PRIVACY MANAGEMENT IN CANADIAN ELECTION ADMINISTRATION: CURRENT STATE AND NEXT STEPS

Amie Mae Smith Foster, MPA candidate
School of Public Administration
University of Victoria
July 9, 2016

Client:	Dr. K. Archer Chief Electoral Officer of British Columbia (Elections BC)
Supervisor:	Dr. E. Lindquist School of Public Administration, University of Victoria
Second Reader:	Dr. K. Speers School of Public Administration, University of Victoria
Chair:	Dr. R. Marcy School of Public Administration, University of Victoria

ACKNOWLEDGEMENTS

About half-way through my program, my eldest son (then 6 years old and a budding scientist) asked me a random question about snake venom, to which I responded, "I'm not sure honey - we'll need to look that up." Without skipping beat, he replied, "Why not, you study all the time?" To my children - I love you to the moon and back, 852,672 times – I hope someday you will understand all of the bedtimes and sunny Sundays I missed.

Aaron - Thank you so much for giving me the support and the space to finish this program. You have pulled more than your weight over the last three years, and I will be forever grateful.

Dr. Keith Archer - Thank you for systematically removing every major barrier in my way. You encouraged me to apply, funded my scholarship, and sponsored this project. None of this would have been possible without you.

And finally, thank you to Dr. Evert Lindquist, Dr. Kimberly Speers and the many faculty members at the University of Victoria who have made this experience both challenging and worthwhile.

EXECUTIVE SUMMARY

Objective

Voting is often described as a public or "communal" act, and in Canada, less than 50 years ago voters lists were routinely nailed to trees and telephone poles for all to see and scrutinize. However, the field of privacy is constantly evolving, and privacy management programs must be rigorously and continuously maintained to reflect (real or anticipated) statutory and environmental change, public expectation and operational innovations. As a result, privacy management is an increasingly relevant subject for election administrators.

This study provides context for understanding the current state in privacy management in Canadian electoral management bodies (EMBs), and identifies opportunities for the development and implementation of good privacy management practices by answering the following questions: What are Canada's EMBs doing in this space, what common opportunities and challenges are these agencies facing, and what can Elections BC do to continue to improve its privacy management program?

Methodology and Methods

This report employs a mixed method approach to address the research questions. The qualitative approach was a literature review that explored the historical and foundational privacy principles emerging from academic and professional writing. The literature review also assessed the privacy material published by Canada's federal, provincial, and territorial EMBs regarding their privacy management programs. The final part of the research, the empirical, primary source data from Canada's Chief Electoral Officers (or their delegates) in the form of semi-structured interviews, was sought to allow for a better understanding of the state of privacy in Canada's federal, provincial, and territorial EMBs.

Findings and Analysis

There is a significant amount of useful information available to election administrators describing privacy program management and privacy principles. It was found that the resources all rest on the premise that privacy is about choice – the choice of individuals to choose when and how to expose their personal information to others.

While there are similarities, this research also found that there is great diversity between Canada's federal, provincial and territorial EMBs, and as a result, there is also a wide range of privacy management activities. While some jurisdictions have little or no program to speak of, others have formal and informal privacy management programs in place (or the beginnings of such programs). Almost all of this work was triggered by a series of highly publicised breaches emerging from Canada's EMBs between 2011 and 2013, and to a lesser degree, changes in statute and efforts to simply be proactive.

Despite their differences, this research has uncovered a series of common challenges experienced by agencies including the following:

- a need to dramatically increase their staffing complement in very short periods of time;
- the very high expectations from stakeholders for compliance;

- the highly distributed model of election administration;
- the need to balance privacy obligations and operational requirements;
- the need to adjust to new environmental, statutory and technological requirements;
- the need to acquire or develop expertise in this area;
- and the need to disclose personal information to electoral participants who may or may not have the capacity to maintain their own privacy management programs including political parties, elected officials, candidates and others.

The findings also demonstrated that privacy and digital issues constitute a rapidly evolving landscape, and that EMBs need to anticipate new issues and develop new capabilities as a result. Moreover, it was found that Elections BC's privacy management program should be rigorously and continuously maintained to reflect (real or anticipated) statutory and environmental changes, public expectations, and operational innovations. While Elections BC has a robust framework in place and is currently performing strongly in this space, in order to stay current and develop appropriate responses, the agency can benefit from participating in an ongoing national dialogue among Canada's EMBs on the subject of privacy.

Options and Recommendations

There are several options available to facilitate a national dialogue among EMBs on privacy management:

1. Share research informally through the Canadian Election Resource Library (CERL)
2. Develop a working group on information and privacy management
3. Encourage the addition of privacy on the agenda of annual conferences and meetings commonly attended by election administrators
4. Add privacy to the Canadian Society of Election Official Training curriculum
5. Develop a privacy network across all of Canada's EMBs

This research recommends the establishment of a national dialogue in the form of an informal privacy network across Canada's EMBs (Option 5 with Option 1) and the establishment of a formalized privacy training module that is specific to the election business (Option 4). Together these activities can help to ensure the client (and other Canadian EMBs) remain compliant with statute, are proactive in preventing breaches, and can effectively maintain public trust.

Conclusion

Most of Canada's EMBs have begun to consider privacy as an operational responsibility, and some, particularly the larger agencies are developing and/or maintaining mature privacy management programs in an effort to comply with statute, reduce risk and maintain public trust. These programs should be continuously maintained to address environmental and statutory changes. While each EMB's approach to privacy differs, they share similar challenges that are unique to election administration. In order to stay current and develop appropriate responses, the client (and other participating Canadian EMBs) can benefit from an ongoing formal and informal national dialogue on the subject of privacy.

Table of Contents

TABLE OF FIGURES

1. INTRODUCTION

Elections BC (EBC) is an independent and non-partisan office of the Legislative Assembly. It is led by Chief Electoral Officer Dr. Keith Archer, and is responsible for administering electoral events in British Columbia (Elections BC, n.d., "About"). In 2012, in acknowledgement of Elections BC's statutory responsibilities and significant breaches at other public agencies, Dr. Archer established a formal privacy program at Elections BC (K. Archer, personal communication, March 22, 2016). Elections Ontario established their own program that year, and other Canadian electoral management bodies (EMBs) have undertaken similar work in the intervening years (Elections Ontario, November 2012, Elections BC, August 2013 and M. Boda, personal communications, March 10, 2016).

The field of privacy is constantly evolving, and privacy management programs must be rigorously and continuously maintained to reflect (real or anticipated) statutory and environmental change, public expectation and operational innovations. This is true for election administrators and public administration more generally. Further, a series of breaches at Canada's EMBs between 2011 and 2013 "highlighted sharply what happens if there is no framework in place" (K. Archer, personal communication, March 22, 2016). This project is designed to help the client understand the current state of privacy management in Canada's election management bodies (EMBs), and to provide recommendations for keeping Elections BC's privacy management program current and effective.

This project is a continuation of Elections BC's privacy work and highlights the agency's commitment to sharing knowledge and to good privacy management practices by asking the following questions:

1. What are Canada's electoral management bodies (EMBs) doing in this space?
2. What common opportunities and challenges are these agencies facing?
3. What can Elections BC do to improve their privacy management program?

These questions are addressed by reviewing academic and professional literature, and publicly available information on privacy management as it relates to election administration, and by conducting personal interviews with Chief Electoral Officers (CEOs) and/or their delegates from Canada's federal, provincial and territorial EMBs. It consolidates the learning from these methods into options and recommendations that support the client's need to further their privacy program.

This report starts by providing the reader with background information on the client and its context, and then describes, in greater detail, the research methodology. It includes a literature review and outlines the results gathered from interviews with senior election administrators from across the country. The findings inform possible recommendations for next steps.

2. BACKGROUND

This section provides context for this research report. It begins with a description of the project client, and then provides comprehensive contextual information related to election administration, and the emergence of information privacy in Canada. It closes with a description of how these subjects converge, and why this research is important to Canada's election administrators.

2.1 Project Client

The project client is Dr. Keith Archer, Chief Electoral Officer (CEO) of British Columbia. Dr. Archer is an independent officer of the Legislative Assembly responsible for administering provincial general elections, by-elections, referenda, plebiscites, initiative petitions, initiative votes, recall petitions and other on-demand events as well as local election campaign finance rules. Dr. Archer was appointed by the Lieutenant Governor on the recommendation of the Legislative Assembly in 2011 following the unanimous recommendation of an all-party committee. His appointment as CEO and head of Elections BC is for a fixed term - two provincial general elections plus one year (Elections BC, n.d.). Prior to his appointment as CEO, Dr. Archer was a Professor of Political Science at the University of Calgary and Director of Research at the Banff Centre where his teaching and research focused on the study of elections and voting (Elections BC, n.d.).

The CEO is supported by approximately 55 permanent staff. To prepare for and administer elections, the CEO and permanent staff can be supported by up to 38,000 temporary Elections BC staff. The CEO is guided by several provincial statutes: the *Election Act* (1996), the *Local Elections Campaign Financing Act* (2014), the *Local Government Act* (1996), the *Recall and Initiative Act* (1996), the *Referendum Act* (1996), the *Constitution Act* (1996), and the *Freedom of Information and Protection of Privacy Act* (1996).

2.2 Election Administration and Privacy Issues: Defining the Problem

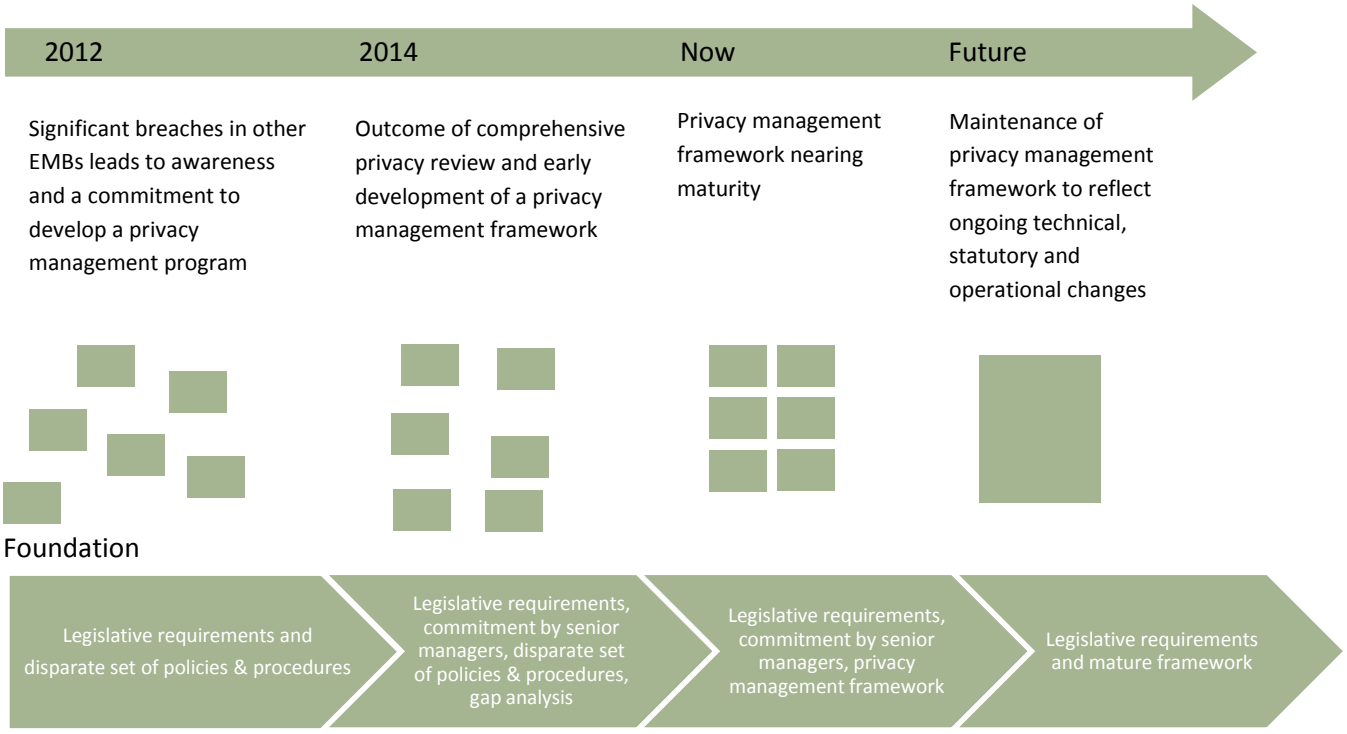
In mid-2012 following breaches at several election and other public agencies, Dr. Archer established a formal privacy program at Elections BC. With a provincial general election less than a year away, the agency chose to address only critical risks, and develop a project plan for a comprehensive privacy project beginning immediately after the event. This commitment was captured in the agency's annual service plan (Elections BC, 2013, p.9).

Elections BC then commissioned David Loukidelis, B.C.'s former information and privacy commissioner to assess the agency's compliance with information and privacy obligations by completing a comprehensive review of the agency's policies, procedures, training and contracts, and by conducting an inventory of all of Elections BC's personal information holdings. The resulting recommendations and guidance for establishing an accountable privacy management plan were contained in an internal report entitled *Privacy Management Plan for Elections BC: Report & Recommendations* (Loukidelis, 2014). This report reinforced the general recommendations for public bodies set out in *Accountable Privacy Management in BC's Public Sector* (Office of the Information and Privacy Commissioner of British Columbia, n.d.) and established a large number of more granular activities to support compliance, including specific updates to guides, forms, processes, procedures, and the agency's websites. The second phase of this project addressed each recommendation in a methodical way to ensure the program was fully operational before the 2017 provincial general election planning began in earnest.

Elections BC has a robust privacy program in place. Its privacy framework (a central repository of all of the agency's privacy policies and programs) has been lauded by BC's Information and Privacy Commissioner as an example for other public agencies and Elections BC serves as a leader in this subject area among Canada's EMBs. Elections BC staff now proactively discuss privacy obligations alongside other operational requirements, their framework is updated frequently to respond to changes in the internal and external environment and they have two individuals certified by the International Association of Privacy Professionals on staff.

The next year will be challenging and will include a boundary redistribution, a targeted enumeration, and a provincial general election which will require the agency to continue to balance operational and privacy obligations. Despite Elections BC's significant investment in privacy management over the last several years (See Figure 1, below), there is an acute awareness among the agency's senior leaders that the field of privacy is constantly evolving. The program should be rigorously and continuously maintained to reflect (real or anticipated) changes in statute, environmental changes including public expectation and new technological developments, and operational innovations. This study continues Elections BC's privacy work and highlights its commitment to sharing knowledge and to good privacy management practices.

Figure 1 – Elections BC: Moving toward a Formalized Privacy Management Framework



2.3 Election Administration in Canada: Current State

Elections BC is one of 14 agencies across Canada at the federal, provincial and territorial level which are responsible for election administration. Canada has a strong international reputation for "professional, independent and non-partisan" election management (Balasko, 2015, p. 65) led by electoral management bodies (EMBs) which are defined by Catt, Ellis, Maley, Wall and Wolf (2014, p. 5) as:

> *"…an organization or body that has the sole purpose of, and is legally responsible for, managing some or all of the elements that are essential for the conduct of elections and direct democracy instruments—such as referendums, citizens' initiatives and recall votes—if those are part of the legal framework. These essential (or core) elements include:*
>
> *a. determining who is eligible to vote;*
> *b. receiving and validating the nominations of electoral participants (for elections, political parties and/or candidates);*
> *c. conducting polling;*
> *d. counting the votes; and*
> *e. tabulating the votes."*

In addition to these activities, EMBs may also "…undertake other tasks that assist in the conduct of elections and direct democracy instruments, such as voter registration, boundary delimitation, voter education and information, media monitoring and electoral dispute resolution" (Catt et al., 2014, p. 5-6).

There are three broad electoral management models governing EMBs which are distinguished by their "degree of structural independence from executive government and freedom to manage (Balasko, 2015, p. 67). They include the independent model in which elections "are organized and managed by an EMB that is institutionally independent and autonomous from the executive branch of government", the government model in which elections "…are organized and managed by the executive branch through a ministry," and a mixed-model which includes a "…policy, monitoring or supervisory EMB that is independent of the executive branch… and an implementation EMB located within a department of state and/or local government" (Catt et al., 2014, p. 7-8). In Canada, statute in all 14 federal, provincial and territorial jurisdictions has established an independent EMB led by a CEO.

In 2015, Richard Balasko, the former CEO of Manitoba published "The Nature and Functions of Electoral Management Bodies" in the *Informed Citizens' Guide to Elections: Electioneering Based on the Rule of Law*, a special edition of the *Journal of Parliamentary and Political Law*. He sets the context for how elections are administered in Canada. Specifically, he explains that "the functions performed by electoral management bodies rest upon two main pillars, namely the legal framework as well as normative imperatives." Legal frameworks can change over time and provide prescriptive guidance to election administrators in areas such as elections, campaign finance, and electoral redistribution, while normative functions "relate to the qualities or attributes of an independent and non-partisan electoral management body" (p. 66-70). Importantly Balasko explains that the extent to which these functions are met will directly affect whether the agency is seen as credible, and this can have a knock-on effect on the legitimacy of the jurisdiction's political institutions (pp. 65-66).

2.4 The Rise of Information Privacy

Like many other public organizations, EMBs have had to pay close attention to balancing the privacy concerns of citizens with their operational responsibilities. Canada's courts have "recognized privacy as a fundamental right protected by Sections 7 and 8 of the Canadian Charter of Rights and Freedoms (1982)" and some have argued that "privacy in relation to one's personal information is essential to ensure the basic dignity and integrity of the individual" (Privacy Commissioner of Canada, 2005, Preface). Further, Canada and other Western industrialized nations are working to "balance protection of their citizens' personal information with governmental interests in national security and promotion of commercial competitiveness". It is these efforts that are driving the body of law known as the "International Data Privacy (IDP) regime (McLennan and Schick, 2007, p. 669). An IPD regime "attempts to reconcile the rights and conduct of three major actors in this regime: governments, businesses and the individuals whose information is gathered, stored or traded" (McLennan et al., 2007, p. 669).

The United States and Europe have taken different approaches in this context, and Canada, as a result of the EU Data Privacy Directive (1995), more closely resembles the European Union's comprehensive data protection model. This model favours the individual's rights over those of the corporation (McLennan et al., 2007, p. 669) and establishes data protection laws "which govern the collection, use and dissemination of personal information in the public and private sectors" (Swire and Ahmad, 2012, p. 31). Under this model, every federal, provincial and territorial jurisdiction in Canada has a Data Protection Authority (DPA) who is responsible for overseeing enforcement by ensuring compliance, investigating breaches, and educating the public on data protection issues (Swire et al., 2012, p. 31).

The EU Data Privacy Directive (1995) is one of the most important documents for developing an IDP regime as it set comprehensive requirements for exporting data from the European Union. It has forced other nations, including Canada, to "reconsider, or consider for the first time, their positions and attitudes toward data privacy" (McLennan et al., 2007, p. 670). Canada had privacy laws in place before the EU Directive (1995), including the federal *Privacy Act* (1985) which regulated public entities' treatment of personal information, and Quebec's *Act Respecting* Access to Documents Held by Public Bodies and the Protection of Personal Information (1982). However, these laws were insufficient to meet the requirements of the EU Directive (1995) (McLennan et al., 2007, p. 671). Canada subsequently passed the *Personal Information Protection and Electronic Documents A*ct (PIPEDA) which was adopted in 2000 and implemented gradually through 2004 (Klein, 2012, p. 23). PIPEDA established a "national standard for protection of individuals' data across virtually all private industries" and demonstrated "…the federal government's commitment to securing Canadian Citizens' personal information" (McLennan et al., 2007, p. 671).

2.5 Context: Convergence of Election Administration and Privacy

Section 2.3 established that the extent to which EMBs' legal and normative imperatives are met will have a direct effect on whether the agency is seen as credible, and this will affect the perceived legitimacy of the jurisdiction's political institutions (Balasko, 2015, pp. 65-66). This research argues that the protection of privacy (or lack thereof) in the context of election administration is important because it can impact both pillars. From a legal framework point of view, every federal, provincial and territorial jurisdiction in Canada is governed by a Data Protection Authority (DPA) and statute governing the use of personal information. From a normative perspective, privacy protections may be even more important - research related to privacy in the voting place has found that "a lower sense of privacy is strongly

associated with lower voter confidence" and a decreased sense that the outcome of the election was fair (Karpowitz et al., 2011, p. 661).

