CANADIAN REQUIREMENTS FOR PERSONAL INFORMATION PROTECTION

By

Stuart Rennie, JD, MLIS, BA (Hons.)

September 15, 2017

Project Underwritten by:
ARMA International Educational Foundation

www.armaedfoundation.org

Table of Contents

1.0 Introduction

In 2008 and 2009 the ARMA International Educational Foundation (AIEF) published two reports on requirements for personal information protection: *Requirements for Personal Information Protection Part 1: U.S. Federal Law* and *Requirements for Personal Information Protection Part 2: U.S. State Laws*.[i] These reports identify specific privacy laws that impact on records management programs.

Until this report, there has been no Canadian equivalent to these American state and federal law reports regarding personal information protection and its implication for records management. This report reviews the Canadian personal information statutes in Canada from a records management perspective.

Canada and the United States have different privacy regimes. Canada has a harmonized privacy regime grounded by similar statutes across Canada, based on the Organisation for Economic Co-operation and Development and the European Union (EU)'s data protection directive. In the EU, privacy is a fundamental right, accorded broad protection in EU statutes and case law. In the United States, privacy is protected by sector—characterized as a "safe harbour" or "shield"; that protection is less comprehensive than the EU.[ii] Compared to the EU and the United States, Canada occupies a middle ground regarding personal information.

Canada and the United States have a similar constitutional structure. Canada is a federal state under a constitutional monarchy. Canada has a federal government, 10 provinces and 3 territories. The Canadian Parliament and the provincial and territorial Legislative Assemblies meet regularly (usually at least once a year) to debate, enact, amend and repeal laws.

The United States also has a federal government and 50 states. The United States has the Congress, Senate and state legislatures that regularly convene to make and amend laws.

2.0 How Federal Law is Made

Federal law is made in the Parliament of Canada. The proposed law is called a bill. Bills can change or amend current law or repeal current law or create new law. The Parliament of Canada must pass the bill in both the House of Commons and the Senate. Either the House of Commons or the Senate may propose the bill.

It takes 6 stages for a bill to become law. First, is First Reading where the bill is introduced in either the House of Commons or Senate. Second, is Second Reading where the bill is debated and voted upon. Third, if the vote is affirmative, the bill passes to Committee stage. In Committee, members study each of the bill's clauses. The Committee may make amendments to the bill. Fourth, the Committee submits the bill as a Report. Fifth, the bill is debated at Third Reading. Once a bill reaches Third Reading, it is then sent to the second house of Parliament where the bill must pass through the same stages. If the second house proposes amendments to the bill, the first house must vote to pass those amendments; if the vote fails, the bill does not become law. Sixth, if the bill completes all these stages, it is enacted and given Royal Assent. The bill is now a statute. The statute comes into force on the date of Royal Assent, unless the statute itself states that it comes into force on some other day. Different provisions of a statute can come into force on different days. The statute itself may specify an exact date or may specify that the statute or provisions of it, will come into force at a future date specified by order of the Governor in Council. For a statute to be in force an Order in Council must be published.

After a statute is in force, the government may deposit regulations under that statute. Regulations are subordinate law made under the authority of the statute. Regulations provide the detailed rules and procedures that are contemplated under the statute. Regulations are often amended by governments. Regulations are more often amended than statutes.

3.0 How Provincial and Territorial Law is Made

Provincial and territorial law is made in a similar way to federal law with some exceptions. While the provincial and territorial law must complete First Reading, Second Reading, Committee, Report, Third Reading and Royal Assent, there is no second house to review or approve the bill. As well, a provincial statute or provisions of it may come into force not by Governor in Council but by regulation of the Lieutenant Governor in Council. A territorial statute or provisions of it may come into force neither by Governor in Council nor by Lieutenant Governor in Council but by Commissioner in Executive Council.

4.0 State Sovereignty

The principle of state sovereignty applies to Canada and the United States. State sovereignty says that countries have the exclusive right to make laws within their own boundaries. Recently, in 2014, the Supreme Court of Canada explained that:

> Sovereignty guarantees a state's ability to exercise authority over persons and events within its territory without undue external interference. Equality, in international law, is the recognition that no one state is above another in the international order.[iii]

An integral part of Canada's state sovereignty, is that Canada has federal, provincial and territorial governments. Each government has its own exclusive jurisdiction as defined in the *Constitution Act, 1867*.[iv] The federal or Canadian government has responsibility for laws of national and international concern, like a national currency, defence, foreign trade, criminal law, citizenship and terrorism. The provinces are responsible for local concerns like education, health, property and civil rights and municipal government. The territories have jurisdiction, not from the *Constitution Act, 1867*, but from the federal government. Similar to the provinces, the territories have responsibility to make laws for local concerns like education, health, administration of justice and municipal government.

