, I appreciate that Elections Ontario wanted to try to identify the exact scope of the breach, including the specific electoral districts impacted, prior to undertaking public notification.

At some point prior to July 17, 2012, it should have been apparent to Elections Ontario that the USB keys were unlikely to be recovered and that the identity of all individuals affected could not be established with any specificity. Timely notification of affected parties is essential to give those individuals an opportunity to manage their financial and personal affairs in a way that would minimize the impact of the breach on them. It can take several years for individuals to clear their names once they have become the victim of identity theft. Early action and detection of unusual transactions or activity will minimize the potential impact of the breach. The delay involved in the containment and notification of this incident to affected individuals may have caused unnecessary harm, undue stress and alarm to Ontario voters.

Restarting the Strike-off Project

Strike-off Project staff were not working at the time the USB keys went missing, as the mould issues identified earlier were being addressed. However, the Strike-off Project resumed its work on April 30, 2012. A number of measures were implemented over the next month to address the security deficiencies in the project. However, I consider these measures to be totally inadequate, failing to address the glaring privacy risks raised by the loss of the USB keys.

Most notably, the project resumed using a replacement set of USB keys. On May 8, 2012, the following request was sent by the Manager EES to Technology Services:

> 2 USB memory sticks are needed for the Strike-Off project. These sticks are to be used by PREO full time staff only and are needed to back up data and to transfer encrypted data from the Birchmount warehouse to [Elections Ontario].

We were informed that Technology Services again refused to sanction the use of USB keys. However, EES once again managed to acquire identical keys to those that were missing and put them into active use!

As the email request of May 8, 2012 indicates, procedures regarding the use of the keys were altered after the incident. For example, only the project coordinators and the Manager of the Strike-off Project were allowed to use the USB keys, keys were to be kept in their possession at

all times and were to be purged of data once completed electoral districts had been transferred to the secure server at the Rolark headquarters. Other steps that were taken included:

- The laptop computers which contained unencrypted data that were in use by the project team were secured to the desks with a padlock.
- Each user was instructed to create his or her own unique user name and password.
- A security guard was retained to guard the premises.
- The number of individuals having access to the alarm code was reduced.

Given the experience of the previous week, it is inconceivable that the Strike-off Project would have continued using USB keys. Even more egregious is the fact that the data on the keys continued to be unencrypted. The confusion as to the difference between zipping/password protecting files and encrypting files continued. In fact, a report prepared by the Director of EES for the Chief Electoral Officer on May 25, 2012 states that protocols were put in place on May 1, 2012 to ensure that **passwords** were attached to laptop computers and USB keys. Amazingly, it was not until May 14, 2012 that a request was sent from EES to Technology Services asking that an alternative to the use of USB keys be explored. The use of the keys continued until May 26, at which time a server was installed at the Birchmount warehouse to convert the environment from a stand-alone to a network. In short order, on May 28, 2012, the decision was made to move the Strike-off Project from the Birchmount warehouse to the Rolark headquarters, thus negating any further need for the use of USB keys.

In general, I found that Elections Ontario's efforts to continue the Strike-off Project were wholly inappropriate in light of the breach that had just been experienced. A much more prudent approach would have been to put the project temporarily in abeyance until all the privacy and security implications of the missing USB keys had been addressed. Instead, the project was restarted with essentially the same vulnerabilities. USB keys were still employed for the storage of unencrypted personal information! In addition, front-line staff remained uneducated as to the meaning of encryption and how to deploy the encryption capabilities of the USB keys. Alternatives to the use of the keys were slow in being requested and implemented. Further, although the laptops in use were secured to their desks and the passwords changed, the data on the laptops remained unencrypted. It seems that the need to continue the Strike-off Project in a timely fashion trumped the need for proper privacy and security measures. It may only be through good fortune that a reoccurrence of a similar breach was avoided.

This failure to adequately learn from the privacy breach and to implement the required privacy protocols demonstrates the need for the development and implementation of a comprehensive, agency-wide privacy policy. This will be addressed in my recommendations.

Identifying Technology Vulnerabilities

In reviewing the steps taken by Elections Ontario in responding to this breach, I am concerned that the organization did not recognize that greater action was required to determine whether vulnerabilities existed with the way in which technology was deployed throughout the entire

organization. Simply put, a major privacy breach occurred on April 25, 2012, potentially affecting a massive number of individuals, and damaging the reputation of the organization. In addition to addressing the privacy and security issues raised by the Strike-off Project, one might have expected Elections Ontario to conduct an immediate review of other potential vulnerabilities elsewhere in the organization. For example, were other staff members storing unencrypted personal information on their mobile devices? To what extent were personal devices being used throughout the organization? Were laptops and other portable devices appropriately secured physically – was the data they contained protected? Such a comprehensive review and audit has yet to happen.

Only two initiatives of relevance seem to have been taken in this regard. First, on May 25, 2012, the Director of Technology Services sent an email to all Elections Ontario staff, saying, in part:

> In a few moments, Technology Services staff members will be coming to your desk to verify the contents of every USB key that you may have in your desk space. They will ask you for any USB keys, if you have one, I ask that you provide it to them.
>
> We are looking for a specific file and hence this will only take seconds – literally. They will open the USB at your workstation.