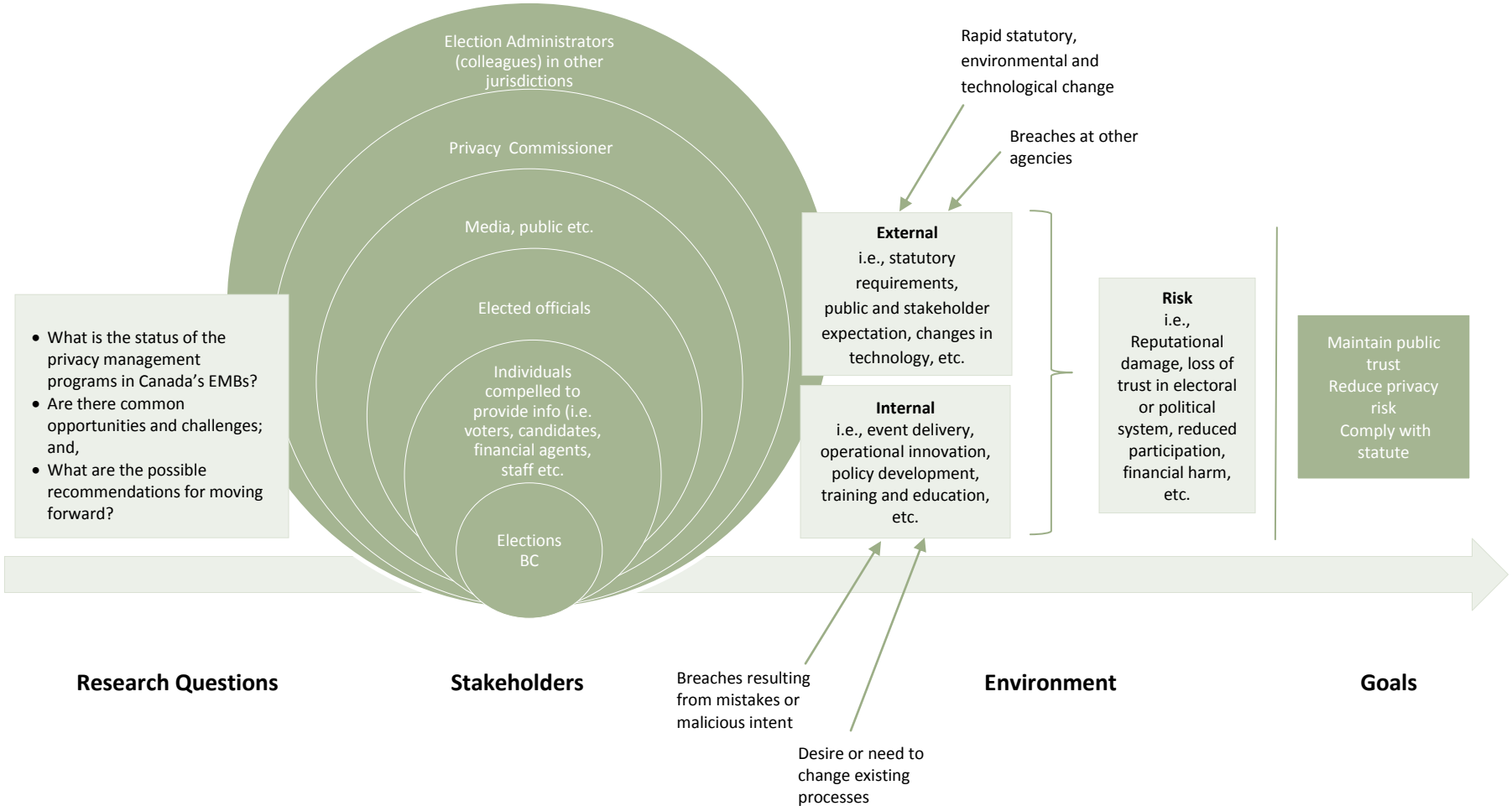
The unique responsibilities of election administrators are to: determine voter eligibility; receive and validate the nominations of electoral participants; administer voting; and, conduct voter registration activities through enumeration and other activities presents unique privacy challenges for EMBs. In order to participate in democratic processes individuals are compelled to share personal information with the EMB. These agencies then hire (sometimes) tens of thousands of temporary staff each with some responsibility for data processing to deliver the event. For example, Elections Canada added 285,000 temporary staff to their payroll in advance of the 42nd Federal General Election (A.M Delisle, personal communication, June 22, 2016), Elections Ontario hires 80,000 temporary staff (G. Essensa, personal communication, April 28, 2016) and in British Columbia one in every 125 of its 4.5 million residents are employed by Elections BC in the days and weeks surrounding a provincial general election (K. Archer, personal communication, March 22, 2016). These staff receive a few hours of training and their employment is typically counted in days rather than weeks or months. This example represents just one of the many unique challenges that is explored as part of this research.

Privacy and digital issues constitute a rapidly evolving landscape, and EMBs must anticipate new issues and develop new capabilities as a result. This research seeks to better understand how other similar agencies are managing their privacy portfolios in the unique context of election administration, and to provide some guidance on how Elections BC can continue to mature its privacy management program to ensure that the agency is compliant with statute, proactive in preventing breaches, and can effectively maintain public trust associated with its information privacy practices. As such, this research looks at the convergence of election administration and privacy by seeking to answer the questions: What are Canada's EMBs doing in relation to privacy? What common opportunities and challenges are these agencies facing in this portfolio? And, what can Elections BC do to improve their privacy management program?

2.6 Analytic Framework and Focus of this Study

Figure 2 (below) sets out the analytic framework guiding this project. As demonstrated, the research question is defined by carefully assessing the forces driving information and privacy work at Canada's EMBs, the issues that can arise from inaction, the stakeholders with an important voice, and the client's strategic goals. Additional details regarding how the research question(s) will be answered can be found in the next section entitled "Methodology and Methods."

Figure 2 – Analytic Framework



3. METHODOLOGY AND METHODS

Privacy and digital issues constitute a rapidly evolving landscape, and a privacy framework, regardless of how robust, must continuously evolve to address emerging environmental and statutory changes. The empirical focus of this study is to understand what other similar EMBs are doing to address their privacy obligations and what guidance is available in the form of publicly available reports and other sources to address for the client how they can continue to mature their privacy management program in a way that is compliant with statute, proactive in preventing breaches, and effective in maintaining public trust associated with its information privacy practices.

The sections below provide a thorough description of the methodology and methods used in this research study, as well as the project's identified strengths, limitations and risks.

3.1 Methodology

This is a mixed-methods qualitative research project that references both documents and interviews in an effort to answer the questions, "What are Canada's EMBs doing with respect to privacy, what common opportunities and challenges are these agencies facing, and what can Elections BC do to improve their privacy management program? The research is designed to support a comprehensive exploration of the research questions while respecting smart or wise practices in qualitative research (Tracy, 2010, p. 840).

The literature review was designed to explore the historical and foundational privacy principles emerging from academic and professional writing, as well as to assess what Canada's federal, provincial and territorial EMBs publish regarding their privacy management programs (by reviewing their websites).

The final part of the research was empirical and sought primary source data from Canada's CEOs or their delegates to better understand the information and privacy work currently underway, the work planned in the near and long term, and the challenges and opportunities they are facing in this arena. Together, the literature review and the interviews inform the project's recommendations. The sections below provide additional detail and a description of the study's strengths, limitations and risks.

3.2 Literature

The literature review (secondary data collection) involved a review of published academic research and writing, statutes, and publicly available reports produced by Canada's Information and Privacy Commissioners and CEOs. This effort supported the development of a high-level understanding of the subject area and identified knowledge gaps for the semi-structured interviews that followed.

Key search terms included privacy, privacy framework, election administration and privacy, privacy best practices, privacy management, privacy by design, privacy for public bodies, privacy breach, and privacy breach response. Research was conducted using advanced search options at the University of Victoria library and Google Scholar, on EMB and data protection authority websites, and through consultation with the project client and senior staff at Canada's EMBs.

3.3 Jurisdictional Scan

In Canada, statute in all 14 federal, provincial and territorial jurisdictions has established an independent EMB led by a CEO. A jurisdictional scan by way of a comprehensive review of the websites in each jurisdiction was conducted to assess what information each federal, provincial and territorial agency publicly discloses regarding their information and privacy programs. This effort focussed on references to policies, resources, general information and tools related to information privacy and access to better understand what these agencies are sharing about their privacy management efforts.

3.4 Interviews

Interviews as a primary research method were designed to gather information regarding the information and privacy work underway at Canada's EMBs, the work planned in the near and long term and the challenges and opportunities they are facing in this arena. CEOs (or their delegates) from all of Canada's 14 EMBs were identified as the best source of this information.

The initial invitations were delivered via email in February 2016 (see Appendix A) and a follow-up email was sent in March 2016 (see Appendix B). A follow-up telephone call was made to the remaining agencies in April 2016. In the end, nine of Canada's 14 EMBs agreed to participate including Elections Alberta, Elections BC, Elections Canada, Elections Manitoba, Elections Newfoundland and Labrador, Elections Nunavut, Elections Ontario, Elections Quebec and Elections Saskatchewan (see Appendix C for the interview script, Appendix D for the consent form, and Appendix E for a detailed list of individuals invited to participate in this research, including their interview status, name, jurisdiction and participation date).

The agencies that agreed to participate are reasonably representative of Canada's federal, provincial and territorial EMBs including representatives from Alberta, British Columbia, Canada, Manitoba, Newfoundland and Labrador, Nunavut, Ontario, Quebec and Saskatchewan. They represent some of the largest and some of the smallest agencies, as well as some mid-sized agencies. There are participants from: the federal, provincial and territorial levels; English and French speaking Canada; and western, central, eastern, northern and Atlantic Canada. They also include some of the "early adopters" of privacy programs, including Elections Canada (A. M. Delisle, personal communication, March 22, 2016) and Elections Ontario (G. Essensa, personal communication, April 28, 2016), and others working in that direction now, including Elections Saskatchewan (M. Boda, personal communication, March 10, 2016) and Elections Manitoba (S. Verma, personal communication, March 23, 2016). The study also includes agencies that have experienced highly publicised privacy breaches including Elections Alberta, Elections BC, Elections Ontario, Elections Quebec, and Elections Canada (see section 4.9 Triggering Incident) and Newfoundland and Labrador which is governed by recently updated privacy statute (Executive Council, 2015, June 1).

Semi-structured interviews were chosen as the most appropriate structure as they could be "…organized around a set of predetermined open-ended questions, with other questions emerging from the dialogue between interviewer and interviewee" (DiCicco-Bloom and Crabtree, 2010. p. 315). Questions posed in the interviews were designed to both expand on themes identified in the literature and address identified gaps. The interviews were semi-structured to introduce some consistency while also allowing for some room for the interviewees to provide additional detail regarding their experiences and/or

thoughts on the emergence of privacy, their privacy efforts, their future plans and the opportunities and challenges presented by this portfolio. The interviews also sought information regarding the trigger or call to action to begin this work.

Participants' responses were attributed with consent as part of this research and a late draft of this report was shared with interview participants at their request to confirm consent for attribution.

3.5 Data Analysis

The data from the literature review and the interviews were analyzed separately to assess common themes, patterns and if necessary, outliers. Each line of evidence contained unique themes and did not necessarily overlap. The literature review was designed to assess the subject of privacy from a historical, theoretical and foundational perspective. The interviews were focused on the practical implications of privacy in a real-world context (see Figure 3 – Methods and Methodology). The two streams were complementary and were combined to develop the findings found in sections 4-6 of this report.

Figure 3 – Methods and Methodology

3.6 Project Strengths, Limitations and Risks

This project's greatest strengths were the general knowledge and context produced by the literature review and the EMB specific information resulting from the interviews. The combined benefit of these methods resulted in a comprehensive resource for election administrators that describes what Canada's EMBs are doing in this space, what common opportunities and challenges these agencies are facing and what Elections BC can do to improve their privacy management program.

Limitations associated with this project included the inability of some of Canada's EMBs to participate in the research due to operational demands. Others explained that their privacy management efforts were limited at the time the research was conducted and as such they could not effectively contribute. As a result, nine of 14 federal, provincial, territorial (FPT) EMBs participated in this research.

There are four primary delimitations associated with this project. First, this report focuses on privacy management in election administration at the FPT level – it does not assess privacy efforts at the municipal level in Canada, or efforts underway by political parties and/or candidates. Second, due to language barriers, French language resources could not be included in this study. Third, this research did not seek to obtain more information on the facts of publicly reported breaches, or to reveal any further breaches. Instead, publicly reported breaches were used as the starting point in assessing why a focus on privacy is important. Finally, feedback regarding the training materials appended to this research was not sought during this course of study. As a result, there is no ability to evaluate the efficacy of these materials.

Risk to research participants has been carefully considered. The research protocol has been reviewed and approved by the Human Resources Ethics Board (HREB) at the University of Victoria which determined that "in all respects, the proposed research meets the appropriate standards of ethics as outlined by the University of Victoria Research Regulations Involving Human Participants." (Human Research Ethics Board, 2016, February 16).

This research acknowledges the risk of research bias as the researcher is also an employee of Elections BC. Further, one of the interview subjects, and the project client is also the researcher's supervisor. Finally, and also due to the researcher's employment, the researcher was acquainted with all of the interview participants prior to the commencement of the research. These risks were mitigated through transparency and a shared acknowledgement of the need to guard against such bias.

4. FINDINGS: LITERATURE REVIEW

The sections below provide the information gathered as part of the literature review (secondary data collection). This review included published academic research available through the library at the University of Victoria as well as statutes, and publicly available reports produced by Canada's Information and Privacy Commissioners and CEOs. It provides an overview of the field of information and privacy, using both academic and professional resources.

It begins with some definitions and theoretical perspectives on why information and privacy is relevant for public bodies, and explores information and privacy recommendations for election and other public agencies. Key search terms included privacy, privacy framework, election administration and privacy, privacy best practices, privacy management, privacy by design, privacy for public bodies, privacy breach, and privacy breach response. Research was conducted using advanced search options at the University of Victoria library and Google Scholar, on EMB and data protection authority websites, and through consultation with the project client and senior staff at Canada's EMBs.

4.1 Terminology

The terms "personal information", "sensitive personal Information", "data processing" and "privacy "can be understood differently depending on context, culture, and other factors (Swire and Ahmad, 2012, p. 4-5). The definitions below provide reference for these terms as they relate to this research.

In Canada, **personal information** is typically defined as "…information about an identifiable individual, but does not include certain business contact information" (Swire and Ahmad, 2012, p. 4). This could include, but is not limited to, street address, telephone number and email address, etc., and it includes paper and electronic records (Swire and Ahmad, 2012, p. 5). **Sensitive personal information** is a subset of personal information, and is specific to jurisdiction and regulation (Swire and Ahmad, 2012, p. 5). In Europe, sensitive personal information can include "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life" and in the United States, sensitive personal information includes social security numbers, financial information, driver's licence information and health information (Swire and Ahmad, 2012, p. 5). In Canada "any information can be sensitive depending on the context" (Swire and Ahmad, 2012, p. 5).

Common examples of personal and sensitive personal information processed by Canada's EMBs include payroll and personnel records; mailing or physical address; social insurance number; political contributions (although some may be publicly available by statute); investigations case file information; banking information; birthdate; gender; phone number; email address; driver's licence number; social insurance number; electoral participation data etc. (Elections Canada, 2015, August 30).

Data processing relates to how data are used, and it is defined by the International Association of Privacy Professionals as:

> *"Any operation or set of operations which is performed on personal data, such as collecting; recording; organizing; storing; adapting or altering; retrieving; consulting; using; disclosing by transmission, dissemination or otherwise making the data available; aligning or combining data, or blocking, erasing or destroying data. Not limited to automatic means."*

This research refers to processing and/or data processing in this context.

Privacy is another term that is defined differently depending on the context. Swire and Ahmad (2012) have distilled the concept of privacy to:

> *"…the desire of people to freely choose the circumstances and degree to which individuals will expose their attitudes and behavior to others. It has been connected to the human personality and used as a means to protect an individual's independence, dignity and integrity" (p. 1).*

This definition is particularly interesting and useful in a culture where election administrators are finding that "people are more comfortable sharing personal information on Facebook, than with [them]" (S. Verma, personal communication, March 23, 2016). It is also interesting in this context as electoral participation involves the collection of data that is statutorily disclosed to political parties, candidates elected officials, and others, and when combined with other private or commercial data could be used to develop comprehensive profiles about voter attitudes and behaviors (Bennett, 2015).

Kris Klein (2012) distinguishes information privacy (information about an individual) from privacy of the person (bodily integrity) and territorial privacy (environment privacy including home and workplace). This research is concerned with **information privacy** which is fully defined as:

> *"…the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. Its protection is predicated on the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain as he sees fit…" (p 1-2).*

These definitions demonstrate that privacy is about choice – the choice of individuals to choose when and how to expose their personal information to others.

4.2 Origins of Privacy

Klein (2012) describes the "origins of privacy" as "…rooted in some of the oldest religions, texts and cultures known" and acknowledges the presence of references to privacy in classical Greece and ancient China, as well as to European laws dating back to 1361 (p. 2-3). Klein (2012) also connects privacy to human rights with the establishment of privacy rights in the United Nations' Declaration on Human Rights (1948), the Organization of American States' American Declaration of the Rights and Duties of Man (1948), and the Council of Europe's European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) (p. 2-3). He adds that modern concepts of information privacy and concern for collection and handling of personal information have emerged from the advent of information technology and "…the abuses that characterized the era of the Third Reich in postwar Germany" (p. 3). Contemporary concepts of privacy were founded in the 1960s and 1970s, and the "demand for formal rules governing the collection and handling of personal information grew as powerful new computer systems with increased surveillance potential were developed" (p. 3).

While there are several models for data protection, Canada has adopted comprehensive privacy laws similar to the laws in Europe which "govern the collection, use and dissemination of personal information in the public and private sectors" (p.4). In Canada, these laws are enforced in every provincial and federal jurisdiction (Office of the Information and Privacy Commissioner of Canada, "Provincial Privacy Laws", para 6) by a commissioner or ombudsperson who is responsible for ensuring

compliance, investigating alleged breaches of the Acts they administer, and "acting as a liaison for data protection issues" (Klein, 2012, p. 4-5). It is the latter responsibility that has led Canada's information and privacy commissioners to develop tools and resources for public and private organizations.

4.3 Foundational Principles

Several foundational principles serve as the basis for all modern privacy regimes (Klein, 2012) including: the Council of Europe Convention (1981), the European Data Protection Directive (1995), the APEC Privacy Framework (2004), the Madrid Resolution (2009) and others (Swire and Ahmed, 2012, p. 18-22). For simplicity, the two most significant Canadian contributions to this thinking have been included here.

Firstly, the Canadian Standards Association's (CSAs) "Model Code for the Protection of Personal Information (1996) calls for ten privacy principles (Klein, 2012, p. 19-20) including accountability; identifying purposes; consent; limiting collection; limiting use; disclosure and retention; accuracy; safeguards; openness; individual access; and, challenging compliance. Each principle is defined in detail in Figure 4 (see next page). The principles were influenced by a similar set of principles published in 1981 by the Organization for Economic Cooperation and Development entitled the "Guidelines Governing the Protection Privacy and Transborder Data Flows of Personal Data." Ultimately, fundamental principles such as these underlay all modern privacy regimes (Klein, 2012, p. 19-20).

In *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* (Cavoukian, 2012) reinforces the CSA's principles and issues seven principles of "privacy by design," a concept which calls for agencies to "[embed] privacy into information technologies, business practices, and networked infrastructures as a core functionality, right from the outset…intentionally, with forethought" (p. 8). Privacy by design principles include:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

These foundational principles have some minor variation but all call for similar protections with varying levels of detail (Swire and Ahmed, 2012, p. 18-22). Ultimately, they serve to form an important building block to all privacy management programs.

Figure 4 – Canadian Standards Association's Model Code for the Protection of Personal Information

1. **Accountability**. An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. **Identifying Purposes**. The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent.** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate.
4. **Limiting Collection**. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention.** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
6. **Accuracy.** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards.** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness**. An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access.** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance.** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Note: Reprinted from Canadian Privacy: Data Protection Law and Policy for the Practitioner (Second Edition). Copyright 2012 by International Association of Privacy Professionals.