5.0 Report Methodology

This report is based on data acquired from legal research of primary personal information and privacy provisions contained in the statutes enacted by Canada's federal, provincial and territorial governments (Privacy Statutes). The Appendix lists these Privacy Statutes.

These Privacy Statutes are:

British Columbia
Freedom Of Information And Protection Of Privacy Act, R.S.B.C. 1996, c. 165;

Personal Information Protection Act, S.B.C. 2003, c. 63;

Alberta
Personal Information Protection Act, S.A. 2003, c. P-6.5

Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25;

Saskatchewan
The Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01;

The Local Authority Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. L-27.1;

Manitoba
The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F.175;

Ontario
Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F. 31;

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56;

Québec
An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, C.Q.L.R. c. A-2.1;

An Act respecting the Protection of Personal Information in the Private Sector, C.Q.L.R. c. P-39.1;

An Act to Establish a Legal Framework for Information Technology, C.Q.L.R. c. C-1.1;

Archives Act, C.Q.L.R. c. A-21.1;

Charter of Human Rights and Freedoms, C.Q.L.R. c. C-12;

Civil Code of Québec, C.Q.L.R. c. C.C.Q.-1991;

New Brunswick
Right to Information and Protection of Privacy Act, S.N.B. 2009, c. R-10.6;

Nova Scotia
Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5;

Municipal Government Act, S.N.S. 1998, c. 18 (Part XX only);

Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3;

Prince Edward Island
Freedom of Information and Protection of Privacy Act, R.S.P.E.I. 1988, c. F-15.01;

Newfoundland And Labrador
Access to Information and Protection of Privacy Act, 2015, S.N.L. 2015, c. A-1.2;

Yukon
Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1;

Northwest Territories
Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20;

Nunavut
Access to Information and Protection of Privacy Act, S.N.W.T. (Nu) 1994, c. 20;

Canada
An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23 (Canada's Anti-Spam Act);

Digital Privacy Act, S.C. 2015, c. 32;

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (PIPEDA);

Privacy Act, R.S.C. 1985, c. P-21;

Security of Canada Information Sharing Act, S.C. 2015, c. 20, s. 2 (as enacted by Part I of the *Anti-terrorism Act, 2015*, S.C. 2015, c. 20).

The information in this report is current to July 1, 2017. This report's focus is on the statutes currently in force because those are the statutes with which organizations must comply. This report contains legal information only, not legal advice, and should not be relied upon. While every effort has been made to ensure the accuracy of the information in this Report, neither the author nor AIEF assumes any responsibility for any errors or omissions or damage caused from the use of this Report.

This Report examines 10 topics contained in the Privacy Statutes. These topics are:

1. Creation, defining:
    a. Personal Information.
    b. Record.
2. Collection.
3. Access.
4. Accuracy and correction.
5. Protection.
6. Use and disclosure, storage within and outside Canada.

7. Retention.
8. Disposition.
9. Special features:
    a. Personal Information Banks (PIBs).
    b. Privacy Impact Assessments (PIAs).
    c. Records and information management (RIM). policies/procedures/practices/schedules.
    d. Manuals.
    e. Cloud Computing.
    f. Social Media.
    g. Terrorism.
10. Recommendations.

These research topics mirror the life cycle of the record. Each of these research topics is further explained in this Report.

5.1 Comparison Between Privacy Statutes in Canada with the United States

As comprehensively detailed in the AIEF's *Requirements for Personal Information Protection Part 1: U.S. Federal Law* and *Requirements for Personal Information Protection Part 2: U.S. State Laws* there are dozens and dozens of statutes and regulations in a wide variety of legal areas that touch on personal information. Since Canada's private and public sector legislative regime for personal information is different than the United States, the result is that the comparison between Canada and the United States is not a direct one. While there are some similarities, such as the definition of personal information and privacy torts, there are more differences. For example, none of Canada's Privacy Statutes expressly provide for phishing, spyware, radio frequency identification or prescription drugs. Future research is needed to tease out the specific similarities and differences between Canadian and United States law governing personal information.

5.2 Privacy Statutes and the ARMA Principles®

To understand how the Privacy Statutes operate, it is helpful to compare and contrast them to the ARMA International Generally Accepted Recordkeeping Principles® (ARMA Principles®).

The ARMA Principles® are a series of 8 recordkeeping principles. They are used to foster awareness of recordkeeping standards and principles and to assist organizations in developing systems to comply with them.

The Principle of Accountability provides that an organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel and ensure program auditability. None of the Privacy Statutes have all of these elements.

The same applies to the ARMA Principle of Integrity. None of the Privacy Statutes requires that a recordkeeping program be constructed so the records and information generated by, or for the organization, have a reasonable and suitable guarantee of authenticity and reliability.

The Privacy Statutes do contain the Principle of Protection. They require that the organization shall ensure a reasonable level of protection but do not mention records and information that are private, confidential, privileged, secret, or essential to business continuity as do the ARMA Principles®.