My staff have confirmed that the purpose of this exercise was to locate the two missing USB keys. It was not designed as a general review of USB keys deployed in the agency to ensure that personal information or other sensitive material was not contained on the keys, in an unencrypted state.

Second, on July 13, 2012, after my investigation had commenced, the Director of Technology Services sent an email to all Elections Ontario staff. The email announced the implementation of three changes aimed at protecting data through encryption. These changes included:

- The installation of an encryption utility on every staff members' PC and laptop by Technology Services. The encryption will be seamless and work automatically in the background.
- Personal portable devices such as USB keys and external hard drives cannot be used in conjunction with Elections Ontario hardware. Should a portable drive be required, an encrypted drive will be provided by Technology Services and will come with a "how-to" instruction.
- Assigned cellphones such as BlackBerrys or other devices such as iPads will require a password.

Although this was clearly a step in the right direction, these changes alone are not sufficient. This direction was only provided to staff almost three months following the privacy breach experienced by the Strike-off Project. Further, this direction reveals additional, ongoing privacy and security issues within the organization. For example, the email suggests that, until July 13, 2012, cellphones and other mobile devices were being used by Elections Ontario staff without the basic security offered by password protection. Most important, these changes do not represent

a comprehensive review of Elections Ontario's information technology policies and procedures nor the manner in which technology has been deployed by the organization. One might have expected that the April 25, 2012 breach would act as a catalyst for such a review. I believe that it is now overdue, and this will be addressed in my recommendations.

Issue 6: What actions, if any, should the government of Ontario take in response to this breach?

The Need for Privacy Audit Powers

The circumstances of this privacy breach are a cause of great concern, and, in my view, provide a reasonable basis for concluding that if an audit had been conducted on the personal information management practices of Elections Ontario prior to this incident, this breach may have been avoided.

Implementing policies, procedures and controls to ensure personal information is accorded appropriate protection is a critical component of good privacy management. While my office is willing to work with organizations that approach us for assistance in the development and implementation of appropriate policies and procedures, we do not have the authority to conduct an audit or a review on a proactive basis. This incident has demonstrated that at least one government organization in Ontario has failed to put in place reasonable measures to protect the privacy and security of personal information. This is one organization too many, and steps should be taken to ensure that this does not happen again.

In the context of an audit of personal information practices, organizational leaders can identify and ultimately seize opportunities to improve privacy protection in new or existing information management systems by taking a *Privacy by Design* or *Privacy by ReDesign* approach. Upon implementation, the goal is to render privacy as the default condition.

The growth in the use of electronic information management systems and the increasing number of identity theft cases calls for a proactive solution. Mandatory, organization-wide privacy audits will help to ensure that an organization is operating properly with respect to privacy and will help to reduce the risk of a privacy breach.

The general utility of organizational privacy audits has been recognized by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA), which have jointly published their *Generally Accepted Privacy Principles (GAPP) – A Global Privacy Framework* (the *GAPP Privacy Framework*).[17] The *GAPP Privacy Framework* was developed to assist organizations in identifying and managing privacy risks and serves as an excellent basis for conducting independent audits. I note that section 18(1) of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) confers an audit power on the Privacy Commissioner of Canada.

17 The *GAPP Framework* is available from the CICA'a website: **http://www.cica.ca/index.cfm/ci_id/36529/la_id/1**.

Within this province, the Office of the Auditor General has the specialized expertise to review public sector organizations and their compliance with a standard such as the *GAPP Privacy Framework*. Such a review could be conducted in cooperation with my office. Providing such audit powers does not mean that all public sector organizations will have their privacy practices reviewed. However, even auditing a cross-section of government agencies would provide valuable lessons for others.

I will therefore be recommending that the provincial government ask the Office of the Auditor General of Ontario to conduct privacy audits of information management practices of selected public sector organizations.

Review of the *Election Act*

Two fundamental concerns with regard to the *Election Act* arise from my office's investigation. First, the information lost includes electors' personal information (dates of birth and gender, and whether the individual had voted in the previous election) that is only available to political parties and MPPs through the PREO, and is to be used for electoral purposes only. This information is not available to the general public in any form. Second, the information lost was in electronic format which heightens concerns for its misuse, given the realities of the modern digital age. In light of Elections Ontario's privacy breach, it is important that the *Election Act* be reviewed and modernized to ensure that only necessary elector information is collected, and appropriate protections and oversight are in place to protect against improper uses of voter information, by both individuals and political parties. I will therefore be recommending that the Ontario government review the provisions of the *Election Act* to consider what changes need to be made to reflect the realities of the digital age, and to ensure that the personal information of electors is secured throughout the entire lifecycle of the data.

Conclusions

Through this investigation, I have arrived at the following conclusions:

Elections Ontario staff lost two USB keys containing the personal information of between 1.4 and 2.4 million Ontario voters, living in 20 to 25 electoral districts in Ontario. However, over 4 million voters were affected by this breach because although Elections Ontario determined that the personal information of voters in 20 to 25 districts were stored on the USB keys at the time of the breach, they were not able to identify which of 49 potential electoral districts, involving a total of 4 million voters, may have been involved.