4.4 Privacy Management Programs – Expectations for Public Agencies

There are a large number of publicly available resources published by Canada's DPAs designed to guide the work of public (and private) bodies in the area of information and privacy. These tools emerge from an obligation for Canada's DPAs to act as a liaison for data protection issues (Klein, 2012, p. 4-5). There are also published materials on effective program management more generally. While not exhaustive, the documents described below identify several useful themes.

In 2012, the Offices of the Information and Privacy Commissioners of Alberta, BC and Canada, produced a joint report entitled *Getting Accountability Right with a Privacy Management Program*. In it they explain that "an accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program (p. 1). They add that when implemented, such programs provide a number of benefits - they assist organizations in demonstrating that they are compliant with statute (and policy), they foster a culture of privacy within the organization, they help ensure effective resourcing for "training and education, risk assessment and monitoring, and auditing", and they enhance the agency's trust and reputation (p. 4).

The report defines accountability as "the acceptance of responsibility for personal information protection" (p.1) and lays out a series of steps for achieving accountability for personal information. See Figure 5. The report concludes by stating that "accountable organizations are able to demonstrate that they have a comprehensive privacy management program in place" (p. 18).

Figure 5 – Steps for Achieving Accountability for Personal Information

Developing a Comprehensive Privacy Management Program	• Organizational commitment • Internal governance structure • Buy-in from senior leaders • Effective resourcing • Designated privacy officer/office • Reporting mechanisms to ensure staff understand obligations • Internal audit programs to monitor compliance • Reporting escalation process
Program Controls	• Develop a personal information inventory • Develop and document internal policies • Work-specific training and education for all staff • Breach and incident management response protocols • Service provider management • Transparency - Inform individuals of privacy rights and organizational privacy controls
Ongoing assessment and revision	• Maintain the privacy management program by assessing and revising program controls (regularly update the data inventory, policies, privacy impact assessments, training, breach management, and communications tools)

Note: Adapted from *Getting Accountability Right with a Privacy Management Program by* the Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, retrieved from https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf, Copyright 2012.

Program management is typically driven by internal and external pressure to change (Thiry, 2010, p. 31), and this context is no different. Privacy program management, like all program management is cyclical, and aims to address pressures from strategy development through operational improvements, performance measurement, and in some cases further operational improvements to address "issues created by the realization of these objectives or new developments" (Thiry, 2010, p. 31). *Accountable Privacy Management in BC's Public* Sector is a manual for implementing such a privacy management program for public bodies, with a foundational principle that privacy should be designed in to every program, initiative or service from the outset (Office of the Information and Privacy Commissioner of British Columbia, n.d.). It also calls for public bodies to keep their privacy management programs current, and to make privacy management part of their "routine" operational work (p.2).

While this manual acknowledges that there is no one-size-fits-all for privacy management, it calls for every public body to provide evidence of a privacy management program in the event of a breach, and lays out a series of general recommendations. These recommendations call for public sector agencies to effectively resource privacy management programs; to appoint a privacy officer; to evaluate and report on compliance on an ongoing basis; to develop a response and escalation plan in the event of a breach; to document and demonstrate compliance with privacy statute; to conduct privacy impact assessments for new or changed programs; to conduct mandatory and job-specific privacy training; to hold contractors accountable for compliance with the agency's privacy management program and privacy statute; and, to be transparent about the collection, use and disclosure of personal information and individual privacy rights.

Another example is Densmore's (2013) *Privacy Management Program: Tools for Managing Privacy within Your Organization* which established a series of core tenants of privacy program management including strategic management (i.e. a vision, a strategy and a team); policies; standards and guidelines; performance measurement and assessment; data protection and lifecycle management; ongoing monitoring and maintenance; and effective response to information requests; legal compliance; and finally, a plan for incident handling.

This list of resources, while not exhaustive, demonstrates ongoing and similar efforts by DPAs in different jurisdictions to guide agencies in this arena. Common themes and recommendations emerging from these resources include a call to develop an accountable, evergreen, and well-resourced privacy management program as part of the agency's ongoing operational work; to design privacy into activities, projects and programs from the outset; to appoint a privacy officer; to evaluate and report on compliance; to develop a breach response plan; to develop an inventory of personal information holdings; to implement and communicate privacy policies; to conduct privacy impact assessments for new or changed programs; to initiate training and education with staff and contractors; and, to be transparent with clients and stakeholders about how their information is used, and what their rights are.

4.5 Ensuring Compliance – Findings of Canada's Data Protection Authorities

In addition to acting as a liaison for data protection issues (Klein, 2012, p. 4-5) Canada's information and privacy commissioners (or ombudspersons) must ensure compliance and investigate alleged breaches of the Acts they administer. This responsibility drove the production of Ann Cavoukian's (2012) *Elections Ontario's Unprecedented Privacy Breach: A special Investigation Report.* It described how Elections Ontario had emerged from a provincial general election with a minority government and as a result the agency was obliged to concurrently close-out the 2011 Provincial General Election while also preparing for a possible "snap" provincial general election. One of the primary "close-out activities" was the voters list strike off project which would see the Permanent Register of Electors for Ontario (PREO) updated to reflect new information gathered during the most recent event. A decision to do this work off-site was made, and because the secondary work space was not connected to Elections Ontario's servers, USB keys were used to transfer the updates between the temporary site and Elections Ontario headquarters. On April 26, 2012, Elections Ontario staff discovered that two unsecured and unencrypted USB keys were missing, and a significant effort to locate the keys was undertaken. After a comprehensive investigation involving the agency, an investigation firm, the Ontario Provincial Police and the Information and Privacy Commissioner, the agency failed to locate the missing USB keys (Cavoukian, 2012).

Cavoukian's (2012) report following this incident issued seven recommendations and marked a critical milestone for Canada's election administrators, as it was the first time that a Canadian information and privacy commissioner (and fellow independent officer of the Legislative Assembly) had issued a public report containing privacy recommendations specific to an EMB. The recommendations called for Elections Ontario to (p. 25):

- 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.

- 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.
- Establish Technology Services as the center 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.
- 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.
- Develop a comprehensive, mandatory privacy training program for: all temporary and full-time newly hired staff; all staff, on an annual basis.
- 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.
- 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.

Following the publication of Cavoukian's report, Elections Ontario took immediate steps to develop a comprehensive privacy program. It commissioned Deliotte to assess their privacy strengths and weaknesses (Elections Ontario, November 2012, and G. Essensa, personal communications, April 28, 2016). Their efforts were followed closely by Elections BC (Elections BC, August 2013) and David Loukidelis, B.C.'s former information and privacy commissioner, was commissioned to assess Elections BC's compliance with its information and privacy obligations.

Loukidelis' (2014) report included a comprehensive review of the agency's policies, procedures, training and contracts, and an inventory of all of Elections BC's personal information holdings. This report reinforced the general recommendations for public bodies set out in *Accountable Privacy Management in BC's Public Sector* (Office of the Information and Privacy Commissioner of British Columbia, n.d.) and also established a large number of more granular activities to support compliance, including specific updates to guides, forms, processes, procedures, and the agency's websites.

Canada's information and privacy commissioners (ombudspersons) have a statutory obligation to ensure compliance and investigate alleged breaches of the Acts they administer. Cavoukian's (2012) report, and Loukidelis' (2014) subsequent report provide useful guidance for this research.

4.6 Other Reports of Interest

Elections Canada maintains a Compendium *of Election Administration in Canada: A Comparative Overview.* The introduction presents this compendium as

> "…a comprehensive summary of the federal, provincial and territorial electoral frameworks. It is based on the legislation in force and does not include administrative practices not mentioned in

> the law with the exception of the section concerning advisory committees of political parties. The Compendium covers most major elements of the electoral process, including the redistribution of electoral boundaries, the administration of elections, the registration of electors, the voting process, the nomination and registration of political entities, election financing and advertising, enforcement of the legislation, and referendums, plebiscites, recalls and initiatives" (August 2015, p. 5).

This report serves to illustrate that there are vast differences between agencies due to their statutes and/or the way they operationalize their statutory obligations.

Interestingly there are only two incidences of the word "privacy" in the 156 page document and both refer to statute. The first references Alberta's *Freedom of Information and Protection of Privacy Act* in the context of the CEO's authorities regarding enumeration (p. 41). The second incidence references the Nunavut's *Access to Information and Protection of Privacy Act* as part of "Appendix E. List of Legislation, Regulations and Official Reports" (p. 154).

The report clearly states that the "…reader should be aware that Elections Canada is not responsible for the completeness or accuracy of the information herein provided." However, it is interesting that privacy has very little mention, and the privacy statute is only referenced in the context of two jurisdictions. Every EMB in Canada processes volumes of personal information, has statute governing the processing of that data, and a commissioner or ombudsperson who is responsible for ensuring compliance investigating alleged breaches of the Acts they administer (Office of the Information and Privacy Commissioner of Canada, "Provincial Privacy Laws", para 6).

4.7 Summary

This review included published academic research and writing, statutes, and publicly available reports produced by Canada's Information and Privacy Commissioners and CEOs. Academic and professional resources have revealed that privacy is "…rooted in some of the oldest religions, texts and cultures known" (Kris Klein 2012, p. 2-3), and that the terminology which acts as the basis for our modern understating of privacy is unique to its context. This research also reveals a number of foundational principles that guide the privacy work of public agencies and highlights a call by Canada's DPAs to develop "evergreen" program management programs.

5 FINDINGS: JURISDICTIONAL SCAN

This research sought to assess what information each federal, provincial and territorial agency discloses regarding their information and privacy programs (or lack thereof) on their agency websites. As Figure 6 demonstrates (see next page), most of Canada's EMBs share little or no information regarding their privacy management programs. The exceptions (and also the largest jurisdictions in Canada) including Quebec, Ontario, BC and Canada are inconsistent in the types of policies and information they publish.

One of the recommendations in *Getting Accountability Right with a Privacy Management Program* is that agencies "inform individuals of privacy rights and organizational privacy controls" (Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, 2012, pp. 1-18). If this test were applied to Canada's EMBs based on what is available on their websites, Elections Ontario would be the only agency able to demonstrate this achievement as it provides clear information regarding their privacy policies, how voters can be removed from the list, and how the agency handles personal information. However, the "privacy statement" accessible from the bottom of every page on the site that references the "Elections Ontario Privacy Policy" carries no live link to the information. Instead, the information can only be found by using the site map or by clicking through several layers of information under the heading "Voting in Ontario."

Elections Quebec also provides comprehensive information about their privacy program, however, there are some gaps. For example, under the "Register of the institution's personal information disclosures, established under section 67.3 of the Access Act" is the notation "document to come," and while much of the information on the website is available in both French and English, some critical information about their privacy practices is available only in French.

British Columbia publishes policy information regarding how stakeholder can access voter data and a set of FAQs which are informative however the site is missing specific information regarding the agency's privacy controls. Elections Canada provides a number of links, however they focus more on access than on privacy, and the information is peppered throughout the site.

In all, four EMBs performed well when reviewed for information about the stakeholder privacy rights and organizational privacy controls - although all could benefit from more prominent/centralized placement of their privacy management information, and/or from more information about privacy controls/disclosure. A further three either redirect the user to central government privacy policy, providing very little detail, or focus on a narrow aspect of privacy protection, i.e. having a voter's name obscured from the list.

Seven of 14 EMBs publish no information about their privacy programs and/or only discuss privacy in relation to the use of their websites. Interestingly, Saskatchewan has published a video on YouTube regarding their privacy management program – an innovative and accessible addition to their site.

The website review has demonstrated that for most EMBs very little is shared publicly regarding their privacy management programs and that all of the EMBs can benefit from some more work on the presentation of such information.

Figure 6 – Information and Privacy Policies on EMB Websites

Jurisdiction	Web Policies Related to Information and Privacy
Elections Alberta	A *Privacy & Security* page is accessible from the homepage. It refers to the agency's "privacy policy and practices on the web site". It also redirects users to the Alberta's *Freedom of Information and Protection of Privacy Act.* http://www.elections.ab.ca/privacy-security/
Elections BC	A "Privacy" link is accessible from the bottom of every page of the site. The link points to a page with the header "Privacy Policy Framework" which describes requirements for eligible stakeholders to file an "acceptable privacy policy with the CEO" in order to receive the voters list. The page also provides privacy policy templates and acceptance criteria for these stakeholder groups as well as general FAQs related to the agency's privacy program. http://www.elections.bc.ca/index.php/privacy/
Elections Canada	The privacy notice which describes privacy in relation to website use can be accessed from the bottom of each page by clicking on the "Terms and Conditions" link. http://www.elections.ca/content.aspx?section=pri&lang=e&document=index. Other information (i.e. The Annual report on the *Privacy Act*, privacy policies, etc.*)* is peppered throughout the website and can be found using the site map.
Elections Manitoba	There is a link from the bottom of every page entitled "Personal Security" which provides information for individuals who would like to have their name obscured from the voters list and vote by "homebound ballot." There is also a reference to privacy on the "Web site Information" page which discusses privacy as it relates to the use of the website. http://www.electionsmanitoba.ca/en/Voting/Personal_Security
Elections New Brunswick	A "Privacy" link is accessible from the bottom of every page of the site. The link redirects website users to the privacy page for the provincial government, and it addresses privacy only in relation to use of provincial government websites. http://www2.gnb.ca/content/gnb/en/admin/privacy.html.html
Elections Newfoundland and Labrador	No information regarding information and privacy is available on the agency's website. http://www.elections.gov.nl.ca/elections/
Elections Nova Scotia	A "Privacy Policy and Routine Disclosure" link is accessible from the bottom of every page of the site. The privacy policy portion refers to privacy in relation to use of the site. The disclosure policy refers to requests for records. https://electionsnovascotia.ca/privacy-policy
Elections Nunavut	No information regarding information and privacy is available on the agency's website. http://www.elections.nu.ca/apps/authoring/dspPage.aspx?page=home
Elections NWT	A "Privacy" link is accessible from the bottom of every page of the site. It addresses privacy in relation to use of the site. http://www.electionsnwt.ca/privacy
Elections Ontario	The "privacy statement" accessible from the bottom of every page on the site references the "Elections Ontario Privacy Policy" however there is no live link to the document. Using the site map, the *Permanent Register of Electors for Ontario and List of Electors Guidelines* and the *Elections Ontario Privacy Policy* can be found here http://www.elections.on.ca/en/voting-in-ontario/be-a-registered-elector/privacy-of-the-register.html
Elections PEI	A "Privacy" link from the homepage redirects users to a government page which discusses privacy in relation to use of government websites. http://www.electionspei.ca/index.php?number=1046928
Elections Quebec	A "Policy on Privacy" link is accessible from the bottom of every page on the site. The content is focused on privacy in relation to use of the site. http://www.electionsquebec.qc.ca/english/policy-on-privacy.php. The "Access to information" page also accessible from the website footer, provides information regarding the "*Access Act*" and the "Policy on release of information and privacy" however both resources are available only in French. http://www.electionsquebec.qc.ca/english/access-to-information.php
Elections Saskatchewan	A "Privacy Policy" link is accessible from the bottom of every page on the site. The policy begins with a short description of the "Agency's Commitment to Privacy" and then discusses privacy in relation to use of the site http://vote.elections.sk.ca/privacy-policy/index.html. Although not apparent on the agency's site, the agency also published an informational YouTube video on the subject of privacy https://www.youtube.com/watch?v=Fh1MWIjq4dI
Elections Yukon	No information regarding information and privacy is available on the agency's website http://www.electionsyukon.gov.yk.ca/

6. FINDINGS - INTERVIEWS WITH TOP ELECTION ADMINISTRATORS

Voluntary, semi-structured interviews in support of this research were conducted with CEOs (and/or their staff) from Alberta, British Columbia, Canada, Manitoba, Newfoundland and Labrador, Nunavut, Ontario, Quebec and Saskatchewan with a goal of better understanding what Canada's EMBs are doing in this space, what common opportunities and challenges these agencies are facing, and to help formulate some possible recommendations for next steps for Elections BC. The results of these interviews are presented in the sections below.

6.1 Triggering Incident(s)

Privacy management in the context of Canadian election administration has been growing in importance for several years with many of Canada's agencies reporting that a series of publicly reported breaches at Elections Alberta, Elections New Brunswick, Elections Ontario and/or Elections BC between 2011 and 2013 were an important trigger for this awareness and subsequent efforts (personal communications: G. Resler, March 9, 2016; K. Archer, March 22, 2016; S. Verma, March 23, 2016; M. Boda, March 10, 2016; G. Essensa, April 28, 2016).

A privacy breach "…occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information" and this type of activity is "unauthorized" if it occurs in contravention of the jurisdiction's statute (OIPC, Alberta, 2016). A privacy breach emerging from an EMB can contain a wide range of personal information depending on the jurisdiction and the stakeholder (Elections Canada, 2015, August 30). Common examples of stakeholders and data types include:

- **Staff (permanent and temporary):** Payroll data; employee performance information; name; address; social insurance number; resume, etc.
- **Candidates and Political Parties**: Financial disclosure information (although some may be publicly available by statute); investigations case file information; banking information, etc.
- **Voters:** Name; address (mailing and/or physical); birthdate; gender; phone number; email address; driver's licence number; social insurance number, participation data, etc.

An agency's decisions regarding breach response are unique to the circumstance (Office of the Information and Privacy Commissioner of British Columbia, 2012, March). Reasons for reporting to either the media and/or DPAs can include a statutory requirement (Office of the Information and Privacy Commissioner, 2016, March 9), a desire to be transparent (G. Resler, personal communication, March 9, 2016), a need for guidance or expertise (K. Archer, personal communication, March 22, 2016), concern for possible risk or harm to affected individuals (Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, April 2012, P. 4) and/or a need to communicate a breach where direct communication with affected individuals is not possible (CBC news, 2013, June 7). Further, there is a significant cost to a breach for both the agency and also the affected individuals (Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, April 2012, P. 4). In addition to reputational risk, EMBs can face significant expenses and operational disruptions associated with managing privacy breaches.

High-profile breaches in five Canadian EMBs in as many years (2011-2015) have "highlighted sharply what happens if there is no framework in place" (K. Archer, personal communication, March 22, 2016) and ushered in a "true sense of the importance of privacy" (M. Boda, personal communication, March

10, 2016). The breaches described below show the challenges associated with the maintenance, use, disclosure, and disposition of personal information in the custody and control of EMBs:

- Between August and October 2011, enumerators working for Elections Alberta mislaid three binders containing the personal information for 781 voters (CBC News, 2011, October 24). The binders included "names and addresses and, in some cases, phone numbers and birth dates of electors" (Elections Alberta, 2011). The breach garnered widespread media attention (CBC News, 2011, October 24).
- In May 2012, Elections New Brunswick mistakenly included sensitive information in their regular release of voters list information to Members of the Legislative Assembly and political parties. The breach, which affected some 553,000 individuals resulted in the erroneous distribution of phone numbers, dates of birth and driver's licence information (in addition to the regularly distributed name and address). The breach was heavily reported in the media and was quickly contained (CBC News, 2012, June 5). The following month an encrypted laptop containing the same data was stolen from Elections New Brunswick's offices (CBC News, 2012, June 6).
- In July 2012, Elections Ontario announced that it had lost two USB drives "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" (Cavoukian, 2012). In this instance, Ontario's Information and Privacy Commissioner publicly criticized the agency for the loss (Cavoukian, 2012).
- In May 2013, Elections BC lost the personal information belonging to voters at 300 residential addresses when a voting book contained within a ballot box was lost after voting proceedings closed in the Vancouver-Langara electoral district (Canadian Press, 2013). In this instance, the breach included names and addresses for all of the registered voters assigned to that voting place as well as information such as driver's licence numbers and birth dates for voters who had registered in conjunction with voting (Canadian Press, 2013).
- A hard drive containing "names, social insurance numbers, addresses, phone numbers and dates of birth of 611 temporary employees hired to work during the election campaign, as well as information about landlords who were providing space to Elections Canada" was stolen from a returning office in a Jonquière shopping mall during the 2015 Federal General Election (McGregor, 2015, para. 3). The agency explained that "the mall required access to the office to repair underground pipes and asked that the rear door be left open. A staff member was on hand to watch the office for all but a few minutes while the door was open. The next morning…the hard drive used for daily back-ups of the office computers had gone missing" (McGregor, 2015, para. 6). In this instance, "the agency agreed to provide ongoing monitoring of the employees' credit history, at a cost of $22,995 over the next year" (para. 5).

Almost every agency interviewed cited heavily publicised breaches at their own or other EMBs and frequent news reports of breaches at other public agencies within their jurisdictions as the primary catalyst for their privacy awareness and/or efforts. A small minority also cited statutory change (A. M. Delisle, personal communications, March 22, 2016) or a desire to be proactive (T. Forget, personal communications, April 4, 2016) as a driver.