As well, the Privacy Statutes mirror the Principle of Compliance. They require that the organization comply with applicable laws.

The Privacy Statutes reflect the Principle of Availability. They require that the organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.

The same applies for the Principle of Retention. The Privacy Statutes require that an organization shall maintain its records and information for an appropriate time. Unlike the ARMA Principles®, the Privacy Statutes do not expressly state that the organization must account for legal, regulatory, fiscal, operational and historical requirements.

For the Principle of Disposition, this is uncertain. While the Privacy Statutes refer to disposition or disposal, the Privacy Statutes do not specify that an organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.

Finally, the Privacy Statutes contain the Principle of Transparency. They require that the organization provide the required information in an understandable manner and be available to all personnel and appropriate interested parties.

Table 1 illustrates the comparison between the ARMA Principles® and the Privacy Statutes:

ARMA Principles®	**Privacy Statutes**
Accountability	✗
Integrity	✗
Protection	✓
Compliance	✓
Availability	✓
Retention	✓
Disposition	"✓"

Transparency	✓

Table 1: Comparison between ARMA Principles® and the Privacy Statutes

5.3 Privacy Regime In Canada

In contrast, to the United States and the EU, under the Canadian system, personal information is regulated from the: (1) government, (2) public sector bodies and (3) private sector organizations.

As a result of the Canadian Constitution, Canada has a jurisdiction shared between federal law and the laws of the provinces and territories.

6.0 Canada (Federal) Privacy Law

Under Canadian federal privacy law, 2 statutes govern the field. First, in the public sector, the *Privacy Act* applies. Second, in the private sector, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies.

6.1 Privacy Act

First enacted in 1983, the *Privacy Act* covers some 250 federal government departments and agencies. The *Privacy Act* gives Canadians the legal right of access to personal information held about them by the federal government and imposes rules on the federal government how it collects, maintains, uses and discloses personal information under its control. The *Privacy Act* is enforced by an independent Agent of Parliament, the Privacy Commissioner of Canada.

6.2 PIPEDA

First enacted in 2000, the PIPEDA establishes rules governing the collection, use and disclosure of personal information by organizations in the private sector, but only in the course of commercial activities and not in how these organizations manage employee information. PIPEDA does not apply to provinces that have substantially similar privacy laws to PIPEDA for private sector organizations. Those provinces are: Alberta, British

Columbia and Québec.

Consequently, the PIPEDA applies in these provinces:

- Manitoba;
- New Brunswick;
- Newfoundland and Labrador;
- Nova Scotia;
- Ontario;
- Prince Edward Island; and
- Saskatchewan.

The PIPEDA applies in all the territories:

- Northwest Territories;
- Nunavut; and
- Yukon.

The PIPEDA also applies to organizations whose commercial activities cross provincial or national boundaries. Finally, the PIPEDA applies to federally-regulated organizations carrying on commercial activity in Canada, including their management of health and employee personal information. These organizations include: airlines, banks, broadcasting corporations and telephone companies.

Like the *Privacy Act*, the PIPEDA is enforced by the Privacy Commissioner of Canada.

7.0 Provincial and Territorial Public Sector Privacy Laws

There are statutes regulating public sector privacy law for each of Canada's 10 provinces and 3 territories.

7.1 RIM and Privacy Statutes

When examined, RIM and the Privacy Statutes offer a number of important similarities and differences.

For similarities, both have a definition of record and follow the life cycle of the record.

For differences, RIM focuses on meeting an organization's business needs and complying with the law in general, not just privacy law. For privacy, the focus is on the balance between providing to citizens access to government and other information versus protecting the individual's privacy.

7.2 Jurisdiction Compared To Number Of Privacy Statutes

There are 14 jurisdictions enacting Privacy Statutes in Canada as between the provinces, the territories and the government of Canada.

Table 2 shows the comparison between the number of jurisdictions and the number of Privacy Statutes:

Jurisdiction (N=14)	**Number of Privacy Statutes** (N=29)
BC	2
AB	2
SASK	2
MAN	1
ONT	2
QUÉ	6
NB	1
NS	3
PEI	1
NEWF & LAB	1
YUKON TERRITORY	1

NORTHWEST TERRITORIES	1
NUNAVUT	1
CANADA	5

Table 2: Comparison between Jurisdiction and Number Of Privacy Statutes

The jurisdiction with the most privacy statutes is Québec with 6. Second place is Canada with 5. Third place is Nova Scotia with 3. Fourth place is shared between British Columbia, Alberta, Saskatchewan and Ontario, each with two.

Québec is a special jurisdiction. Québec has the only civil law jurisdiction in Canada, everywhere else is the common law. In Québec, the government Commission d'accès à l'information regulates privacy.
Québec is the only jurisdiction in Canada requiring registration of "personal information agents" with the Commission. These are businesses that provide credit reports and do collections.