Elections Ontario staff failed to put into place reasonable measures to protect the privacy and security of the personal information in their custody and control. In particular, Elections Ontario:

- failed to ensure that measures were in place in relation to the physical security of the Birchmount warehouse facility where the Strike-off Project was carried out;

- failed to ensure that measures were in place to protect the privacy and security of the personal information used by the Strike-off Project team; and
- failed to ensure that the personal information stored on mobile electronic devices was encrypted.

I have also found that Elections Ontario:

- failed to ensure that appropriate policies and procedures were in place to protect the privacy and security of personal information, including an agency-wide Privacy Policy and a Privacy Breach Protocol;
- failed to take steps to ensure that the existing policies were reflected in actual practice through the implementation of routine practices and procedures;
- failed to ensure that one or more senior staff were accountable and responsible for the privacy and security of personal information;
- failed to adequately train its staff to ensure that they understood and implemented the measures to be taken to protect the privacy and security of personal information; and
- failed to respond adequately to the privacy breach by continuing to store unencrypted data on USB keys, even after having learned of the earlier privacy breach.

Recommendations

In light of the conclusions contained in this Report, I have made the following recommendations.

Elections Ontario

I recommend that Elections Ontario take the following steps to enhance the protection of personal information in its custody and under its control. Specifically, Elections Ontario should:

1. Retain the services of an independent third party to conduct a thorough and comprehensive audit of all of the personal information management policies, practices and procedures at Elections Ontario.
2. In conjunction with the independent third party audit, develop an overarching privacy policy that applies to all aspects of Elections Ontario information management processes. At a minimum, this privacy policy must include specific direction on the appropriate use of mobile devices, including a requirement that any personal information stored on such devices be encrypted – identifying exactly what that means and who should be responsible for performing the encryption.

3. Establish Technology Services as the centre of responsibility and accountability at Elections Ontario for the implementation of strong measures to protect the privacy and security of personal information on all electronic devices, and for ensuring that staff are fully trained and supported regarding the use of these devices.

4. Appoint a senior manager within the organization as the Chief Privacy Officer to be responsible and accountable for all privacy-related matters, with the authority to approve any proposal or program impacting electors' privacy or their personal information.

5. Develop a comprehensive, mandatory privacy training program for:

    a. all temporary and full-time newly hired staff;

    b. all staff, on an annual basis.

6. Develop an ongoing communications plan to ensure that all staff are made aware and reminded of the organization's privacy and security protocols and policies.

7. Provide my office with a copy of the audit report, and any new or revised policies and procedures, for review and comment within six months of the date of this Report.

Government of Ontario

I recommend that the government of Ontario:

1. Ask the Office of the Auditor General of Ontario to conduct privacy audits of the information management practices of selected public sector agencies in the province.

2. Conduct a complete review and modernization of the *Election Act* to ensure that the privacy and security of personal information in the custody and control of Elections Ontario is strongly protected and used prudently, as prescribed.

Commissioner's Message

While Ontarians have the right to vote, they also have a right to assurances that when exercising their right to vote, their right to privacy will also be protected. Managing the electoral process, and the personal information collected as an essential part of that process, is the primary responsibility of Elections Ontario.

In the course of this investigation, I learned that the policies in place at Elections Ontario to protect the privacy and security of the personal information of Ontario electors were wholly inadequate. While there appeared to be a general recognition of the importance of privacy and security, for the most part, concerns about how personal information was managed tended to be directed outward to the recipients of information from the agency. The need for internal vigilance to protect personal information at the agency itself was not supported by robust policies or procedures. The need to protect the privacy and security of electors' information entrusted to Elections Ontario must become internalized and form part of the organizational culture.

Ultimately, at the root of the problems uncovered in the course of my investigation was a failure to build privacy into the routine information management practices of the organization. It should be a given that every organization that manages personal information must have comprehensive privacy policies in place. However, once these are developed, privacy policies must then be translated into actual practices and procedures in order to be effective. The best privacy policies are rendered meaningless if they do not translate into the fibre of an organization's operations, to guide the manner in which staff undertake their responsibilities. The existence of staff training and regular refreshers regarding the importance of privacy cannot be overstated in accomplishing this goal.

This privacy breach occurred as a result of two lost USB keys that contained the unencrypted personal information of a massive number of individuals. But my concerns with Elections Ontario's policies and procedures go beyond the need to develop practices to ensure that encryption is enabled as the default setting on all mobile devices. I believe that a complete review of the information management and IT practices throughout Elections Ontario is necessary. I remain committed to working with the Chief Electoral Officer to ensure that the privacy of Ontario voters is "baked" into its operations, not by chance, or by disaster – but by design. Given that *Privacy by Design* originated right here in Ontario, it would only stand to reason that this international framework for data protection, unanimously passed as a global standard in 2010, be followed in its own birthplace.

July 31, 2012

Ann Cavoukian, Ph.D.
Commissioner

Date

Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada
416-326-3333 1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca
Email: info@ipc.on.ca