Interestingly, in the last five years, the publicly reported breaches from Canada's EMBs have emerged primarily from the largest agencies including Elections Canada, Elections Quebec, Elections Ontario, Elections BC and Elections Alberta. It is not clear whether this is because they have the systems and resources in place to detect and respond to such incidents, whether the smaller agencies are less prone

to breaches due to tighter controls, and/or more centralized service delivery, whether this difference is related to the priority placed on privacy in a given jurisdiction.

6.2 Complexity of Privacy Programs

The interviews revealed little consistency among EMBs regarding their privacy management programs. Instead, the agencies appear to sit on a continuum with the absence of any privacy activity on one extreme and substantive formalized privacy programs on the other (See Figure 7, p. 41).

For example, Prince Edward Island (G. McLeod, email communication, March 1, 2016) and Northwest Territories (N. Latour, personal communication, February 29, 2016) chose to decline participating in this study citing a lack of contact with the DPA, a lack of breaches, and/or the absence of formal privacy management activities. Nunavut participated in the study, but described a similar situation (S. Kusugak, personal communications, April 8, 2016), and Yukon declined due to operational demands. These agencies comprise the smallest jurisdictions in the country.

Elections Newfoundland and Labrador, also a small agency, has not developed a privacy management program but has committed to adhering to or exceeding government standards, and plans to consider privacy in conjunction with other operational activities such as planned voting process improvements (B. Chaulk, personal communication, April 1, 2016).

Elections Alberta provides a good example of an informal privacy management program. Information and privacy considerations form an active part of Elections Alberta's operational work and the agency regularly seeks the advice of the Province's information and privacy commissioner in the development of new programs and activities (Glen Relser, personal communication, March 9, 2016). A senior-level staff member is accountable for privacy at the agency, and when breaches occur there is an active effort to review processes to prevent further occurrences. The CEO has also developed a set of recommendations for legislative change that would require voters list recipients to have and share with the CEO their privacy policies, to notify the agency of the loss of voter data, and to pay the costs of recovering any lost data (or having the agency recover the data on their behalf) (D. Westwater, personal email, March 22, 2016). This informal model falls within expectations of an accountable privacy management program as defined by the Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada (2012, p. 1).

Elections Manitoba also has an informal privacy management program. Shipra Verma, CEO, explained in an interview on March 23, 2016 that the agency has an internal policy regarding the processing of personal/voter information, and adheres to privacy statute and central government privacy policy. All staff take an oath of confidentiality, and that the agency restricts the use of USB keys, disposition of paper records in the field, and has restricted access on agency servers based on business need. Elections Manitoba has plans to move to a more formalized program with the anticipated hiring of a new Deputy CEO (S. Verma, personal communication, March 23, 2016).

In 2012 Elections BC began to develop a formal privacy management framework. The agency focussed on critical risks ahead of the 2013 Provincial General Election, and developed a project plan for a comprehensive privacy review and framework project (K. Archer, personal communication, March 22, 2016). As part of the project, Elections BC commissioned David Loukidelis, B.C.'s former information and privacy commissioner to assess the agency's compliance with information and privacy obligations by completing a comprehensive review of the agency's policies, procedures, training and contracts, and by

conducting an inventory of all of Elections BC's personal information holdings. Loukidelis' (2014) report reinforced the general recommendations for public bodies set out in *Accountable Privacy Management in BC's Public Sector* (Office of the Information and Privacy Commissioner of British Columbia, n.d.) and established a large number of more granular activities to support compliance, including specific updates to guides, forms, processes, procedures, and the agency's websites. The second phase of this project sought to address each recommendation in a methodical way to ensure the program was operational before the 2017 provincial general election planning began in earnest. At the time of writing, the agency was still working to move to a fully operational or "evergreen state" (K. Archer, personal communication, March 22, 2016).

Michael Boda, Saskatchewan's CEO also led the development of a two-phased privacy management program. Similar to the program undertaken in B.C., phase one addressed critical policies, procedures, training and communications tools ahead of the 2016 Provincial General Election with the help of internal election administrators and external privacy experts. Phase two, commencing after the election, involves the development and ongoing maintenance of a formalized privacy management program and the appointment of a privacy officer (M. Boda, personal communication, March 10, 2016).

Elections Canada's Access to Information and Privacy Office is working towards the completion of an institutional privacy framework to link Election Canada's governance structure into its various privacy instruments, as well as to link the privacy instruments together into a coherent whole. The agency complies with Treasury Board of Canada Secretariat (TBS) policies, directives and guidelines as they relate to the *Privacy Act*, and the management of personal information and they submit annual reports to Parliament. To facilitate the right of access, Elections Canada publishes an annually updated chapter of *Info Source*, a resource which describes the records and personal information used in the conduct of the agency's programs. Elections Canada has also developed various internal instruments and processes used to manage the collection, use, disclosure and protection of personal information including: project initiation and preliminary risk assessments, privacy impact assessments, a protocol for non-administrative uses of personal information (i.e. statistical research), and the agency's privacy breach protocol (A. M. Delisle, personal communication, June 22, 2016).

Elections Quebec has been governed by privacy laws since 1982, however, until last year, there had been no coordinated effort toward the development of a privacy management program. They have since established an access and privacy office with three staff as well as a multi-disciplinary committee on access and privacy chaired by the CEO. Elections Quebec has also published a 3-year action plan on access and privacy (French only) that focuses on training and compliance with statute, and is preparing to do a comprehensive review of all of the agency's information systems (T. Forget, personal communication, April 4, 2016).

Elections Ontario has a rigorous and mature privacy program comprising six foundational privacy policies (i.e. general, acceptable use, breach management, PREO guidelines etc.). The agency has undergone security threat assessment, conducts regular training, audits the activities of field and headquarters staff for compliance with policy, and reports annually on compliance. Their efforts are guided by the Privacy by Design principles established by Cavoukian in 2012 (G. Essensa, personal communications, April 29, 2016).

In short, the complexity of the privacy management programs in Canada's EMBs appear to fall on a continuum with the absence of a program at one end, and a highly formalized program at the other. While the larger agencies tended to have more formal programs the complexity of these programs is

inconsistent - some similarly sized agencies have taken vastly different approaches (i.e. Elections Alberta versus Elections Saskatchewan, Elections Canada versus Elections Quebec).

6.3 Privacy Accountability

All 14 Canadian federal, provincial and territorial jurisdictions have an information and privacy commissioner or ombudsperson responsible for overseeing information and privacy legislation (Office of the Information and Privacy Commissioner of Canada, "Provincial Privacy Laws", para 6). All of the agencies interviewed as part of this research indicated that the agency has assigned the responsibility for the privacy portfolio to an individual or office (See Figure 7, p. 41). This accountability takes on many forms across the country. For example, in Nunavut, due to the size of the agency, the CEO is responsible for privacy (S. Kusugak, personal communications, April 8, 2016). Elections BC initially sought external expertise from B.C.'s former information and privacy commissioner to assist with that agency's privacy program initiation, but now has two certified information and privacy professionals on staff (one of which is the author of this study). At Elections Canada, the CEO has delegated his authority under the *Privacy Act,* to the Access to Information and Privacy (ATIP) Coordinator and while the ATIP Office leads a lot of this work, senior officials and executives also have responsibilities under Treasury Board directives (i.e., initiating privacy impact assessments) (A.M. Delisle, personal communication, June 22, 2016). Quebec has a similar structure with their Access to Information and Protection of Privacy Office (T. Forget, personal communication, April 4, 2016). At Elections Newfoundland and Labrador (B. Chaulk, personal communication, April 1, 2016), Elections Manitoba (S. Verma, personal communication, March 23, 2016), and Elections Alberta (G. Resler, personal communication, March 9, 2016) the Deputy has been (or will be) assigned this responsibility. At Elections Saskatchewan, the effort to develop a formal privacy management program is currently being led by the CEO, key staff and a privacy expert on loan to the agency. The office intends to appoint a permanent privacy officer as part of the next phase of their framework development project (M. Boda, personal communication, March 10, 2016). In Ontario, the CEO has delegated this responsibility to the agency's General Counsel and Director of Election Finance (G. Essensa, personal communications, April 28, 2016). In all cases, employees also have responsibility for the proper management of personal information under their control.

The central focus of EMBs is to deliver electoral and other events per their respective legislation. As a result they do not always have privacy expertise in-house and there is very little consistency when it comes to addressing this knowledge gap. Instead, agencies have employed a range of strategies including hiring external expertise (on a temporary or permanent basis), appointing and then training and/or certifying one or more staff members, establishing a privacy office and/or simply appointing a senior official to do this work off of the "side of their desk."

6.4 Environmental Changes

EMBs process personal information from stakeholders including voters, temporary and permanent staff, candidates and their agents and others. The obligations for processing this information are typically prescribed in statute administered by the CEO or the DPA (Elections Canada, 2015, August 30). Additional guidance can be found in the agency's privacy policies, established procedures and/or the agency's privacy management framework (if there is one in place).

An obligation common to most of Canada's EMBs is the requirement to disclose voter data to candidates and political parties at different points in the election cycle (Elections Canada, 2015, August 30). A

review of election statute guiding the work of Canada's EMBs demonstrates that there is a long-standing practice of allowing/requiring candidate representatives/election officials to manually collect information about who voted during voting proceedings. Candidate representatives or scrutineers then transmit this information to candidate or political party offices to assist with their get-out-the-vote campaigns. EMBs also regularly disclose voter information to elected officials and political parties on an annual basis and/or after electoral events (Elections Canada, 2015, August 30). Recently, however, there has been a push to compel EMBs to disclose voter information in more readily accessible formats (i.e. electronically), and to formally disclose new data elements regarding voters including voter participation flags and voter age or birthdate. For example:

- In 2015, the Government of British Columbia passed Bill 20 requiring election officials to provide MLAs, parties and candidates information regarding whether an elector voted in the last election (K. Archer, personal communications, March 22, 2016). The agency operationalized this requirement by introducing electronic strike-off, and delivering the data on encrypted memory sticks (Archer, 2016).
- Since 2009, Sections 42-44 of the Nova Scotia *Election Act* (2013) has required the agency to provide participation information to political parties on an annual basis along with other voter information including a unique identifier and the voter's "age category" (a curious addition as the exact year of birth would be apparent to the data recipients as electors move from one age category to another). Section 52 of the Act also requires that the preliminary list of voters provided to each candidate before General Voting Day include an indication whether the voter has voted in the current election.
- Legislative change in 2015 established a permanent register of voters (Elections Saskatchewan, 2015) and "…new requirements for voters' birth date information to be included on lists of voters…" (Boda, 2015, para. 1). However, "sections 18.6(3) and 18.7(4) of the Act also provide the CEO with discretionary ability to remove information contained on lists of voters to protect against potential misuse of voter registration information and to protect the personal privacy and security of voters" (Boda, 2015, para 2). The agency has operationalized this to provide year of birth only when necessary to distinguish between two individuals with the same name in the same household, and to provide complete birthdate information when an Information Sharing Agreement (ISA) is in place to protect it (Boda, 2015).
- Section 86 of the Ontario *Election Act* (1990) requires that voting documents (which contain participation information) be available for public inspection. Elections Ontario has operationalized this process to provide the participation information directly to political parties during and after electoral events (G. Essensa, personal communication, April 28, 2016).

The list above illustrates the complexity of just one set of data processing responsibilities faced by Canadian EMBs. It also highlights that new statutory obligations regarding the collection and disclosure of data are compelling these agencies to disclose more information about voters, in formats that candidates, political parties, elected officials and others can more readily process.

There is also a persistent interest from some election administrators, elected officials and members of the public to make election administration more convenient and efficient by introducing technology to administrative processes that have been performed manually since confederation (K. Archer, personal communications, March 22, 2016; Elections Canada, 2012). For example, by-elections in British Columbia in early 2016 were used as a testing-ground for electronic voter participation strike-off for advance and absentee voting. This was an effort to improve operational process, reduce errors, and

respond to statutory change requiring the agency to provide rapid and comprehensive access to a list of voters who voted (Office of the Information and Privacy Commissioner for British Columbia, 2015; Elections BC, 2016, June). A similar strike-off system was used in Ontario during the agency's last by-election, where the agency piloted a "Party Portal" program which provided participation information via a shared reference number (i.e. "bingo sheet") online in (almost) real time to assist political parties with their get out the vote efforts (G. Essensa, personal communication, April 28, 2016). A recommendation in favour of electronic strike-off at the federal level was also made in 2013 following the Supreme Court of Canada's judgement in *Opitz v. Wrzesnewskyj*, a case which challenged the validity of the election in Etobicoke Centre due to the number of administrative errors made by election officials (Elections Canada, 2013, "The New Brunswick Model", para 7), and many Canadian jurisdictions are investigating opportunities for introducing electronic-strike off in their own jurisdictions (M. Boda, personal communications, 2016).

This change in process can reduce operational risk to privacy in some areas while introducing new risk in others. For example, electronic strike-off reduces the number of voters lists in the field and requires less effort to track and secure the paper-based data while simultaneously introducing questions about how the data processed in the voting place can be securely transmitted back to headquarters (i.e. Are there passwords? Where are they stored? Who has access to them? Are the data transmitted wirelessly? Are the data transmitted from the voting place or from the Returning Office/District Electoral Office?) (Personal communications: K. Archer, March 22, 2016; G. Essensa, April 28, 2016).

There are other examples of the introduction of technology in election administration. For example, Prince Edward Island is preparing for a plebiscite on electoral reform (MacLauchlan, 2015) which will be conducted via alternative vote or electronic voting "provided the standards for security, accuracy, privacy, integrity, cost-effectiveness and auditability can be assured" (Brown, J. Bevan-Baker, P., Biggar, P., Macewen, S. and Sherry, J. 2016, April 15). This is on the heels of the 2014 report of B.C's Independent Panel on Internet Voting, which reviewed "best practices with respect to Internet voting in other jurisdictions and examined issues associated with implementing Internet voting for provincial or local government"(Independent Panel on Internet Voting, 2014, p.5). Ultimately, the panel concluded that "if Internet voting is implemented, it should be limited to those voters with specific accessibility challenges" and that "jurisdictions need to recognize that the risks to the accuracy of the voting results remain substantial" (Independent Panel on Internet Voting, 2014, p.2). British Columbia and Alberta are both exploring electronic "web-based poll books," and finally, in 2017, B.C.'s targeted enumeration strategy will include the use of tablets rather than printed materials to collect and transmit voter registration updates (K. Archer, personal communication March 22, 2016).

Election administration is changing due to environmental factors such as technology and statutory change and interviews conducted as part of this research have demonstrated an awareness of the need for election administrators to be proactive in their approach to privacy (personal communications: G. Resler, March 9, 2016; M. Boda, March 10, 2016; K. Archer, March 22, 2016; S. Verma, March 23, 2016; B. Chaulk, April 1, 2016; A. M. Delisle, March 22. 2016).

6.5 Contact with the Data Protection Authority

Each interviewee was asked to characterize their contact with their respective data protection authority and again there was very little consistency in approach. Instead these relationships appeared to reflect the preferences and attitudes of the leadership in each organization (rather than the size of the agency). For example, Elections Alberta, Elections Ontario and Elections BC, all described a strong relationship

with the DPA in which they report breaches and seek advice on an ongoing basis out of "courtesy" (personal communications: G. Resler, March 10, 2016; K. Archer, March 22, 2016; G. Essensa, April 28, 2016) and in Saskatchewan the CEO has regular and ongoing engagement with the commissioner (M. Boda, personal communication, March 10, 2016). Elections Canada and Elections Manitoba both characterized the relationship as proactive, and provided examples where they had worked with the DPA in the development of new programs and activities, and the DPA in Manitoba also recently delivered privacy training to all headquarters staff at Elections Manitoba as part of that agency's ongoing professional development activities (personal communications: A. M. Delisle, March 2, 2016; S. Verma, March 23, 2016). In contrast, Elections Newfoundland and Labrador described the relationship with the DPA as limited and primarily focussed on access to information (B. Chaulk, personal communication, April 1, 2016), and in Nunavut the relationship was limited to advice and guidance during the drafting of the election statute (S. Kusugak, personal communication, April 8, 2016). In Quebec, the relationship was also characterized as limited and primarily focussed to access requests. In this instance, there was an acknowledgement that the DPA was operating with limited resources (T. Forget, personal communication, April 4, 2016).

While most of the individuals interviewed indicated that the relationship between their EMB and the DPA was positive, there was little consistency in approach to that professional relationship.

6.6 Common Challenges

Several common challenges (in addition to those discussed above) were identified as part of the interviews with Canada's CEOs (or their delegates). They include the distributed model of election administration, finding a balance between operational obligations and privacy compliance, public expectation, and data disclosure and processing. Each is described in detail below.

Distributed model of election administration in Canada

EMBs are required to quickly "staff-up" for electoral events. For most of Canada's EMBs this means rapidly hiring thousands or tens of thousands of temporary staff. Elections Canada added a whopping 285,000 temporary staff to their payroll in advance of the 42nd Federal General Election (A.M Delisle, personal communication, June 22, 2016), Elections Ontario hires 80,000 staff (G. Essensa, personal communication, April 28, 2016) and in British Columbia one in every 125 of the 4.5 million residents of the province are employed by Elections BC in the days and weeks around a provincial general election (K. Archer, personal communication, March 22, 2016). These staff receive a few hours of training. Their employment is typically counted in days, rather than weeks or months. Some jurisdictions, like Saskatchewan, also rely on volunteers in care homes, hospitals and other locations to support enumeration and the administration of voting (M, Boda, personal communication, March 10, 2016).

All of these individuals have access to personal information, from the information officer at the entrance of the voting place screening and directing voters based on the information on their voter information card, to enumerators knocking on doors to update the voters list, to the office manager in the Returning Office/District Electoral Office managing the hiring process for hundreds of election officials. Almost every aspect of this work involves processing personal information. The challenge for election administrators is how to effectively communicate and implement effective processes, best practices and training in privacy management in this unique environment (personal communications: M. Boda, March 10, 2016; S. Verma, March 23, 2016: G. Essensa, April 28, 2016). Further, these temporary individuals are "hired on a good faith basis" (S. Verma, personal communication, March 23, 2016), and often only

have a "tangential relationship with the agency" (K. Archer, personal communications, March 23, 2016). Human error, old habits, ignorance or malicious conduct, can have a significant impact on the agency's reputation (personal communications: K. Archer, March 22, 2016; S. Verma, March 23, 2016).

Finding a balance between operational obligation and compliance

Several EMBs highlighted that finding the right balance of privacy protection while still allowing for effective operations and/or innovation in the unique electoral field was a challenge. Further, there is no common agreement on "what is enough" protection for a particular data set, and prescriptive election legislation drafted 40-50 years ago can conflict with best practices in privacy management (G. Essensa, personal communication, April 28, 2016).

Extraordinary compliance

Public expectation of extraordinary compliance also emerged as a concern during the interviews. For example, during the 2011 Enumeration in Alberta, three enumeration binders were mislaid affecting 781 voters (CBC News, 2011, October 24). The binders included "names and addresses and, in some cases, phone numbers and birth dates of electors" (Elections Alberta, 2011). These breaches garnered widespread media attention (CBC News, 2011, October 24) despite representing just 3 of approximately 6000 binders, or one half of one percent of the enumeration binders in the field during that event (G. Resler, personal communication, March 9, 2016).

The ballot box containing the voting book lost during British Columbia's 2013 Provincial General Election included names and addresses for all of the registered voters assigned to that voting place, as well as information such as driver's licence numbers and birth dates for voters who had registered in conjunction with voting (Canadian Press, 2013). It affected just one of 10,518 general voting books (Elections BC, Statement of Votes, 2013, p. 2) and represented a compliance rate of 99.9905%. However, BC's CEO reported that it was "the kind of situation in which the reputation of the organization can be called into question" (K. Archer, personal communications, March 22, 2016).

Data disclosure and processing

Interviews with Canada's CEOs have revealed genuine concerns about the statutory disclosure and processing of voter data by list recipients. These concerns were centered on several primary themes including voter profiling and possible use of the information to determine how someone voted; disclosure of voter data to political parties and others who are not bound by statute governing its use (Bennett C. and Bayley R., 2012, March 28); an inability to monitor or audit the use of such data or confirm its disposition (personal communications: S. Verma, March 23, 2016; G. Essensa, April 28, 2016); and, difficulty determining data ownership/responsibility for clean-up when a breach of voter data by a recipient of the voters list occurs (G. Resler, personal communication, March 9, 2016). These themes are explored in greater detail below.