8.0 Creation: Defining "Personal Information" and Record"

All of the Privacy Statutes contain definitions of "personal information" and "record". All the provincial and territorial jurisdictions have similar definitions of "record" in their respective privacy statutes.

8.1 "Personal Information"

A central core concept in all the Privacy Statutes is the definition of "personal information". Determining if information is "personal information" is an important first step in to know if the privacy legislation applies or not. If information is not "personal information" that information is not regulated by privacy legislation.

In the public sector, the core definition of "personal information" to mean information about an identifiable individual is used in all jurisdictions across Canada, except Québec.

The phrase "identifiable individual" is not defined in any of the privacy statutes but in case law. In *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII) at para. 34 the Federal Court of Canada adopted this test to determine when information will be about an "identifiable individual":

> Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

Canada in the PIPEDA has the shortest definition in the Privacy Statutes. Section 2(1) of the PIPEDA provides that "personal information means information about an identifiable individual".

BC requires "personal information" to be recorded and excludes business contact information from the definition. Ontario also excludes business contact information.

Like BC, Alberta, Saskatchewan, Manitoba, Ontario, Québec, New Brunswick, Nova Scotia, Prince Edward Island, Yukon and Canada in the *Privacy Act* require "personal information" to be recorded. Canada in the PIPEDA, the Northwest Territories and Nunavut do not require "personal information" to be recorded.

With the exception of Canada and BC, all the other jurisdictions in Canada also employ a larger definition to include examples of "personal information". This definition is expansive because of the use of the word "includes".

Alberta includes the individual's name, business contact information, race, national or ethnic origin, colour or religious or political beliefs or associations, age, sex, marital or family status, identifying number or symbol, fingerprints, health and genetic information, individual's educational, financial, employment or criminal history and opinions or views about the individual.

Saskatchewan has a similar list to Alberta. But Saskatchewan also includes sexual

orientation and an individual's tax information and finance history where Alberta does not. Saskatchewan excludes health information as defined in *The Health Information Protection Act* from the definition. Saskatchewan excludes specified government employment information from the definition as well.

Manitoba's list includes information about the individual's name, home contact information, age, sex, sexual orientation, marital or family status, individual's ancestry, race, colour, nationality, or national or ethnic origin, religion, creed or belief, association or activity, health and genetic information, fingerprints, political belief, association or activity, individual's educational, financial, employment or criminal history, identifying number or symbol and opinions or views about the individual.

Ontario's list includes information about the individual's race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, educational, medical, psychiatric, psychological, criminal or employment history and financial transactions of the individual, identifying number or symbol, home contact information, fingerprints or blood type of the individual and opinions or views about the individual. Unlike the other jurisdictions in Canada, Ontario includes as "personal information" correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature and replies to that correspondence that would reveal the contents of the original correspondence. Similarly, Ontario includes in the definition the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual. Ontario is singular across the country by excluding information from the definition about an individual who has been dead for more than 30 years.[v]

Québec defines "personal information" to mean, in any document, information concerning a natural person which allows the person to be identified. Québec's use of "natural person", while different than "individual" as used in the rest of Canada has a

similar legal meaning to "individual".

Québec excludes public information from the definition of "personal information". Québec defines "public information" to be the specified government and public body employment information (unless its disclosure would hinder suppression of crime, would reveal other information whose release must or may be refused under the statute or reveal the person's salary if that person is employed by a public body). Finally, Québec provides that the name of a natural person is not personal information, except where it appears in conjunction with other information concerning that person or where the mere mention of that person's name would disclose personal information concerning that person.

The Maritime jurisdictions in New Brunswick, Nova Scotia, Prince Edward Island and Newfoundland and Labrador have lists that are similar. They include the individual's name, home contact information, age, gender, sexual orientation, marital status or family status, ancestry, race, colour, nationality or national or ethnic origin, religion or creed or religious belief, health information about the individual, fingerprints, political belief, association or activity, education, employment or occupation or educational, employment or occupational, financial and criminal history, identifying number or symbol and opinions or views about the individual.

Yukon, Northwest Territories and Nunavut have lists similar to the Maritimes.

In Canada, the *Privacy Act* has a list similar to the other provinces and territories that use a list. But under the *Privacy Act*, unlike elsewhere in the country, information about an individual's personal opinions or views is not personal information except where they are about another individual, about a proposal for a grant, an award or a prize to be made to another individual by a government institution. The *Digital Privacy Act* uses the PIPEDA's definition of "personal information".

In the private sector, the definition of personal information is similar to that used in the

public sector. Only BC, Alberta and Québec have private sector privacy legislation of their own that is substantially similar to the PIPEDA. Everywhere else in Canada, the PIPEDA applies to private sector organizations so the PIPEDA's definition of "personal information" applies there as well.

BC uses a different definition of "personal information" in its private sector *Personal Information Protection Act* than the one it uses in its public sector *Freedom Of Information And Protection Of Privacy Act*. The *Personal Information Protection Act* does not require personal information to be recorded. The *Personal Information Protection Act* defines "personal information" to mean information about an identifiable individual and includes employee personal information but does not include either contact information or work product information. For "employee personal information", that means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required for employment, but does not include personal information that is not about an individual's employment. The definition is further expanded in the definition of "employment". "Employment" means not only paid employment but volunteers.

Alberta uses the same definition of "personal information" in its *Personal Information Protection Act* as that used in the PIPEDA. In a similar way, Québec, in its *Protection of Personal Information in the Private Sector*, uses the same definition of "personal information" that it has in its *Access to Documents Held by Public Bodies and the Protection of Personal Information.*

8.2 "Record"

In the RIM profession, understanding what is a "record" is fundamental. Records management standards define a "record" as:

> information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business.[vi]

As well, a "record" for RIM has these characteristics: authenticity, reliability, integrity, usability and metadata.[vii] Implied in the definition and characteristics of a record is what does not come under the definition of a record: transitory records. Transitory records do "not need to be retained to meet operational, legal, regulatory, fiscal or other requirements"[viii]. Transitory records include: copies, duplicates, drafts and other items that are not evidence and not information assets that the organization needs to pursue its business or to comply with the law.

Although this is the accepted records management definition of a "record", in the world of the Privacy Statutes, organizations must comply with various legislative definitions of "record" that are different from the RIM concept of "record".

All the provincial and territorial jurisdictions have similar definitions of "record" in their respective privacy statutes. A representative example of this is found in Nova Scotia. In section 3(1)(k) of the *Freedom of Information and Protection of Privacy Act,* "record" is defined this way:

> "record" includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

Unlike RIM, this privacy definition of "record" defines not the function or characteristics of the record, but the format in which the information resides, is recorded, or is stored. The format is expansive and does not set out a complete list because of the use of the word "includes" as in a "record includes…". Then this privacy definition excludes computer software (and by implication hardware) that produces records. By implication of this exclusion, the privacy definition includes electronic records.

Canada's privacy definition of "record", like its provincial and territorial counterparts, includes an expansive definition of record that focuses on the format in which the

information resides, is recorded, or is stored. For example, section 2(1) of the PIPEDA defines:

> *record* includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

This PIPEDA definition of "record" has been adopted by Canada's Anti-Spam Law and the *Digital Privacy Act.* The PIPEDA does not have the qualifier that the provincial and territorial privacy statutes have excluding computer software and hardware that produces records.

Records managers need to be aware of these differences between the RIM definition of "record" and the privacy definition of "record" and adjust their practices and systems accordingly. For example, if a record has the substantive characteristics of authenticity, reliability, integrity, usability and metadata it has a greater likelihood of it being admitted into evidence in Canadian courts as credible real evidence[ix] or as documentary evidence using a best practice standard.[x] One cannot say the same for a transitory record accepted as a record under all the privacy statutes across the country. The evidential rules of admissibility, including authenticity, must be proven before a transitory record could become admissible, credible evidence before a court in Canada.

8.3 Transitory Records

In the Privacy Statutes, the definition of "record", does not expressly, or by implication, exclude transitory records. As a result, the definition of record can include transitory records in the custody and control of a public body or organization at the time of an access request. The consequence of this is that there is an apparent conflict between RIM practice and the Privacy Statutes. Common RIM practice is to destroy (or at least identify but not manage) transitory records viz-a-viz records while the Privacy Statutes require accessibility and production of all records, both transitory records and records, at the time of the access request for personal information.

To resolve this apparent conflict, it is useful to review a recent analysis of transitory records made by the BC Information and Privacy Commissioners, one a sitting Commissioner at the time and the other, a former Commissioner.

In 2015, Elizabeth Denham, the Information and Privacy Commissioner for BC investigated the Ministry of Advanced Education and the Premier's Office after a complaint was made that government staff were destroying emails that were responsive to an access request for information. As a result of that investigation, the Commissioner released a report that found that both the Ministry and the Premier's Office contravened section 6(1) of the public sector *Freedom of Information and Protection of Privacy Act* (FIPPA) to make every reasonable effort to respond without delay to the applicant openly, accurately and completely.

The issue of transitory records arose because the Commissioner uncovered an improper practice in the BC government regarding electronic mail. The belief, wrongly held by some government staff, was that email, due to it existing in digital form, is only transitory and is not a record and thus can be destroyed, even if subject to an information request. This wrongly held belief was accompanied by the practice to "triple-delete" email so that the email was completely expunged from the electronic mail system and not then accessible.[xi] The Information and Privacy Commissioner found:

> In conducting this investigation, it has become clear that many employees falsely assume that emails are impermanent and transitory, and therefore of little value. What this investigation makes clear is that it is a record's content and context that determines whether a record is transitory, rather than its form.
> …
> It is important to note that once a public body receives an access to information request, it must keep all records, including both transitory and non-transitory records, in its custody or under its control. If these records are responsive, the public body must produce them unless specific exemptions to disclosure under FIPPA apply.[xii]

In 2015, the BC government retained the former Information and Privacy Commissioner, David Loukidelis, Q.C., to provide advice on how to respond to Commissioner Denham's recommendations.