Privacy in the context of voting is a relatively new phenomenon. Karpowitz et al (2011) observed that "Prior to the twentieth century, the act of voting was not at all private" (p. 661). This changed significantly with the twentieth century introduction of the secret ballot which allowed voters to "vote without coercion or fear of reprisal" (op.cit., p.660), and further changed with the advent of technology. A review of the election statute in each Canadian jurisdiction reveals that a process for displaying or calling out the name and/or voter number of each voter to allow others to scrutinize (and challenge if

necessary) voter eligibility is very common. The 21st century has seen the development of a further trend across Canada to compel EMBs (before, during and/or after electoral events) to provide new data elements including age range, birthdate, and/or participation information to candidates and political parties (Office of the Information and Privacy Commissioner of British Columbia, 2015; also see Section 5.4 Environmental Changes) to assist with their "get out the vote efforts" (Archer, 2014, p.6). This information can be uploaded to the candidate's or political party's databases and/or voter management platforms where it is combined with other private or commercial data to develop comprehensive profiles about those who vote (or not), (Bennett, 2015). While a candidate or political party can never know for certain how an individual voted, research by Karpowitz et al. (2011) indicates that voters in the political minority may be "especially sensitive to issues of privacy…" (p. 678) and that "voters may not be so much concerned about overt fraud or physical coercion as they are about poll workers or other voters knowing how they voted…" (p. 661). Further, and of particular concern to election administrators, is the finding that "a lower sense of privacy is strongly associated with lower voter confidence" and less confidence the outcome of the election was fair (Karpowitz et al., 2011, p. 661).

A second concern of Canada's EMBs is that they are required to disclose voter data at regular intervals to political parties and others (of varying professionalism) who are not bound by statute governing its use (Bennett C. and Bayley R., 2012, March 28; S. Verma, personal communication, March 23, 2016). Further Canada's EMBs have no ability to monitor or audit the use of such data (S. Verma, personal communication, March 23, 2016), and some struggle to determine data ownership/responsibility for clean-up when a breach of voter data by a recipient of the voters list occurs (G. Resler, personal communication, March 9, 2016). The risk resulting from these conditions was highlighted in a 2012 report prepared for the Office of the Privacy Commissioner of Canada entitled, *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis.* In it the authors state that

> "the downward trend in democratic participation could be accelerated if a significant loss of confidence in the parties' respect for personal privacy were to occur. A well-publicized privacy breach could not only hurt the specific party, it could also damage the other parties and the whole political system. Potentially, the public disclosure about a party's personal information practices, if widely seen as unethical or unreasonable, could create a backlash against the parties and the democratic system as a whole" (Bennett C. and Bayley R. , 2012, March 28, p. 4).

Interviews with Canada's CEOs has revealed genuine concerns about the processing of voter data by political parties, and candidates and the lack of statute governing these activities. Secrecy of the ballot and confidence in the electoral process are significant issues for election administrators, and they have taken a varied approach in an attempt to address these concerns. Elections British Columbia has agreed to work with the privacy commissioner to develop a set of tools to guide the use of voter information by political parties and other recipients, and they have established a regulation that requires list recipients to have an acceptable privacy policy in place before the data will be shared (K. Archer, personal communications, March 22, 2016). Elections Quebec has issued a recommendation in their annual report to review the province's election statute in relation to privacy (T. Forget, personal communications, June 16, 2016), Elections Alberta has issued recommendations for legislative change that would provide some protections/restrictions (G. Resler, personal communications, March 9, 2016), and Elections Saskatchewan has issued a Bulletin which restricts the sharing of some types of data including date of birth unless an information sharing agreement is in place (M. Boda, personal communications, March 10, 2016).

6.7 Next Steps

Each agency interviewed was asked about their plans for their privacy portfolio in the next year and beyond, and there was a wide variance about planned activities. Figure 7 (p. 41) provides a comparison. A few interesting themes emerged from these discussions.

First, Keith Archer, B.C's CEO highlighted the importance of timing in relation to the privacy program development and explained that such programs can take more than one cycle (period from the end of a general election through the end of the next general election) to complete (personal communication, March 22, 2016). This was echoed by Michael Boda, CEO of Saskatchewan (personal communication, March 10, 2016) and is reflected in both agencies' continued efforts to formalize and operationalize their privacy programs.

Second, an understanding of the "dynamic nature" of privacy program management was a theme of these discussions. For example, Elections British Columbia raised the need to modify the privacy framework to reflect statutory change (K. Archer, personal communications, March 22, 2016) and Elections Quebec plans to review all of their information systems in acknowledgement of the fact that the systems were developed at a time when privacy and security was a less prominent feature of their work (T. Forget, personal communications, April 4, 2016). Elections Ontario also acknowledged that technology is evolving and so are the number of digital transactions. As a result, agencies need to constantly monitor for compliance and update programs and activities accordingly (G. Essensa, personal communications, April 28, 2016).

Third, not all agencies feel the same pressure to undertake privacy programs/activities. For example, the CEO of Nunavut, Sandy Kusugak explained that although she monitors the privacy challenges and efforts in other jurisdictions "there is no reason to act at this time as the risks in other jurisdictions are not relevant to the way [they] do business" (personal communications, April 8, 2016). Like most other aspects of their privacy activities, Canada's EMBs have wide variance when it comes to their future plans.

6.8 Summary

The interviews revealed that the primary catalyst toward privacy awareness and the development of privacy management programs in Canada's EMBs over the last five years can be overwhelmingly attributed to highly publicized breaches at election and other public agencies. Public sensitivity, guidelines from DPAs, the use of technology to make election administration more efficient, accurate and convenient, and new statutory obligations affecting the collection and disclosure of personal information are also driving this work.

While approaches differ, the privacy goals for EMBs with privacy management programs are substantially similar - to maintain the public trust by ensuring processes are in place to protect voter and other personal information in the custody and control of the agency, to reduce privacy risk, and to comply with statutory obligations.

Interviews conducted as part of this research have uncovered a series of challenges faced by Canada's election administrators including the distributed model characterizing event delivery; the need to dramatically increase their staffing compliment in very short periods of time; the expectation from the

public of extraordinary compliance; the need to balance privacy obligations and operational requirements; and the need to adjust to new statutory and technological requirements.

Information and privacy awareness and management in Canada's EMBs is inconsistent across the country. Some agencies have comprehensive privacy programs, others have sound but more informal programs, and others have yet to address privacy as part of their ongoing operational work. Regardless, effective privacy management requires maintenance of programs and policies to reflect changing statute, technology and the expectations of stakeholders *(*Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, 2012).

Figure 7 – Privacy Activities at Canada's EMBs – Interview Data Master

Jurisdiction	Triggering incident	Program Complexity	Accountability*	Public breaches since 2011	Relationship with DPA	Privacy Portfolio – Next 12 months and beyond
Alberta	Breach at Elections Alberta in 2011	Decentralized policies/No structured framework	Senior staff member	2011 - Enumerators working for Elections Alberta mislaid three binders containing the personal information for 781 voters (CBC News, 2011, October 24). The binders included "names and addresses and, in some cases, phone numbers and birth dates of electors" (Elections Alberta, 2011). The breach garnered widespread media attention (CBC News, 2011, October 24).	Proactive – Meets regularly with DPA, reports breaches to obtain advice or as a courtesy regardless of the size of the breach. Sends privacy impact assessments to DPA for review	Status quo from a privacy management program perspective. The agency is seeking legislative change that would require political parties and others to provide the CEO with a copy of their policy relating to the care, custody and use of the list of electors before they are given the list, it will also require recipients to take all reasonable steps to protect the list of electors from loss and unauthorized use, to require parties to notify the CEO of loss, and to pay the costs of recovering the data or having the CEO recover the data on their behalf in the event of a breach (D. Westwater, personal communication, March 9, 2016)
British Columbia	Breaches at Elections Ontario and Elections Alberta	Formal program - Institutional framework in place - still working to move to operational "evergreen state"	Two privacy officers trained as certified information and privacy professionals. Temporarily hired outside privacy expertise for program initiation	2013 - Elections BC lost the personal information belonging to voters at 300 residential addresses when a voting book contained within a ballot box was lost after voting proceedings closed in the Vancouver-Langara electoral district (Canadian Press, 2013). The breach included names and addresses for all of the registered voters assigned to that voting place as well as information such as driver's licence numbers and birth dates for voters who had registered in conjunction with voting (Canadian Press, 2013).	Proactive – Meets regularly with DPA, reports serious breaches to obtain advice or as a courtesy. Sends privacy impact assessments for significant projects to DPA for reference	Further implementation of the agency's "dynamic" privacy management framework primarily focussed on updating the program to reflect recent statutory change, operational innovations, additional staff training and records management (K. Archer, personal communication, March 22, 2016)
Canada	Statutory obligations under the *Privacy Act*	Decentralized policies primarily from Treasury Board/Working toward a structured framework	Manager and Coordinator, Access to Information and Privacy (ATIP) with three additional staff and ad hoc consultants - senior officials and executives also have responsibilities under Treasury Board directives	2015 - A hard drive containing "names, social insurance numbers, addresses, phone numbers and dates of birth of 611 temporary employees hired to work during the election campaign, as well as information about landlords who were providing space to Elections Canada" was stolen from a returning office in a Jonquière shopping mall during the 2015 Federal General Election (McGregor, 2015, para. 3).	Proactive – Ongoing communication with the DPA currently focused on significant projects requiring a privacy impact assessment	Development of a formal framework and some additional election specific privacy management tools. However, there is uncertainty regarding anticipated changes to the *Election Act*. The privacy framework will ultimately reflect all changes to legislation (A. M. Delisle, personal communications, June 22, 2016)
Manitoba	Breaches at Elections Ontario and Elections New Brunswick	Decentralized policies/No structured framework	Deputy CEO		Proactive – Ongoing collaboration with the DPA regarding significant projects, process change, statutory change, staff training and informal advice	Formalizing the agency's privacy program (S. Verma, personal communication, March 23, 2016)

Jurisdiction	Triggering incident	Program Complexity	Accountability*	Public breaches since 2011	Relationship with DPA	Privacy Portfolio – Next 12 months and beyond
Newfoundland and Labrador	Breaches at Elections Ontario and Elections New Brunswick	Decentralized policies/No structured framework	Assistant CEO		Limited – Very little contact with DPA	Improving operational processes and voting methods, while respecting privacy obligations (B. Chaulk, personal communications, April 1, 2016)
Nunavut	None	No program	CEO		Very limited - Only contact was when the commissioner assisted with drafting the Nunavut *Elections Act*	Status quo – No privacy management activities are planned as the risks in this jurisdiction have been assessed as very low. Continue to monitor privacy activities in other EMBs (S. Kusugak, personal communications, April 8, 2016)
Ontario	Had an existing program however, recent trigger was Ontario's 2012 breach	Formal program with a set of six comprehensive privacy policies	General Counsel and Director of Election Finance is the Chief Privacy Officer. Temporarily hired outside privacy expertise for program initiation	2012 - Elections Ontario announced that it had lost two USB drives "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" (Cavoukian, 2012).	Proactive – Positive and ongoing relationship focused on policy development, breach response and informal advice	Staff training, monitoring and reporting on compliance, maintaining their privacy program through an awareness of environmental change, and building privacy in to their 2018 project/event planning (G. Essensa, personal communication, April 28, 2016). Also, making a recommendation to the legislative assembly to allow for electronic poll-books and electronic tabulation beyond the 2011 by-election pilot program (Elections Ontario, 2016).
Quebec	Desire to be proactive and transparent	Formal – Established a 3-year action plan on access and privacy (French only) focused on training and compliance with statute	Dedicated Access to Information and Protection of Privacy Office and a multi-disciplinary committee on access and privacy chaired by the CEO		Limited - Primarily related to access requests	A comprehensive assessment of all of the agency's information systems (10 in total) is planned for next year. There will also be a focus on staff training, and an effort to educate political parties, candidates, MNAs and the public regarding the use of the voters list (T. Forget, personal communications, April 4, 2016).
Saskatchewan	Breaches at EMBs in Ontario, New Brunswick, and British Columbia, and at other public agencies	Decentralized policies/ structured framework is in progress	Senior staff member. Temporarily hired outside privacy expertise for program initiation		Proactive – Positive and ongoing relationship	Formalize their privacy management program and see the appointment of a privacy officer (M. Boda, personal communications, March 10, 2016).

*Refers to the senior staff with delegated responsibility for privacy. In all cases, employees are also responsible for the proper management of personal information under their control.

7. DISCUSSION: FINDINGS, THEMES, STRATEGIC IMPLICATIONS

This research was designed to assess the status of the privacy management programs in Canada's EMBs and uncover any common opportunities and challenges they are facing. It also sought to develop some possible recommendations to guide Elections BC's next steps. The following section attempts to distill the findings, themes, and strategic implications of this work.

Findings from Literature and Jurisdictional Scan

The literature review revealed that privacy is "rooted in some of the oldest religions, texts and cultures known" (Klein, 2012, p. 2-3), and that it is fundamentally about choice or the ability of individuals to choose when and how to expose their personal information to others (Klein, 2012). Canada's courts have "recognized privacy as a fundamental right protected by Sections 7 and 8 of the Canadian Charter of Rights and Freedoms (1982)" (Privacy Commissioner of Canada, 2005, Preface), and fundamental principles underlay all modern privacy regimes (Klein, 2012, p. 19) which have emerged as governments work to "balance protection of their citizens' personal information with governmental interests in national security and promotion of commercial competitiveness" (McLennan et al., 2007, p. 669).

In Canada, privacy laws are enforced in every provincial and federal jurisdiction (Office of the Information and Privacy Commissioner of Canada, "Provincial Privacy Laws", para 6) by a commissioner or ombudsperson who is responsible for ensuring compliance, investigating alleged breaches of the Acts they administer, and "acting as a liaison for data protection issues" (Klein, 2012, p. 4-5). These DPAs have produced a large number of reports and tools to guide public agencies, and in 2012, the Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, produced a joint report calling for organizations to "have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program (p. 1). The report also stated that "…accountable organizations are able to demonstrate that they have a comprehensive privacy management program in place" (p. 18).

The risk of inaction is high for any public agency as a breach can result in significant reputational and financial risk (Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, 2012). Notably, this research has revealed that the risk is even higher for an EMB where poor privacy management can weaken confidence that the outcome of the election was fair (Karpowitz et al., 2011, p. 661), and that a "hit" on an EMB's credibility can have a knock-on effect on the legitimacy of that jurisdiction's political institutions (Balasko, 2015, p. 65-66). Rationally, every EMB in Canada should have in place an "evergreen" privacy management program that is appropriate to the size and mandate of the agency.

The research also involved a review of the websites for all of Canada's EMBs with a goal of identifying what information they share about their privacy programs. This assessment has revealed that despite a call to "inform individuals of privacy rights and organizational privacy controls" (Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, 2012, pp. 1-18) most of Canada's EMBs share little or no information regarding their privacy management programs and/or fail to fully address these requirements. Elections BC shares more than most, but has is still lacking publicly available information regarding the agency's privacy controls.

Key Findings from Interviews of EMB Representatives

The interviews involving nine of Canada's 14 EMBs complimented the literature review by gathering information regarding the information and privacy work underway at Canada's EMBs, the work planned in the near and long term and the challenges and opportunities they are facing as they try to address this important field of work. They produced some interesting themes (see Figure 7 on p. 41 for a summary).

Goals are Consistent, but the Approach is not

The interviews revealed that there is very little consistency among EMBs regarding their privacy management programs. Instead, the agencies appear to sit on a continuum with the absence of any privacy activity on one extreme and substantive formalized privacy programs on the other. Predictably, the smallest agencies were the least likely to have a program, and the largest agencies had the more formalized programs. Despite these differences, the privacy goals for EMBs that have privacy programs are substantially similar - to maintain the public trust/agency reputation by ensuring processes are in place to protect voter and other personal information in the custody and control of the agency, to reduce privacy risk, and to comply with statutory obligations. Further, almost all of the individuals interviewed cited high profile breaches at election agencies or other public agencies as catalytic for this work, including British Columbia's CEO, Keith Archer (personal communication, March 22, 2016).

The interviews also revealed that EMBs do not always have privacy expertise in-house and that there is very little consistency when it comes to addressing this knowledge gap. Instead, agencies have employed a range of strategies including hiring external expertise (on a temporary or permanent basis), appointing and then training and/or certifying one or more staff members, establishing a privacy office or simply appointing a senior official to conduct this work off of the "side of their desks" (see Figure 7, p. 41). Interestingly, only the four largest EMB's including Elections Canada, Elections Quebec, Elections Ontario, and Elections BC appear to have built-in bench-strength to accommodate the absence or departure of the "privacy person."

Common Challenges

When asked about the challenges they are facing, several themes emerged. For example, while displaying or calling out the name and/or voter number of each voter to allow others to scrutinize (and challenge if necessary) voter eligibility is very common, the twenty-first century has seen the development of a further trend across Canada to compel EMBs (before, during and/or after electoral events) to provide new data elements including age range, birthdate, and/or participation information to candidates and political parties (Office of the Information and Privacy Commissioner of British Columbia, 2015, also see section 5.4 Environmental Changes) to assist with their "get out the vote efforts" (Archer, 2014, p.6). With new technologies, this information can be rapidly transferred and uploaded to the candidate's or political party's databases and/or voter management platforms where it can be combined with other private or commercial data to develop comprehensive profiles about those who vote (or not), (Bennett, 2015). CEOs expressed concern with voter profiling and the possible use of the information to determine how someone voted. They also raised concerns with the requirement to disclose personal information to stakeholders who are not bound by statute governing its use (Bennett C. and Bayley R., 2012, March 28) and an inability to monitor or audit the use of such data or confirm its disposition (S. Verma, personal communication, March 23, 2016, and G. Essensa, personal communication, April 28, 2016). The question of voter profiling which was foreshadowed in the

literature review, is of particular concern to election administrators because it has the potential to weaken confidence that the outcome of the election was fair (Karpowitz et al., 2011, p. 661) and accelerate the downward trend of democratic participation in Canada (Bennett C. and Bayley R., 2012, March 28, p. 4).

Further, Canada's CEOs raised concerns about the need to hire and train significant numbers of temporary staff for an election – all of whom are responsible for processing personal information, and whom may only have only a tangential relationship to the agency. For example, Elections Canada added 285,000 temporary staff to their payroll in advance of the 42nd Federal General Election (A.M Delisle, personal communication, June 22, 2016) and in British Columbia one in every 125 of the 4.5 million residents of the province are employed by Elections BC in the days and weeks surrounding a provincial general election (K. Archer, personal communication, March 22, 2016). These staff receive a few hours of training and their employment is typically just a few days in duration. The challenge for election administrators is how to effectively communicate and implement effective processes, best practices and training in privacy management in this unique environment (personal communications: M. Boda, March 10, 2016 and S. Verma, March 23, 2016, G. Essensa, April 28, 2016). A breach due to human error, old habits, ignorance or malicious conduct, can have a significant impact on the agency's reputation (K. Archer, personal communication, March 22, 2016 and S. Verma, personal communication, March 23, 2016), and there is an expectation of extraordinary compliance. For example, during the 2011 Enumeration in Alberta, three enumeration binders were mislaid affecting 781 voters (CBC News, 2011, October 24). These breaches garnered widespread media attention (CBC News, 2011, October 24) despite representing just one half of one percent of the enumeration binders in the field during that event (G. Resler, personal communication, March 9, 2016). Further, the ballot box containing the voting book that was lost during British Columbia's 2013 Provincial General Election affected just one of 10,518 general voting books (Elections BC, Statement of Votes, 2013, p. 2). This represents a compliance rate of 99.9905% and still it is "…the kind of situation in which the reputation of the organization can be called into question" (K. Archer, personal communications, March 22, 2016).

Finding Balance

Another theme resulting from the interviews is the need to define and then strike a balance between operational responsibilities and compliance with privacy policy and statute. This section has already discussed what can happen when privacy protections are weak. The other side of this equation occurs when an organization attempts to implement rigid privacy policies which impede operations or stifle innovation.

Future Plans

When asked about future plans for their privacy portfolios there was almost no consistency among Canada's EMBs (see Figure 7, p. 41), however several expressed an understanding of the "dynamic nature" of privacy program management and this was reflected in their plans. For example, Elections British Columbia plans to modify their privacy framework to reflect recent statutory change, operational innovations, additional staff training and records management (K. Archer, personal communications, March 22, 2016) and Elections Quebec plans to review all of their information systems in acknowledgement of the fact that the systems were developed at a time when privacy and security was a less prominent feature of their work (T. Forget, personal communications, April 4, 2016).