Mr. Loukidelis made a thoughtful observation about the volume of email the BC government receives and sends each year and the implications of that fact:

> A major challenge to the efficacy of both freedom of information laws and records and information management flows from the fact that public institutions everywhere are increasingly digitized. As Commissioner Denham observes, the "retention and accessibility of records has been complicated by the adoption of new communications technologies [and] the volume and variability of records." The records management and archival implications of modern electronic communications media are indeed daunting. It is difficult to understate the challenges such phenomena present for records and information management, and archives, in the electronic age.
>
> The situation in British Columbia illustrates this. The provincial government's Office of the Chief Information Officer (OCIO) has advised that some 284,000,000 emails are received by the provincial public service each year, with approximately 86,000,000 being sent each year. The storage space for received emails alone amounts to some 43 terabytes of data annually, with roughly 13 terabytes being required to store sent emails. This is apart from the doubtless staggering volume of other electronic information and records created each year. This matters, obviously, because, if records cannot be found because they have not been properly managed and retained in electronic form, important public interest objectives will be harmed. So will the public's rights of access to records.[footnotes excluded][xiii]

This email situation experienced by the government of BC is not unusual in other public bodies or organizations across the country. All organizations, whatever size, face the exponential explosion of email and the problem of how to manage that.

Mr. Loukidelis responds to the belief that all emails should be retained indefinitely or be forwarded to records management staff for vetting, where records managers decide which email should be kept and which discarded:

> The practical implications of these suggestions demonstrate why neither should be adopted. LexisNexis has estimated that, when printed, each email yields on average 1.5 pages. Using the above averages of emails received and sent, each

> year there would be roughly 426,000,000 pages of received emails and some 129,000,000 pages of sent emails, for a total of roughly 555,000,000 pages of emails. No one would suggest that all emails should be printed, but this gives a sense of the order-of-magnitude implications of the suggestions that, contrary to prudent information management principles, all emails should be kept, or should be vetted by others for retention. The same would be true even if these estimates were reduced by one or even two orders of magnitude, to 55,000,000 pages or 5,500,000 pages.
>
> The truth is, if government tried to vet all emails to identify those that should be kept, it would grind to a halt. The enormous volume to review would alone guarantee this. So would the fact that those vetting the emails would have no real understanding of the context for each email. [footnote excluded][xiv]

The business in most public bodies and organizations would likely also ground to a halt if their email needed to be printed to paper or vetted by records managers, archivists or other information professionals.

How then to resolve this apparent conflict between retaining or destroying transitory records in the context of a privacy request?

Commissioner Denham states that:

> The proper identification of records as transitory or not transitory is an important access to information issue because when records are prematurely destroyed it negatively impacts citizens' access to information rights.
>
> Transitory records are routinely destroyed when they are no longer required for a business purpose. The authority to identify and destroy transitory records is delegated to government employees under the transitory records schedule.
>
> The routine destruction of transitory records is necessary to reduce the volume of government records and the cost of managing records.
>
> Non-transitory records, on the other hand, need to be filed and saved in accordance with the appropriate government records schedule. The classification and scheduling of records should make them readily identifiable and retrievable when subject to an access request.

Mr. Loukidelis agrees, goes further and he recommends:

> The plain truth is that there is no value in retaining records that have no value. As Commissioner Denham explicitly recognizes, "The routine destruction of transitory records is necessary to reduce the volume of government records and the cost of managing records." The key, therefore, is to find a practical way in which identify the records that have value and then retain and manage them appropriately in proportion to their present and enduring value. This is already a significant enough challenge given the evolution of information technologies and the increasing volume of information.
>
> Consistent with this, it is recommended in the strongest possible terms that government resist any notion that all emails should be kept indefinitely, or that they should all be vetted by archivists or records managers to decide which to keep indefinitely. The prudent approach is to ensure that government's transitory records policy is appropriate, understood by all, and properly implemented. [footnotes excluded][xv]

A number of best practices can be employed as a result of this discussion about transitory records. First, the public body or organization needs to identify transitory records. Second, there should be a transitory records policy that is practical, understood by staff and management and implemented. That includes explicitly stating that not all email is transitory; that not all email needs to be retained forever; that records professionals like records managers and archivists do not vet email or other transitory records for retention. Third, the public body or organization, as authorized, and in the usual and ordinary course of business may routinely destroy transitory records. Fourth, if transitory records exist in the custody or control of the public body or organization at the time of an access request and they are relevant to that request, those transitory records must not be destroyed. Instead, those transitory records must be kept on hold—in a legal privacy hold, as it were—until the access process is completed. The public body or organization must produce these transitory records unless there are exemptions in the relevant Privacy Statutes that prohibit disclosure. A further, and final best practice is for the public body or organization to determine if fees should be charged to the applicant making an information request to provide access to transitory records. The Privacy Statutes set out the rules for when a public body or organization may, and may not, charge fees to an applicant.

9.0 Collection

The Privacy Statutes for both the public and private sectors provide for collection of personal information. Collection includes purposes for which personal information can be collected, how it is to be collected and notice for this collection.

9.1 Purposes

A principle contained in the public and private sector Privacy Statutes is that the individual the personal information is about, must be informed about the purposes of that collection.

All of the jurisdictions, except for the public sector legislation in Saskatchewan, Québec and the Canadian *Privacy Act*, list what purposes for which collection is permitted. A representative example is found in Manitoba, section 36 of *The Freedom of Information and Protection of Privacy Act* that lists 3 purposes for collection:

1. collection of the information is authorized by or under an enactment of Manitoba or of Canada;
2. the information relates directly to and is necessary for an existing service, program or activity of the public body; or
3. the information is collected for law enforcement purposes or crime prevention.

Law does not authorize collection that does not conform to this section 36.

For the 3 other jurisdictions, the purpose of collection is broader than the rest of Canada. In Saskatchewan, section 25 of the *Freedom of Information and Protection of Privacy Act* provides that no government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution. Similarly, in Québec, section 64 of *An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal*

Information provides that a public body can collect personal information only if it is necessary for the exercise of the rights and powers of the body or the implementation of a program under its management. For Canada, section 4 of the *Privacy Act* provides that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

In the private sector, for those jurisdictions under the jurisdiction of PIPEDA, clause 4.2 of Schedule 1 provides that the purpose for the collection shall be identified by the organization at or before the time the information is collected. Clause 4.4 of Schedule 1 further circumscribes the purpose by providing that the collection shall be limited to that which is necessary for the purposes identified by the organization; still, further, information shall be collected by fair and lawful means.

In the private sector in BC, section 10 of the *Personal Information Protection Act* requires that an organization must disclose to the individual verbally or in writing purposes for the collection of the information. Section 11 of that Act provides that an organization may collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances, that meet the purpose(s) in section 10 or otherwise are permitted under the Act.

In the private sector in Alberta, like BC, section 11 of the *Personal Information Protection Act* provides that an organization may collect personal information only for purposes that are reasonable. Section 13 of that Act provides that an organization must disclose to the individual verbally or in writing purposes for the collection of the information.

In the private sector in Québec, section 8 of *An Act respecting the Protection of Personal Information in the Private Sector* requires a person to inform the person from whom the personal information is collected, the purpose of the collection, use made of the information including the categories of persons who will have access to the information.

Section 8 also requires the person to be notified where the information will be kept and the person's rights of access and rectification.

9.2 How Personal Information Collected

With some exceptions, the general principle is that personal information is collected directly from the individual in both the public and private sectors.

In the public sector, the general principle for all jurisdictions is that personal information is collected directly from the individual unless an exception in the Privacy Statutes apply. These exceptions vary from jurisdiction to jurisdiction. For example, in Alberta, section 34 of the *Freedom of Information and Protection of Privacy Act* lists 15 exceptions, ranging from collecting personal information because of a health or safety emergency, collecting a debt owed to the government to researching or validating the claims, disputes or grievances of aboriginal people.

9.3 Notice

Another principle of collection is that generally notice is required to be given to the individual of whose personal information is collected in both the public and private sectors.

In the public sector, except for Nova Scotia which does not provide for notice to the individual, notice to the individual must state:

- the legal authority for the collection;
- the principal purpose or purposes for which the personal information is intended to be used; and
- the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

10.0 Access

All the Privacy Statutes provide individuals with a right to access their own personal information under the care or control by the public body or organization. Also, there is a requirement for the public body or organization to assist individuals in making access requests. To protect the privacy of third parties, a public body or organization may restrict access to the record by severing or deleting portions of the record. Access is provided, unless the personal information is made public, conditional on applicants first paying fees (as permitted by statute) to the public body or organization. The Privacy Commissioners of each jurisdiction regulate access and resolve disputes between applicants, third parties, public bodies and organizations.

In the public sector, not all records are accessible. Specific record classes provide for access in 3 ways: (1) records are excluded from access because they do not apply to the statute (2) records are excluded from access because the public body is statute-barred from providing access and (3) records that may be excluded from access at the discretion of the public body as provided by the relevant statute.

For the first record class, those records are excluded from access because they do not form part of the statute. These, for example, include: court records, archival records and test question records. There are a wide variety of records that do not apply depending on the jurisdiction.