Figure 8 – Summary of Key Findings

Literature Review	• Privacy is "rooted in ancient religions, texts and cultures" and is connected to human rights (Klein, 2012) • Modern concepts of information privacy have emerged from the abuses of world war two and the development of powerful new technology (Klein, 2012) • Statute is designed to balance protection of personal information with national security and commercial competitiveness (McLennan and Schick, 2007) • Canada's FPT jurisdictions follow Europe's comprehensive data protection model which is enforced by an independent commissioner or ombudsperson responsible for ensuring compliance, investigating alleged breaches, and acting as a liaison for data protection issues (Klein, 2012) • Similar sets of foundational principles focused on individual rights are the building block to most privacy management programs (i.e. consent, limiting collection, limiting use, disclosure and retention) • Many of Canada's DPAs have published tools and reports to guide public agencies in the development and maintenance of their privacy management programs • There is no one-size-fits-all for privacy management, but public bodies are expected to establish "reasonable protections" and provide evidence of a privacy management program in the event of a breach (OIPC BC, n.d.)
Jurisdictional Scan	• DPAs have called for public agencies to inform individuals of privacy rights and organizational privacy controls • Most of Canada's EMBs share little or no information regarding their privacy management programs • Agencies with established privacy management programs (including EBC) provide some information about their privacy management programs – but the information is universally incomplete and/or difficult to find
Interviews	• There is limited consistency among EMBs in relation to their privacy management programs • EMB's privacy goals are substantially similar (maintain public trust, reduce risk, comply with statute) • Canada's EMBs appear to sit on a continuum with the absence of any privacy activity on one extreme and substantive formalized privacy programs on the other • The catalyst for most privacy management activities at Canada's EMBs was a series of high-profile breaches between 2011 and 2013 • EMBs share several common challenges: o Dramatic increases in staffing at key points in election cycle o Highly distributed model of election administration o Very high expectations from stakeholders for compliance o Need to balance privacy obligations and operational requirements o Limited internal privacy expertise/bench-strength o Statutory requirements to disclose personal information to electoral participants who may or may not have the capacity to maintain their own privacy programs or an understanding of their obligations EMBs share several common opportunities: o New technology allows for new controls and processes o Engagement with DPAs (and fellow independent officers) o Knowledge-sharing and collaboration

Opportunities

While much of the focus has been on common challenges, the privacy portfolio also presents opportunities. For example, as technology replaces paper, administrators can apply more controls for who can access the data, and can encrypt the data to protect it if it is lost. This is a substantial improvement on the heavily paper-based processes in place in most of Canada's EMBs. This portfolio also invites CEOs to further engage with privacy commissioners (or ombudspersons), a relationship that many of the interviewees appreciate, and it can support additional cross-jurisdictional knowledge sharing opportunities.

Looking Across the Findings: Overarching Themes

There are three overarching themes resulting from this research. First, there is great diversity between Canada's federal, provincial and territorial EMBs (Elections Canada, 2015, August 30), and thus great diversity among their privacy management activities. While some have little or no program to speak of, others have begun to develop formal and informal privacy management programs. Almost all of this work was triggered by a series of highly publicised breaches emerging from Canada's EMBs between 2011 and 2013 (personal communications: M. Boda, March 10, 2016, G. Resler, March 9, 2016 and K. Archer, March 22, 2016), and to a lesser degree changes in statute (A.M. Delisle, personal communications, March 22, 2016), and efforts to simply be proactive (T. Forget, personal communications, April 4, 2016). Despite these differences, the goals shared by these agencies are consistent – to ensure compliance with statute, to maintain public trust and to limit privacy risk. This analysis suggests that Elections BC is performing well in this area, and that it is among the leaders in privacy management in Canada's EMBs.

The second overarching theme is that poor privacy management practices can result in significant consequences for the affected individuals, for the EMB, and for the legitimacy of the democratic institutions that the EMBs support. Specifically, the research demonstrates that poor privacy management practices have the potential to negatively affect democratic participation (Bennett et al., 2015, p. 4) and result in a decreased sense that the outcome of the election was fair (Karpowitz et al., 2011, p. 661). This in turn can have a knock-on effect on the legitimacy of the jurisdiction's political institutions (Balasko, 2015, pp. 65-66). Elections BC's 2013 breach affected just one of 10,518 general voting books (Elections BC, Statement of Votes, 2013, p. 2) and represented a compliance rate of 99.9905%. However, BC's CEO reported that it was "the kind of situation in which the reputation of the organization can be called into question" (K. Archer, personal communication, March 22, 2016). There is no room for complacency.

Finally, and related, despite the strength of some of the privacy management programs at Canada's EMBs, privacy and digital issues constitute a rapidly evolving landscape, and all EMBs must maintain privacy management programs that are reflective of ongoing (real or anticipated) statutory, operational and environmental changes. Such programs assist organizations in demonstrating that they are compliant with statute (and policy), foster a culture of privacy within the organization, help ensure effective resourcing for "training and education, risk assessment and monitoring, and auditing", and enhance the agency's trust and reputation (Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, 2012, p. 4). It is this last theme that presents the greatest challenge, and the greatest possible opportunity for future gains for the client.

The Next Wave of Election Privacy Management: Strategic Challenges for BC

Elections BC has a robust privacy management program, and the organization now readily discusses privacy obligations alongside other operational requirements. The agency can be considered a leader among Canada's EMBs from a privacy management perspective, and this research has revealed that aside from some minor changes to the website, that the client is currently performing very well from a privacy management perspective.

However, there is an acute awareness among the agency's senior leaders that the field of privacy is constantly evolving, and that the privacy management program must be rigorously and continuously maintained to reflect (real or anticipated) statutory and environmental change, public expectation and operational innovations. To remain current, and in keeping with agency's commitment to sharing knowledge and to good privacy management practices, it should consider supporting a national dialogue among Canada's EMBs on the subject of privacy management. The next section of this report sets out options for supporting such a dialogue.

8. OPTIONS, RECOMMENDATION(S), IMPLEMENTATION PLAN

Election administration is a profession with a relatively small number of Canadian practitioners and knowledge sharing between jurisdictions is a common and very important practice which promotes professionalism and continuous innovation. The information and privacy portfolio presents another opportunity for this type of cross-agency knowledge sharing and professional development which could include the use of a platform like the Canadian Election Resource Library (CERL); learning through interjurisdictional discussions, meetings or personnel exchange; inclusion of sessions on information privacy at annual conferences commonly attended by election administrators such as the Conference of Canadian Election Officials (CCEO) and the Council on Government Ethics and Laws (COGEL); and/or offering a module in a training and certification program for election administrators (K. Archer, personal Communication, March 22, 2016).

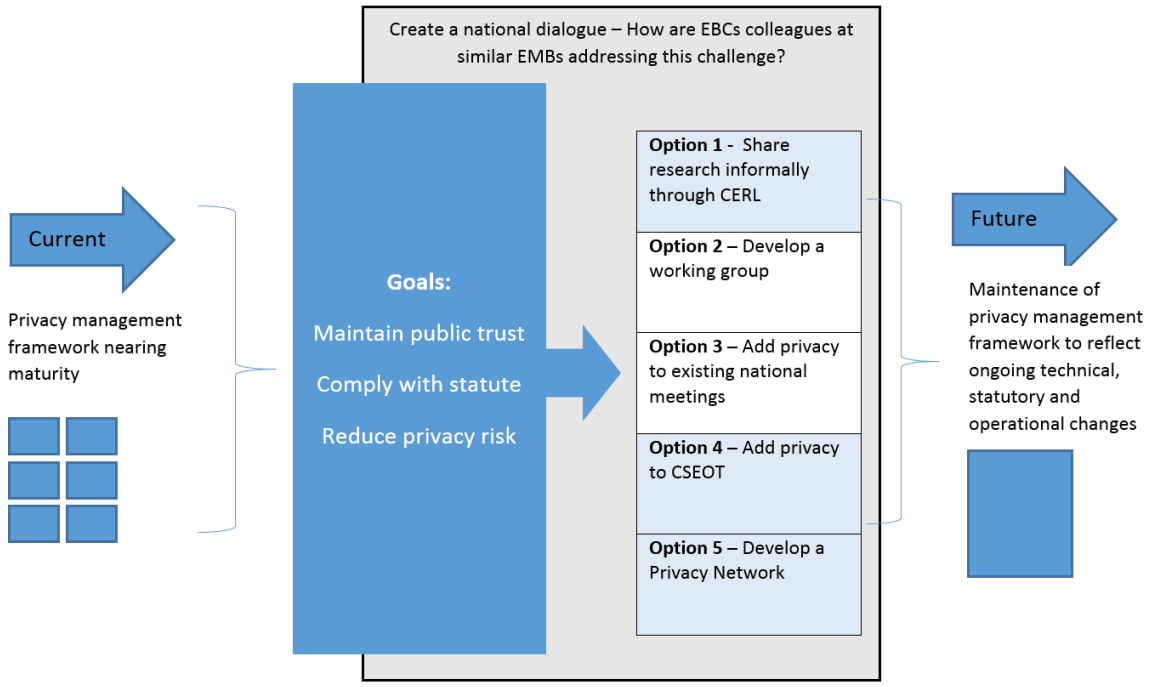
This section presents options for the client to consider. Each option assumes that to achieve Elections BC's stated goal of continuing to mature its privacy management program to ensure that the agency is compliant with statute, proactive in preventing breaches, and can effectively maintain public trust, that Elections BC will support a national dialogue on the subject (See Figure 9, next page, for illustration).

The proposed options for such knowledge-sharing include:

1. **Share research informally through the Canadian Election Resource Library (CERL).** This option places a priority on limiting effort and financial investment while still supporting a national dialogue on the subject of privacy. It supports a conservative approach by simply placing this and other research and tools on an electronic resource library shared by all of Canada's EMBs.

2. **Develop a working group on information and privacy management.** This option would see the establishment of a working group, similar to the Recruitment and Training Working Group and the Technology Working Group established by Canada's CEOs. This option supports thorough, active and in-person dialogue on the subject, and would require a modest investment in time and resources to establish and maintain.

Figure 9 – Achieving the Future State



3. **Encourage the addition of privacy on the agenda of annual conferences and meetings commonly attended by election administrators.** This option supports senior-level and in-person dialogue on the subject. It would require a moderate investment in time and resources to prepare and lead discussions at meetings such as the Conference of Canadian Election Officials (CCEO), the Advisory Committee of Electoral Partners (ACEP) and/or the Council on Government Ethics and Laws (COGEL).

4. **Add privacy to the Canadian Society of Election Official Training curriculum.** This option supports in-depth and in-person dialogue on the subject as part of a three-day training course. It would require a significant investment in time and resources to prepare and lead, and also promises the greatest benefit for participants.

5. **Develop a privacy network across all of Canada's EMBs**
This option is similar to the working group in that it supports thorough, active and in-person dialogue on the subject, however, it is more informal than the working group. It would simply connect individuals with privacy responsibilities from all of Canada's EMBs and allow them to meet virtually or in person to discuss issues and experiences related to privacy.

Following a more detailed review explanation of each option, they will be weighed against the following criteria:

- **Practicality/stated goal:** Whether the option is realistic, achievable and likely to meet the stated goal of a national dialogue to further participants' privacy management programs

- **Implementation effort:** Initial effort from the client to implement
- **Ongoing effort:** Ongoing effort from the client to maintain
- **Cost:** Total cost to establish and maintain
- **Time:** Time to implement

The options will be compared with each other and a recommended approach will be identified for Elections BC to consider, along with an implementation plan.

8.1 Option 1 – Share research through CERL

Canada's EMBs contribute to a digital platform called the Canadian Election Resource Library (CERL). This tool allows election administrators to post existing reports, research and questions to other participating election administrators, and it could be used to support a national dialogue on privacy management as well. Its great advantage is that it would take next to no effort to initiate or maintain, and there would be no new costs associated with this strategy. It could also be used to target individuals responsible for the portfolio in their respective jurisdictions. However, while all of Canada's EMB's support the tool, currently, use within each agency is inconsistent and participation is often focussed on requests for information.

8.2 Option 2 – Develop a working group

Many of Canada's EMBs participate on working groups established by Canada's federal, provincial and territorial CEOs including the Recruitment and Training Working Group and the Technology Working Group. This option would see the establishment of a new working group focused on privacy management. It would be guided by an agenda, a formal output, a common policy and/or terms of reference. The primary advantages are the opportunity for thorough discussions on the topics with the individuals responsible for or most interested in the portfolio, the ability to get the program up and running quickly, the ability to meet on an ad hoc basis as issues arise, and the opportunity for EMBs to develop additional bench-strength by encouraging interested staff to attend. If selected, this option would take a moderate effort to initiate and maintain, and there could be some cost associated with attending meetings (although this could also be conducted through conference or video call). The primary drawbacks are the unpredictable nature of the success of such working groups (without sustained interest some atrophy over time), and the need for Elections BC to commit staff time to "get it going". This effort would include the development of content, meeting coordination, and ongoing communication with Canada's EMB's to ensure continued interest and support. This option could take up to a year to establish the program as it would require endorsement of the CCEO/ACEP, and Elections BC is nearing a provincial general election which will limit their capacity for such activities.

8.3 Option 3 – Add privacy to existing EMB meeting agendas

This option would see British Columbia's CEO encourage the addition of privacy on the agenda of annual conferences and meetings commonly attended by election administrators. Like option two, this option supports active and in-person dialogue on the subject of privacy management. It would require a moderate investment in time and resources to prepare and lead ad-hoc discussions at meetings such as the Conference of Canadian Election Officials (CCEO), the Advisory Committee of Electoral Partners (ACEP) and/or the Council on Government Ethics and Laws (COGEL). This option would be relatively low-cost as representatives from most EMBs are typically in attendance, meetings are already planned,

and the discussions could be led by different EMB's thus distributing the effort to prepare for such discussions. There are two primary drawbacks to this option. First these meetings are typically attended by the most senior officials in each EMB, and may not include the individual(s) responsible for privacy in each jurisdiction. Also, due to the number of items on these agendas, the time allocated to discuss emerging issues related to privacy may be limited.

8.4 Option 4 – Add privacy to the CSEOT curriculum

In July 2015, Canada's CEOs endorsed the establishment of the Canadian Society of Election Official Training designed to meet the training needs for permanent staff in federal, provincial and territorial election administration agencies in Canada. The program is supported as a three-year pilot project of the CCEO, for the period July 2016 to July 2019, and the program committee is chaired by the Chief Electoral Officer of British Columbia. The program does not currently contain a privacy component. However, this option would see the inclusion of a three-day privacy course as part of the program, and the participation of one or more of Elections BC's privacy officers as training instructors. This option is by far the most labour intensive as the model for these courses is to invite three individuals (EMB staff or consultants) to each prepare a full-day of training on the training subject. Travel costs would be covered by the society, however Elections BC's instructor(s) would need to be given some space to prepare and deliver such a program. The significant advantage to this option is the opportunity for thorough discussions, table-top exercises, and formal and informal learning on the topic of privacy management with the individuals responsible for each agency's portfolio. It would also encourage the development of "bench-strength" within participating agencies (including Elections BC). The significant drawbacks to this option are that the training is expected to be delivered just twice per year, there is a cost to attend the training, and the subjects for the next several training sessions have already been established such that it may not be possible to add a privacy course to CSEOT program for some time.

8.5 Option 5 – Develop a privacy network across all of Canada's EMBs

This option is similar to the working group in that it supports thorough, active and in-person dialogue on the subject, however, it differs from the working group as it would be informal and would not include an agenda, a formal output, a common policy and/or terms of reference. It would simply connect individuals with privacy responsibilities from all of Canada's EMBs and allow them to meet virtually or in person to discuss issues and experiences related to privacy. The primary advantages are the opportunity for thorough discussions on the topics with the individuals responsible for the portfolio, the ability to get the program up and running quickly, the ability to meet on an ad hoc basis as issues arise, and the opportunity for EMBs to develop additional bench-strength by encouraging interested staff to attend. This option would require a modest investment in time and resources to establish and maintain.

8.6 Comparing the Options and Recommended Approach

The five options presented involve sharing research informally through the Canadian Election Resource Library (CERL), developing a working group on information and privacy management, encouraging the addition of privacy on the agenda of annual conferences and meetings commonly attended by election administrators, adding privacy course to the Canadian Society of Election Official Training curriculum and developing a privacy network for privacy professionals. This section, (see Figure 10, page 53) briefly summarizes the options for developing a national dialogue on privacy management by comparing the

options against several criteria including whether the option is realistic, achievable and likely to meet the stated goal, effort to implement and maintain, cost and time.

As illustrated in Figure 10 (next page), Option 5 (developing a privacy network across EMBs), provides a significant advantage in the opportunity for thorough discussions and informal learning on the topic of privacy management, while also requiring limited time and resources to implement. The addition of Option 1 (sharing through CERL) would see the creation of a national repository of tools and research with very little effort, and the network could reinforce its use. Further, Option 4 (adding privacy training to CSEOT) while labour-intensive for the client, would establish a formalized training module specific to the election business (a significant benefit to participants and the EMBs they work for).

Options 2 (developing a working group) and 3 (adding privacy to existing EMB meeting agendas) could still be taken up by the client as opportunities arise, however this report recommends that the client's focus be on both Options 4 (with Option 1) and Option 5 to ensure alignment with the stated goals.

8.7 Implementation Plan

This section provides an implementation plan for Options 4 and 5 (see Figure 11, p. 54). The implementation of both options comprise four phases: preliminary, planning, implementation, and evaluation to be delivered over the next 18 months. Appendices F-H provide tools to support training, discussions and table-top exercises associated with Option 5.

8.8 Summary

The purpose of this section was to provide Elections BC with a recommended approach to foster a national dialogue on privacy management among Canada's EMBs and to offer plans for implementation. The selected options are in response to the empirical research contained in this report, and will ensure that Elections BC can maintain their privacy management program in an environment that is rapidly evolving.

Figure 10 – Comparison of Options

	Option 1 Canadian Election Resource Library (CERL)	**Option 2** Working group	**Option 3** Annual conferences and meetings	**Option 4** Canadian Society of Election Official Training (CSEOT)	**Option 5** Develop a privacy network across EMBs
Motivations	Establish a national dialogue on privacy management				
Advantages	Very little effort to initiate or maintain; no costs associated with implementation; could target the individuals responsible for the privacy portfolio; readily accessible resource	Thorough discussions with the individuals responsible for the privacy portfolio; meetings could be scheduled on a regular basis, and could be ad hoc in response to emerging issues	High-level and in-person dialogue on the subject of privacy management at the senior level	Thorough discussions and exercises with the individuals responsible for privacy; development of "bench-strength" within participating agencies, training is specific to the election business	Informal, very little effort to initiate or maintain; no costs associated with implementation; could target the individuals responsible for the privacy portfolio
Disadvantages	Use of the tool is inconsistent and participation is often focussed on requests for information	Unpredictable nature of the success of such working groups; need for Elections BC to commit resources to "get it going"	May not include the individual(s) responsible for privacy; time allocated to discuss privacy may be limited	Labour intensive to develop and maintain a full-day training course	Informal - no agenda, formal output or a common policy
Criteria					
Practicality/ stated goal (is it likely to meet the stated goal of a national dialogue on privacy management)	Limited – due to limited use of the tool	Yes – Would invite thorough discussions with the individuals responsible for the privacy portfolio	Yes – High-level discussions with senior officials and/or individuals responsible for the privacy portfolio	Yes – Would invite thorough discussions with the individuals responsible for the privacy portfolio	Yes – Would invite thorough discussions with the individuals responsible for the privacy portfolio
Implementation effort (Initial effort from the client to implement)	None – simply post on web-based forum	Moderate – Involves the development of content and meeting coordination	Moderate – Involves investment in time and resources to prepare and lead	Significant – Labour intensive to develop and maintain a full-day training course	Moderate – involves some time to set up the network and create a space for shared tools
Ongoing effort (Ongoing effort from the client to maintain)	Very limited	Moderate – Involves the development of content; meeting coordination; and, ongoing communication	Moderate – Involves investment in time and resources to prepare and lead ad-hoc discussions at meetings	Moderate – Involves investment in time and resources to maintain and lead full-day training sessions	Very limited
Cost (Total cost to establish and maintain)	None	Moderate – May involve some net-new staff travel	Moderate – May involve some net-new staff travel	Moderate – May involve some net-new staff travel	Moderate – May involve some net-new staff travel
Time (Time to implement)	Very limited	Could take up to six months to establish the program as it would require endorsement of the CCEO/ACEP	Would follow existing meeting schedule	Could take two or more years to get on the CSEOT agenda as some of the programming is already established	Rapid - could be rolled out quickly once a decision to proceed is made

Figure 11 – Implementation Plan

Phase	Task – Privacy Network	Task – CSEOT Training Program	Timeline
1. Preliminary	Assess Elections BC's organizational capacity to establish a national privacy network ("privacy network") Develop a proposal for the structure of the privacy network (i.e., invitees, frequency and length of meetings/discussions, location of meetings/discussions, location for shared resources etc.) Share this research and the proposal for the structure of the network with Canada's CEOs and ask them to consider establishing a national privacy network (at the next CCEO/ACEP conference)	Develop a proposal encouraging the CSEOT steering committee to include a privacy course in the existing training agenda Send this research and a the proposal to the CSEOT steering committee for consideration	July - December 2016
2017 Provincial General Election – Elections BC staff are fully engaged in event delivery			January 2017-May 2017
2. Planning	If the privacy network is endorsed by the CCEO/ACEP, reach out to all EMBs to invite them to identify individual participants Develop a list of participants Invite the participants to a "virtual" meeting or conference call to discuss their programs, their needs, and their current challenges. Establish a central repository for tools, policies, processes and training materials on CERL (see option 1)	If added to the CSEOT agenda, all administrative and planning details will be managed by the CSEOT committee and affiliated staff. Planning activities include registration, meeting space and accommodation planning, selection of speakers, meal and travel planning etc. If invited to lead one of three days of training, EBC would prepare presentation materials and training exercises.	June 2017
3. implementation	Moderate a "virtual" or conference call meeting of the privacy network to initiate the program. Invite participants to publish any privacy resources they have (i.e. tools, policies, training materials etc.) on CERL	EBC to lead one of three days of privacy training	July 2017
4. Evaluation	Evaluate the program to determine if the privacy network is meeting the needs of the client and the group, and make a recommendation as to whether to continue the activities of the network. If a decision to proceed is made, repeat phases 2-4.	Evaluate the program to determine if the training is meeting the needs of the client and the group, and make a recommendation as to whether to repeat If a decision to conduct another privacy training program is made, repeat phases 2-4.	December 2017

9. CONCLUSION

This project was designed to provide context for understanding the state of art in privacy management in Canadian election administration agencies, and to identify opportunities for the continued development and implementation of good privacy management practices at Elections BC by answering the following questions: What are Canada's EMBs doing in this space, what common challenges are these agencies facing, and what can Elections BC do to improve their privacy management program?

This research found that there is great diversity between Canada's federal, provincial and territorial EMBs (Elections Canada, 2015, August 30), and as a result, there is also great diversity among their privacy management activities. While some have little or no program to speak of others have begun to develop formal and informal privacy management programs which if maintained can "help minimize the risk of …breaches, maximize the organization's ability to identify and address …incidents, and minimize their damage" (Offices of the Information and Privacy Commissioners of Alberta, British Columbia and Canada, April 2012, p. 4). This research also revealed that the awareness of privacy management responsibilities among Canada's EMBs was increased significantly as a result of highly publicised breaches emerging from Canada's EMBs in 2011-2013 (personal communications: M. Boda, March 10, 2016, G. Resler, March 9, 2016 and K. Archer, March 22, 2016), and to a lesser degree changes in statute (A.M. Delisle, personal communications, March 22, 2016), and efforts to simply be proactive (T. Forget, personal communications, April 4, 2016).

Some of the privacy management challenges identified by Canada's CEOs as part of this research included a need to dramatically increase their staffing compliment in very short periods of time; the very high expectations from stakeholders for compliance; the highly distributed model of election administration; the need to balance privacy obligations and operational requirements; the need to adjust to new environmental, statutory and technological requirements; the need to acquire or develop expertise in this area; and the need to disclose personal information with electoral participants who may or may not have the capacity to maintain their own privacy management programs including political parties, elected officials, candidates, and others.

Poor privacy management can weaken confidence that the outcome of the election was fair (Karpowitz et al., 2011, p. 661), and a "hit" on an EMB's credibility can have a knock-on effect on the legitimacy of that jurisdiction's political institutions (Balasko, 2015, p. 65-66) and on electoral participation (Bennett C. and Bayley R. , 2012). In this rapidly evolving landscape EMBs must anticipate new issues and continue to develop new capabilities. Elections BC's privacy management program should be rigorously and continuously maintained to reflect (real or anticipated) statutory and environmental change, public expectation and operational innovations. While Elections BC has a robust framework in place and is currently performing strongly in this space, in order to stay current and develop appropriate responses, the agency (and other participating Canadian EMBs) can benefit from an ongoing national dialogue on the subject of privacy which comprises both an informal knowledge-sharing network and a formal training module in an existing training program for EMBs.

A study similar to this one, two to five years from now may yield entirely different results and provide an interesting comparison for better understanding the evolution of these programs. A follow-up study may also draw participation from a larger number of agencies and/or include French language materials. Detailed research into the causes of privacy breaches (of all sizes) at EMBs and the development and evaluation of shared training tools may also be worthwhile.

REFERENCES

Altschuld, J., & Kumar, D. (2010). A Generic Needs Assessment Model and Steps. *Needs Assessment: An Overview.* (pp. 1-21). Thousand Oaks, CA: Sage Publications, Inc. Retrieved from http://sk.sagepub.com.ezproxy.library.uvic.ca/books/download/needs-assessment-an-overview/n2.pdf

Archer, K. (2014). *Elections BC: Report of the CEO on Recommendations for Legislative Change, October 2014*. Retrieved from http://www.elections.bc.ca/docs/rpt/2014-CEO-Recommendations.pdf

Balasko, R. (2015). The Nature and Functions of Electoral Management Bodies. In G. Tardi (Ed.), *The Informed Citizens' Guide to Elections: Electioneering Based on the Rule of Law*: *A special issue of the Journal of Parliamentary and Political Law*. (pp. 65-78). Toronto, ON: Carswell, Thomson Reuters.

Bennett, C.J. (2015). Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance & Society*. 13(3/4): 370-384. Retrieved from http://library.queensu.ca/ojs/index.php/surveillance-and-society/index

Bennett, C. J. and Bayley, R. (2012, March 28). Canadian Federal political parties and personal privacy protection: A Comparative Analysis. Retrieved from https://www.priv.gc.ca/information/research-recherche/2012/pp_201203_e.asp

Boda, M.D. (2015, December 28). *Interpretation Bulletin, Provision of Birth Date Information on Election Period Lists of Voters Produced for Political Parties, Candidates and Election Officers*. Retrieved from http://www.elections.sk.ca/candidates-political-parties/bulletins-circulars/eskib---2015-01--voters-list-privacy-v1.0-final.pdf

Brown, J., Bevan-Baker, P., Biggar, P., Macewen, S., and Sherry, J. (2016, April 15). Special Committee on Democratic Renewal: First Report of the Second Session Sixty Fifth General Assembly: Recommendations in Response to the White Paper on Democratic Renewal – A Plebiscite Question. Retrieved from http://www.assembly.pe.ca/sittings/2016spring/reports/23_1_2016-15-04-report.pdf

Canada Elections Act, Revised Statutes of Canada, (2000, c. 9). Retrieved from http://laws-lois.justice.gc.ca/eng/acts/E-2.01/

Canadian Press (2013, June 8). *Elections BC looking for voting book from Vancouver-Langara riding*. Retrieved from http://www.theglobeandmail.com/news/british-columbia/elections-bc-looking-for-voting-book-from-vancouver-langara-riding/article12438589/

Catt, H., Ellis, A., Maley, M., Wall, A., and Wolf, P. (2014). Electoral Management Design: Revised Edition. *International Institute for Democracy and Electoral Assistance.* Retrieved from http://www.idea.int/publications/emd/loader.cfm?csModule=security/getfile&pageID=66788.

Cavoukian, A. (2012). *Elections Ontario's Unprecedented Privacy Breach: A Special Investigation Report.* Retrieved from https://www.ipc.on.ca/images/Findings/2012-07-31-Elections-Ont_1.pdf

Cavoukian, A. (2012, December). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices.* Retrieved from https://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf

CBC News. (2011, Oct. 24). *Alberta voter data goes missing.* Retrieved from http://www.cbc.ca/news/canada/edmonton/alberta-voter-data-goes-missing-1.1105846

CBC News. (2012, June 5). *Voter List Privacy Breach Contained, Says Commissioner*. Retrieved from http://www.cbc.ca/beta/news/canada/new-brunswick/voter-list-privacy-breach-contained-says-commissioner-1.1238405

CBC News (2012, June 6). *Laptop with Voter Information Stolen*. Retrieved from http://www.cbc.ca/shift/2012/06/06/laptop-with-voter-information-stolen/index.html

CBC News. (2012, July 31). *Privacy commissioner blasts Elections Ontario managers.* Retrieved from http://www.cbc.ca/news/canada/toronto/privacy-commissioner-blasts-elections-ontario-managers-1.1210627

CBC News. (2013, June 7). *Ballot box, voting book missing in Vancouver-Langara*. Retrieved from http://www.cbc.ca/news/canada/british-columbia/ballot-box-voting-book-missing-in-vancouver-langara-1.1328252

Constitution Act, Revised Statutes of British Columbia. (1996, C-66). Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_96066_01

DiCicco-Bloom, B. and Crabtree, B. (2006). Making Sense of Qualitative Research: The Qualitative Research Interview. *Medical Education*. 40: 314–321. Retrieved from http://onlinelibrary.wiley.com.ezproxy.library.uvic.ca/doi/10.1111/j.1365-2929.2006.02418.x/epdf

Densmore, R. (2013). *Privacy Management Program: Tools for Managing Privacy Within Your Organization*. Portsmouth, NH: International Association of Privacy Professionals.

Election Act, Revised Statutes of Alberta. (2000, C. E.1). Retrieved from http://www.qp.alberta.ca/1266.cfm?page=E01.cfm&leg_type=Acts&isbncln=9780779733903

Election Act, Revised Statutes of British Columbia (1996, c. 106). Retrieved from:

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96106_00

Election Act, Revised Statutes of Nova Scotia (2013, c. 17). Retrieved from https://electionsnovascotia.ca/sites/default/files/elections.pdf

Election Act. Revised Statutes of Ontario (1990, c. E.6) Retrieved from https://www.ontario.ca/laws/statute/90e06#BK44

Election Act, Revised Statutes of Prince Edward Island. (2015, c. E-1.1). Retrieved from http://www.gov.pe.ca/law/statutes/pdf/e-01_1.pdf

Election Act, Revised Statutes of Quebec. (2016, c. E-3.3). Retrieved from http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/E_3_3/E3_3_A.html

Election Act, Revised Statutes of Saskatchewan. (1996, C. E-6.01). Retrieved from http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/E6-01.pdf

Elections Act, Revised Statute of Manitoba. (2006, c. E30). Retrieved from http://web2.gov.mb.ca/laws/statutes/ccsm/e030e.php

Elections Act, Revised Statutes of New Brunswick. (1973, c. E-3). Retrieved from http://web2.gov.mb.ca/laws/statutes/ccsm/e030e.php

Elections Act, Revised Statutes of Newfoundland and Labrador. (1991, c. E-3.1). Retrieved from http://www.assembly.nl.ca/legislation/sr/statutes/e03-1.htm

Elections Act, Revised Statutes of Yukon. (2002, c. 63). Retrieved from http://www.bing.com/search?q=Yukon+election+act&src=IE-TopResult&FORM=IETR02&conversationid=

Elections Alberta. (2011, October). *News Release: Elections Alberta Works to Recover Enumeration Binders*. Retrieved from http://www.elections.ab.ca/wp-content/uploads/Lost_binder_October_24_2011.pdf

Elections Alberta (n.d.). *Privacy & Security.* Retrieved from http://www.elections.ab.ca/privacy-security/

Elections and Plebiscites Act, revised statutes of Northwest Territories. (2006, c. 15). Retrieved from https://www.justice.gov.nt.ca/en/files/legislation/elections-and-plebiscites/elections-and-plebiscites.a.pdf?t1457500700869

Elections BC (n.d.). *About Elections BC.* Retrieved from http://www.elections.bc.ca/index.php/about/ceo/

Elections BC. (n.d.). *Privacy.* Retrieved from http://www.elections.bc.ca/index.php/privacy/

Elections BC. (2013, August 20). *Annual Report 2012/13 and Service Plan 2013/14 - 2015/16.* Retrieved from http://www.elections.bc.ca/docs/rpt/AR1213SP1316.pdf

Elections BC. (2016, June). Report of the CEO on the 2016 Vancouver-Mount Pleasant and Coquitlam-Burke Mountain By-elections, February 2, 2016. Retrieved from http://www.elections.bc.ca/docs/rpt/2016-CEO-CQB-VMP-By-election-report.pdf

Elections BC (2013). *Statement of Votes: 40th Provincial General Election: May 14, 2013*. Retrieved from http://www.elections.bc.ca/docs/rpt/2013GE/2013-GE-SOV.pdf

Elections Canada. (2012, June 5). *A History of the Vote in Canada*. http://www.elections.ca/content.aspx?section=res&dir=his&document=chap2&lang=e.

Elections Canada. (2015, August 30). Compendium of Election Administration in Canada: A comparative Overview. Retrieved from http://elections.ca/res/loi/com/arc/com2015/june2015_e.pdf

Elections Canada. (2013). *Compliance Review: Final Report and Recommendations*. Retrieved from http://www.elections.ca/content.aspx?section=res&dir=cons/comp/crfr&document=p4&lang=e

Elections Canada. (2015, December 16). *Site Map*. Retrieved from http://www.elections.ca/content.aspx?section=aid&dir=sitemap&lang=e&document=index

Elections Manitoba. (2016). *Personal Security*. Retrieved from http://www.electionsmanitoba.ca/en/Voting/Personal_Security

Elections Manitoba. (2016). *Web Site information*. Retrieved from http://www.electionsmanitoba.ca/pd/About/Information

Elections New Brunswick. (2016). *Privacy*. Retrieved from http://www2.gnb.ca/content/gnb/en/admin/privacy.html

Elections Newfoundland & Labrador. (2016). *Home Page*. Retrieved from http://www.elections.gov.nl.ca/elections/

Elections Nova Scotia. (n.d.). *Privacy Policy and Routine Disclosure*. Retrieved from https://electionsnovascotia.ca/privacy-policy

Elections Nunavut. (2013). *Welcome to Elections Nunavut*. Retrieved from http://www.elections.nu.ca/apps/authoring/dspPage.aspx?page=home

Elections NWT. (n.d.). *Privacy.* Retrieved from http://www.electionsnwt.ca/privacy

Elections Ontario. (2014-2015). *Privacy of the Register*. Retrieved from http://www.elections.on.ca/en/voting-in-ontario/be-a-registered-elector/privacy-of-the-register.html

Elections Ontario. (2012, November). *Privacy Policy*. Retrieved from http://www.elections.on.ca/content/dam/NGW/sitecontent/2014/policies/Elections%20Ontario%20Privacy%20Policy.pdf

Elections Ontario. (2016). Proposal for a technology-enabled staffing model for Ontario Provincial Elections. Retrieved from http://www.elections.on.ca/content/dam/NGW/sitecontent/2016/2016-whitby-oshawa-by-election-report/Post%20Event%20Report%20-%202016%20By-election%20for%20ED%20100%20Whitby-Oshawa%20Report.pdf?src=Facebook

Elections Prince Edward Island. (2013, July 15). *Privacy.* Retrieved from http://www.electionspei.ca/index.php?number=1046928

Elections Quebec. (2016). *Access to Information.* Retrieved from http://www.electionsquebec.qc.ca/english/access-to-information.php

Elections Saskatchewan. (2015, February 2). *Elections Saskatchewan, Elections Canada sign information sharing agreement.* Retrieved from (http://www.elections.sk.ca/media/news-releases/information-sharing/

Elections Saskatchewan. (2016). *Privacy Policy.* Retrieved from http://vote.elections.sk.ca/privacy-policy/index.html

Elections Saskatchewan. (2016, Jan 22). *YouTube Video: Privacy.* Retrieved from https://www.youtube.com/watch?v=Fh1MWIjq4dI

Elections Yukon. (2016, March 19). *Welcome.* Retrieved from http://www.electionsyukon.gov.yk.ca/

Executive Council. (2015, June 1). *Office of the Information and Privacy Commissioner of Newfoundland and Labrador: Improving access to Information.* Retrieved from http://www.releases.gov.nl.ca/releases/2015/exec/0601n03.aspx

Freedom of Information and Protection of Privacy Act [FIPPA], Revised Statutes of British Columbia (1996, C-165). Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

Independent Panel on Internet Voting (2014, February). *Recommendations Report to the Legislative Assembly of British Columbia.* Retrieved from http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

International Association of Privacy Professionals. (2016). *Glossary of Privacy Terms.* Retrieved from https://iapp.org/resources/glossary/#paperwork-reduction-act

Karpowitz, C., Monson, J., Nielson, L., Patterson, L., and Snell, S. (2011, Winter). Political Norms and the Private Act of Voting. *Public Opinion Quarterly*. Volume 75, No. 4, pp. 659-685. Retrieved from http://poq.oxfordjournals.org.ezproxy.library.uvic.ca/content/75/4/659.full.pdf+html

Klein, K. (2012). *Canadian Privacy: Data Protection Law and Policy for the Practitioner (Second Edition*). Portsmouth, NH: International Association of Privacy Professionals.

Local Elections Campaign Financing Act [LECFA], Statutes of British Columbia (2014, C-18). Retrieved from: http://www.bclaws.ca/civix/document/id/complete/statreg/14018

Local Government Act, Revised Statutes of British Columbia (1996, C-323). Retrieved from:

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96323_00

MacLauchlan, H.W. (2015, July). *White Paper on Democratic Renewal*. Retrieved from http://www.gov.pe.ca/photos/original/democraticrenew.pdf

McGregor, G. (2015, November 19). *Elections Canada on the hook for monitoring employees' credit history after hard drive stolen*. Ottawa Citizen. Retrieved from http://ottawacitizen.com/news/politics/elections-canada-on-the-hook-for-monitoring-employees-credit-history-after-hard-drive-stolen

McLennan, J. and Schick, V. (2007). *"O, Privacy" Canada's Importance in the Development of the International Data Privacy Regime*. Retrieved from https://www.pillsburylaw.com/siteFiles/Publications/D9582DAA262F4B6491DF17D7CBE9C570.pdf.

Nunavut Elections Act. Revised Statutes of Nunavut, 2002, c. 17). Retrieved from http://www.gov.nu.ca/sites/default/files/gnjustice2/conssnu2002c17.pdf

Office of the Information and Privacy Commissioner for Alberta (OIPC). (2016). *How to Report a Privacy Breach*. Retrieved from https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx

Office of the Information and Privacy Commissioner (OIPC) for Alberta in partnership with the OIPC of BC and the OIPC of Canada. (April 2012). *Getting Accountability Right with at Privacy Management Program.* Retrieved from https://www.oipc.ab.ca/media/383671/guide_getting_accountability_with_privacy_program_apr2012.pdf

Office of the Information and Privacy Commissioner for British Columbia. (2015). *News Release: Statement from B.C. Information and Privacy Commissioner regarding proposed amendments to Bill 20 (Election Amendment Act)*. Retrieved from https://www.oipc.bc.ca/news-releases/1792

Office of the Information and Privacy Commissioner for British Columbia. (2012, March). *Privacy Breach Checklist.* Retrieved from https://www.oipc.bc.ca/media/15062/oipc_privacy_breach_checklist.pdf

Office of the Information and Privacy Commissioner for British Columbia. (n.d.). *Accountable Privacy Management in BCs Public Sector.* Retrieved from https://www.oipc.bc.ca/guidance-documents/1545

Office of the Information and Privacy Commissioner for British Columbia. (2015, October). *A Guide to B.C.'s Personal Information Protection Act.* Retrieved from https://www.oipc.bc.ca/guidance-documents/1438

Office of the Privacy Commissioner (OIPC) of Canada (May 2014). *Fact Sheets: Privacy Legislation in Canada.* Retrieved from https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp

Office of the Information and Privacy Commissioner (OIPC) of Ontario (n.d.). *Privacy Breach Protocol, Guidelines for Government Organizations.* Retrieved from https://www.ipc.on.ca/images/Resources/Privacy-Breach-e.pdf

Office of the Information and Privacy Commissioner of Newfoundland and Labrador (2016, March 9). Commissioner Releases Third Quarter Privacy Breach Notification Statistics. Retrieved from http://www.releases.gov.nl.ca/releases/2016/oipc/0309n06.aspx

Palinkas, L., Horwitz, S., Green, C., Wisdom, J., Duan, N., and Hoagwood, K. (2013, November).

Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. Retrieved from http://download.springer.com.ezproxy.library.uvic.ca/static/pdf/16/art%253A10.1007%252Fs10488-013-0528-y.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs10488-013-0528-y&token2=exp=1458196684~acl=%2Fstatic%2Fpdf%2F16%2Fart%25253A10.1007%25252Fs10488-013-0528-y.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Farticle%252F10.1007%252Fs10488-013-0528-y*~hmac=a5f0a20107133998d81a34c57c33d708fa258998f20447814a1cbfc6d8bbb3d7

Privacy Commissioner of Canada. (2005). *Learning from a Decade of Experience: Quebec's Private Sector Privacy Act*. Retrieved from https://www.priv.gc.ca/information/pub/dec_050816_e.pdf

Province of British Columbia (2015, March 24). *Information Bulletin: Election Act amendments provide increased voter accessibility.* Retrieved from https://archive.news.gov.bc.ca/releases/news_releases_2013-2017/2015JAG0070-000391.htm

Recall and Initiative Act, Revised Statutes of British Columbia (1996, C-398). Retrieved from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96398_00

Referendum Act, Revised Statutes of British Columbia (1996, C-400). Retrieved from:

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_96400_01

Swire, P. and Ahmad, K. (2012). *Foundations of Information Privacy and Data Protection: A survey of Global Concepts, Laws and Practices*. Portsmouth, NH: International Association of Privacy Professionals.

Taylor, B. (1973, September 27). Don't foul up this time out: Get your name of the voters list. *Montreal Gazette*. Retrieved from https://news.google.com/newspapers?nid=1946&dat=19730927&id=phMyAAAAIBAJ&sjid=96EFAAAAIBAJ&pg=996,3050682&hl=en

Thiry, M. (2010). Chapter 2: Organizational Context. *Program Management. Gower Publishing, England.* Retrieved from http://reader.eblib.com.ezproxy.library.uvic.ca/(S(fzmrnxa3xg54kgtodzufjtub))/Reader.aspx?p=564132&o=38&u=md9InDffLKGfg%2bOFvWozhQ%3d%3d&t=1458455593&h=09AC6FAE9EEA060BC53473C82DC58325FB8BBF42&s=43248792&ut=78&pg=1&r=img&c=-1&pat=n&cms=-1&sd=2#

Tracy, S. (2010). Eight "Big –Tent" Criteria for Excellent Qualitative Research. *Sage Journals.* 16(10) 837–851. Retrieved from http://qix.sagepub.com.ezproxy.library.uvic.ca/content/16/10/837.full.pdf+html

University of Victoria. (2015). *Human Research Ethics: Exemptions from Human Research Ethics.* Retrieved from http://www.uvic.ca/research/conduct/home/regapproval/humanethics/

APPENDICES

Appendix A – Email Invitation to Study Participants

Hi, <NAME>

As an academic exercise toward my Master of Public Administration program through the University of Victoria, and as part of my work at Elections BC, I am in the process of developing a foundational paper, a training module, and case studies on information and privacy considerations for Canadian election administrators. The materials will comprise the information and privacy best practices applicable to Canada's EMBs and address how these best practices can be effectively implemented.

I would like to invite you to participate in this research in your capacity as CEO of <JURISDICTION> - you may also identify a delegate within your organization. Participation is voluntary and any information collected as part of the interview will not be specifically attributed to your agency unless express consent is given. The final materials will be shared with the project client, Dr. Keith Archer, CEO of British Columbia, Canada's EMBs, Elections B.C.'s partner agencies and the faculty associated with this project. There are no professional repercussions to individuals who choose not to participate.

Voluntary participation in the interview will require approximately 30-minutes. This is a semi-structured interview which will begin with the following questions:

1. Can you please describe your privacy program?

2. What contact has your agency had with the information and privacy regulator in your jurisdiction since 2011?

3. What specific information and privacy measures has your agency taken since 2011?
    - What was the catalyst for this work?
    - If no work was undertaken, why?
    - If an assessment of your information and privacy program has been undertaken, what were the primary recommendations?

4. What, if any, publicly reported information/privacy breaches have occurred in your agency since 2011?

5. What information and privacy activities are planned for your agency for the next 12 months and/or beyond?

6. What is the greatest challenge faced by your agency regarding information and privacy management?

7. Has privacy changed your work, or that of the agency, significantly? If so, in what ways?

8. What changes in relation to the provision of information about voters to parties and candidates, the maintenance of personnel information, interactions with field staff, etc. have occurred in your jurisdiction in recent years?

I have attached a consent form for your review and consideration and I look forward to hearing from you whether you or a delegate would be willing to participate in this research.

Feel free to contact me if you have questions about this study. You may also contact Dr. Evert Lindquist (Supervisor) at 250-721-8416 or Dr. Keith Archer (Client) at 250-952-6226.

Regards,
Amie Foster

Appendix B – Email Follow-up to Study Participants

Hi, <NAME>:

I hope you are having a good week.

This is just a quick follow-up regarding my invitation to participate in this research study. I look forward to hearing from you and I am happy to answer any questions you have.

Regards,
Amie

Amie Foster
A/Manager, Communications
Elections BC

W: (250) 387-1709 C: (250) 213-6212/778-678-0181
Suite 100-1112 Fort St. Victoria, BC V8V 3K8

Appendix C – Interview Script

Hi, <NAME>,

Thank you for agreeing to speak with me.

As I explained in my earlier email, this research will be used to develop information and privacy resources associated with my position at Elections BC and will assist me in completing my Master of Public Administration program through the University of Victoria.

You are being asked to participate in this study because of your position as CEO, <OR DELEGATE> of <JURISDICTION>. Your participation in this interview is voluntary and is expected to take 30 minutes. Information collected will only be attributed to your agency with your consent and you may withdraw at any time without any consequences or explanation. The final outputs of this research will be shared with the project client, Dr. Keith Archer, CEO of British Columbia, Canada's EMBs, Elections B.C.'s partner agencies and the faculty associated with this project.
Before we begin the interview, do you have any questions about the signed consent form that you submitted or about this project more generally?

This is a semi-structured interview that is expected to take approximately 30 minutes:

1. Can you please describe your privacy program?

2. What contact has your agency had with the information and privacy regulator in your jurisdiction since 2011?

3. What specific information and privacy measures has your agency taken since 2011?
    - What was the catalyst for this work?
    - If no work was undertaken, why?
    - If an assessment of your information and privacy program has been undertaken, what were the primary recommendations?

4. What, if any, publicly reported information/privacy breaches have occurred in your agency since 2011?

5. What information and privacy activities are planned for your agency for the next 12 months and/or beyond?

6. What is the greatest challenge faced by your agency regarding information and privacy management?

7. Has privacy changed your work, or that of the agency, significantly? If so, in what ways?

8. What changes in relation to the provision of information about voters to parties and candidates, the maintenance of personnel information, interactions with field staff, etc. have occurred in your jurisdiction in recent years?

Thank you for speaking with me today. If you have any questions about your participation or the project more generally, please feel free to contact me at 250.952.6226 or at Amie.Foster@elections.bc.ca.

Thank you.

Amie Foster

Appendix D – Participant Consent Form

Participant Consent Form

Information and Privacy Considerations for Canadian Election Administrators

You are invited to participate in a study entitled Information and Privacy Considerations for Canadian Election Administrators that is being conducted by Amie Foster.

Amie Foster is a graduate student in the department of Public Administration at the University of Victoria, and an employee of Elections BC and you may contact her if you have further questions at 250-387-1709 or Amie.Foster@elections.bc.ca.

This research is a requirement for a degree in public administration. It is being conducted under the supervision of Dr. Evert Lindquist. You may contact Dr. Lindquist at 250-721-8416.

Purpose and Objectives
Heavily criticized breaches and ongoing advice from regulatory agencies have highlighted the need for EMBs to take reasonable steps to protect the personal information in their custody and control. This project will produce a foundational paper and course materials to help Elections BC, Elections BC's partner agencies and other Canadian EMBs address the unique information and privacy concerns, challenges, and responsibilities present in their work.

Importance of this Research
There is no training currently available which has been designed to address the unique information and privacy concerns, challenges, and responsibilities of Canadian election administrators, and many small jurisdictions do not have the resources to develop these programs "in-house". This project is intended to fill an important gap for Canada's EMBs.

Participants Selection
You are being asked to participate in this study because of your position as CEO (or delegate) of a Canadian EMB.

What is involved
If you consent to voluntarily participate in this research, your participation will include a 30-minute telephone interview, and the review and signature of this consent form. A transcript of the interview will be made.

Inconvenience
Participation in this study is expected to cause limited inconvenience to you, however, for jurisdictions conducting general elections this year, the researcher acknowledges that this may still be considered a significant request.

Risks
This study will not collect personal information. Contact information will be limited to business contact information. Interviewees may choose to share sensitive information regarding the breaches/vulnerabilities faced by their agencies. This information will be carefully protected using information and privacy best practices and technology fitted with safeguards in compliance with B.C.'s *Freedom of Information and Protection of Privacy Act*. Information collected will only be attributed to specific agencies with the express consent of the participant.

Benefits
Participants will have an opportunity to train their staff using the tools developed as part of this study. Small jurisdictions that do not have the resources to develop their own information and privacy programs stand to gain the most as this project will establish the foundational pieces from which they can build.
Registered voters will benefit by a reduction in information incidents and privacy breaches at Canadian EMBs as agencies' implement this research.
The state of knowledge regarding privacy in election administration will grow with from this research.

Compensation
No compensation for participation will be offered.

Voluntary Participation
Your participation in this research must be completely voluntary. If you do decide to participate, you may withdraw at any time without any consequences or any explanation. If you do withdraw from the study your data will destroyed and will not be

included in the foundational paper or training materials produced as part of this project/study. To withdraw from this study contact, Amie Foster by email at amie.foster@elections.bc.ca or by phone at 250-387-1709.

Anonymity
The nature or size of the sample from which participants are drawn could make it possible to identify individual participants. When in doubt, this information will be excluded from this research.

Confidentiality
Experiences will not be attributed to specific agencies without express consent:
I permit the researcher to attribute experiences to me or my agency (initials) _____
OR
I do not permit the researcher to attribute experiences to me or my agency (initials) _____

Despite safeguards designed to protect information from unauthorized access, use, disclosure, modification, loss or theft – some risk still remains due to human error or malicious intent. Reasonable safeguards in compliance with B.C.'s Freedom of *Information and Protection of Privacy Act (1996)* are in place to address this risk.
All information that is gathered for this research study will be maintained within Canada and on Canadian servers.

Dissemination of Results
The results of this study will be shared with the project client, Dr. Keith Archer, CEO of British Columbia, Canada's EMBs, Elections B.C.'s partner agencies and the faculty associated with this project.

Commercial Use of Results
There will be no commercial use of the results of this study.

Disposal of Data
Data from this study will be disposed of one year after acceptance of the final project by the University of Victoria. Electronic copies will be erased and paper copies will be confidentially destroyed.

Contacts
Individuals that may be contacted regarding this study include Dr. Evert Lindquist (Supervisor) at 250-721-8416 or Dr. Keith Archer (Client) at 250-952-6226.

In addition, you may verify the ethical approval of this study, or raise any concerns you might have, by contacting the Human Research Ethics Office at the University of Victoria (250-472-4545 or ethics@uvic.ca).
Your signature below indicates that you understand the above conditions of participation in this study, that you have had the opportunity to have your questions answered by the researchers, and that you consent to participate in this research project.

_____	_____	_____
Name of Participant	*Signature*	*Date*

A copy of this consent will be left with you, and a copy will be taken by the researcher.

Appendix E – Research Participants - Interviews

Jurisdiction	Status
Alberta	Glen Resler, CEO Drew Westwater, Deputy CEO Interview – March 9, 2016
British Columbia	Dr. Keith Archer, CEO Interview – March 22, 2016
Canada	Andrée Marie Delisle, Manager & Coordinator, Access to Information and Privacy (ATIP) Interview – March 22, 2016, email – June 22, 2016
Manitoba	Shipra Verma, CEO Interview – March 23, 2016
New Brunswick	Declined – Operational Demands
Newfoundland and Labrador	Bruce Chaulk, Assistant CEO Interview – April 1, 2016
Nova Scotia	Withdrew – Operational Demands
Nunavut	Sandy Kusugak, CEO Interview – April 8, 2016
NWT	Declined – No information to contribute/no program
Ontario	Greg Essensa Interview – April 28, 2016
PEI	Declined – No information to contribute/no program
Quebec	Thomas Forget, Bureau de l'access a l'information et de la protection des renseignements personnels (Access to Information and Protection of Privacy Office) Interview – April 4, 2016, email – June 16, 2016
Saskatchewan	Dr. Michael Boda, CEO Richard Hall, Research Analyst Interview – March 10, 2016
Yukon	Declined – Operational Demands

Appendix F – Proposed Training Program – Outline

TITLE - Privacy in Election Administration: Best Practices and Implementation Strategies

PURPOSE - To provide senior level election administrators with practical and task oriented exposure to privacy concepts and challenges present in professional practice

NUMBER OF PARTICIPANTS - 15 to 20

PRIMARY AUDIENCE -

- Headquarters staff from Canadian EMBs
- Staff from executive offices
- Senior managers
- Staff working in this area in the future
- Staff with direct privacy responsibilities
- Managers requiring a foundation in this subject area

RECOMMENDED TIME - Full day, 8:30 - 4:00 p.m.

RECOMMENDED TOOLS -

- Laptop, projector, screen and PowerPoint presentation
- Flip chart and markers
- Case study questions
- Buckets of discussion questions
- Bucket of individually wrapped candy
- Obnoxious trophy

RECOMMENDED READINGS -

Cavoukian, A. (2012). *Elections Ontario's Unprecedented Privacy Breach: A Special Investigation Report.* Retrieved from https://www.ipc.on.ca/images/Findings/2012-07-31-Elections-Ont_1.pdf.

Cavoukian, A. (2012, December). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices.* Retrieved from https://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf.

Office of the Information and Privacy Commissioner for British Columbia. (n.d.). *Accountable Privacy Management in BCs Public Sector.* Retrieved from https://www.oipc.bc.ca/guidance-documents/1545.

Proposed Program

A. Welcome and Orientation (30 minutes)
   - Pulse check
   - Overview
   - Ice breaker activity and presentation of trophy
   - Brief follow-up discussion

B. Seminar - Theoretical and Historical Background (45 Minutes)
   - PowerPoint presentation, seminar style

C. Break (30 minutes)

D. Seminar - Theoretical and Historical Background (75 minutes)
   - PowerPoint presentation, seminar style, continued

E. Meal Break (60 minutes)

F. Case Study Analysis (120 Minutes)

   Case One – The Case of the Smelly Guy and the Lady Who Couldn't Compute
   - 30 minutes to discuss and prepare a presentation
   - 5-10 minute presentation from each group (presenter randomly selected)
   - 10-15 minute class-wide follow-up discussion

   Case Two – The Case of the Voters that Showed Up
   - 30 minutes to discuss and prepare a presentation
   - 5-10 minute presentation from each group (presenter randomly selected)
   - 10-15 minute class-wide follow-up discussion

G. Break (15 minutes)

H. Small Group Discussion (60-75 minutes)
   - Facilitated small groups
   - Bucket with a series of discussion question to draw from
   - Individuals invited to add their own questions to the buckets
   - Groups can move through the questions as quickly or as slowly as they like

I. Review and Closing Comments (15 minutes)
   - Pulse check
   - Review
   - Invitation for any final questions
   - Thank you

Appendix G – Information and Privacy Case-Studies

Case Study Number 1 - The Case of the Smelly Guy and the Lady Who Couldn't Compute

You are an RO/DEO and your office opens next week. You have received several hundred applications for election official and office positions and a staff member who agreed to screen them mistakenly left them on the city bus. You know some of the resumes contain social insurance numbers, and that office staff have handwritten additional information on the materials such as position suitability, (less-than diplomatic) first impressions and/or whether or not to hire the individual based on past experience. You do not know the precise number of resumes/applications that have been lost, or who they belong to (although you might be able to identify the ones that were submitted via email). The materials have not been recovered.

Step One –
Assign each member of your team to one of the roles below. Chart the answers to the questions from the perspective of that individual. How do your perspectives differ? Discuss. When in doubt, use your own jurisdiction's policy/statute as the basis for your answer.

	1. How did you become aware of the breach?	2. What do you need to know?	3. Are you required to report this breach? If yes, to whom? When? How?	4. What is your role in the breach response? Timeframe?	5. What if any steps could you have taken to avoid this situation?
Staff member who misplaced the materials					
RO/DEO					
Director of Communications					
Privacy Officer					
CEO					

Step Two –
On the day after the breach was reported to headquarters, you learn that a concerned citizen has returned the seemingly intact backpack to the transit authority. Answer questions 2-4 in the table above again with this new information. How does your response change? Discuss.

Case Study Number 2 - The Case of the Voters that Showed Up

During annual meetings with your jurisdiction's political parties, they have indicated that they would like access to voter participation information both during and after events in an electronic format so that the information can be easily uploaded into their systems (i.e. Nation Builder etc.). The parties are in agreement that this information would support their get-out-the-vote efforts and ease the increasing challenge of recruiting the number of volunteers needed to support their data collection efforts at voting places (through scrutineers/observers).

Step One –
Using the jurisdiction (and applicable statute) of one of your team members (preferably one that does not already provide this information to political parties), determine if you can grant this request.

Step Two –
If you *can* grant this request answer the following questions:

- Where does the authority to grant this request come from? What, if any, authority do you have to ensure safeguards are in place? (Cite the statute/sections)
- What benefits could this service have for the agency?
- What challenges might it present (technical/operational)?
- What impact will it have on other stakeholders (i.e. voters)?
- Would you recommend that you change your processes to grant this request?
- Would you/could you put safeguards/limitations in place? If yes, what would they be?

If you *can't* grant this request answer the following questions:

- Where does the authority to deny this request come from? (Cite the statute/sections)
- What benefits could such a change have for the agency?
- What challenges could such a change present (technical/operational)?
- If granted, what impact would it have on other stakeholders (i.e. voters)?
- Would you recommend a change in statute so that you can support this request?
- Would you recommend safeguards/limitations? If so, what would they be?

Appendix H – Small Group Discussion Questions

You shipped a box of voting books to the DEO/RO ahead of the general election and the box never arrived at its destination. What do you do? (step-by-step)	How many breaches (or suspected breaches, big or small, have occurred at your agency in the last 12 months? (How do you know? Why don't you know?). Share some examples.
The warehouse just called, they have finished "putting the event to bed" and three laptops are still missing. What do you do? (step-by-step)	Do you have a privacy officer within your organization? If yes, are they a member of the senior management team? Why or why not?
Do you know how many voters lists are printed, distributed and destroyed/returned to your EMB as part of an electoral event? If no, why not? If yes, how do you track them?	You recently received a call from a neighbouring business that rented a set of office furniture from a local supplier. The desk contained thousands of records from the last general election. Is this a breach? What is your advice for next steps?
You have been asked to develop a new financial disclosure application, and you need to start the project now in order to complete it before the financial year end (and before the budget runs out). In passing, a colleague reminds you that a PIA may be required. What do you do?	You have designed a new program for enumeration that involves sending each household a list of voters registered at that address, and a request for them to correct any inaccuracies. Is this strategy OK under your statute/policy? Are there any privacy concerns?
Name three privacy implications of internet voting/technology in the voting place. Can any risks be addressed/mitigated? Are there broader concerns for your agency?	A privacy breach which includes payroll and performance information on a number of temporary election officials has resulted in a real risk of significant harm (RROSH) to the affected individuals - what advice would you give them?
What is a PIA? (Hint, it is not a "pain in the ass")	An encrypted laptop has been lost by the courier on the way to a field office. Is this a breach? What is your advice for next steps?
Name six different types of stakeholder that could be affected by a privacy breach at your agency.	Ask your colleagues a privacy question that has been simmering in your head or share a frustration associated with the subject.