For the second record class, the statute itself lists records that must not be accessible. These records include: Cabinet confidences and third party privacy.

For the third record class, the statute provides the public body with a discretion to provide access or not. These include: trade secrets, confidential business information, records subject to solicitor-client privilege and law enforcement.

In Québec, *An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* permits a public body or government to refuse to provide access to information for years as specified by the Act. For a public body these are a right to:

- refuse to release information regarding negotiation of a collective agreement or a contract for 8 years from the opening of the negotiations (section 27);
- refuse to release a study prepared for the purposes of taxation, tariffing or the imposition of dues for 10 years from the date of the study (section 27);
- refuse to release records regarding its board of directors records until the expiry of 15 years from their date (section 35);
- refuse to release a preliminary draft of a bill or regulations until the expiry of 10 years from its date (section 36);
- refuse to disclose a recommendation or opinion presented less than 10 years earlier, including by a consultant or an adviser less than 10 years earlier on a matter within its jurisdiction or refuse to disclose same until the final decision on the subject matter of the recommendation or opinion is made public (section 37-38);
- refuse to disclose a study until a decision is made on the recommendation or, if no decision is made, until 5 years have elapsed from the date the study was made (section 39); and
- refuse to disclose a test intended for the comparative appraisal of a person's knowledge, aptitudes, competence or experience, until the test is no longer used (section 40).

For Cabinet confidences, the Conseil exécutif may refuse to release or to confirm the existence of information regarding administrative or political decisions for 25 years after the date on which it was made (section 30). Section 33 also mandates that specified records of the Conseil exécutif must not be released before the expiry of 25 years from its date.

The Conseil du trésor (Treasury Board Secretariat) may refuse to release or to confirm the existence of its decisions until the day that is 25 years after the date on which they were made, subject to the *Public Administration Act* (section 30).

These record limitations will affect records retention in Québec where these records need to be retained for the minimum period set by statute. It is a recommended best practice, for the public body to apply security controls to these records to keep them confidential if, and until, they are released for access by the public.

Severance of personal information is a part of the majority of the public sector Privacy Statutes. The following public sector Privacy Statutes require a public body, if that information can reasonably be severed from a record, to provide to the applicant the right of access to the remainder of the record:

- BC (section 4(2));
- Alberta (section 6(2));
- Saskatchewan (section 8 in both *The Freedom of Information and Protection of Privacy Act* and *The Local Authority Freedom of Information and Protection of Privacy Act*);
- Manitoba (section 7(2));
- Ontario in section 10(2) in the *Freedom of Information and Protection of Privacy Act* and section 4(2) in the *Municipal Freedom of Information and Protection of Privacy Act*);
- Québec in section 14 of *An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* ("deleting" is used, not "sever");
- New Brunswick (section 7(3));
- Nova Scotia in section 5(2) *Freedom of Information and Protection of Privacy Act* and section 465(2) in the *Municipal Government Act*;
- Prince Edward Island (section 6(2));
- Newfoundland And Labrador (section 8(2);

- Northwest Territories (section 5(2)); and
- Nunavut (section 5(2)).

These public sector Privacy Statutes do not provide a right to access upon severance:

- Nova Scotia's *Personal Information International Disclosure Protection Act*;
- Canada's *Privacy Act*;
- Canada's Anti-Spam Act;
- Canada's *Digital Privacy Act*; and
- Yukon.

As in the public sector, not all records containing personal information in the private sector are accessible.

In BC, section 23(1) of the *Personal Information Protection Act* requires an organization, subject to specified exceptions, to provide access to an individual upon request: the individual's personal information under the control of the organization, ways that information is used by the organization and the names of the individuals and organizations to whom this personal information has been disclosed by the organization.

Section 23(2) of that Act provides that a credit reporting agency who receives a request must also provide the individual with the names of the sources from which it received the personal information unless it is reasonable to assume the individual can ascertain those sources. Section 23(3) lists exceptions where access may be given by the organization. These exceptions are regarding:

- solicitor-client privilege;
- confidential commercial information;
- investigation;
- mediation or arbitration; and
- solicitor's lien (where a lawyer charges a client's property to secure it in order to be paid for legal services rendered).

Section 23(4) lists the exceptions where the organization is not to give access: information that could threaten the health or safety of an individual other than the individual who made the request and breach of privacy of a third party.

In Alberta, section 24 of the *Personal Information Protection Act* is similar to section 23 of the BC Act except Alberta has no provision for a solicitor's lien and includes an exception that BC does not have, that being the information relates to or may be used in the exercise of prosecutorial discretion.

In Canada's PIPEDA, section 9(1) and (2) prohibits access to personal information of a third party, unless that third party consents or the individual needs the information because an individual's life, health or security is threatened. Section 9(2.1) to (2.4) set out the process where an organization must give access to personal information to an individual upon request.

Section 9(3) gives an organization the discretion to provide access for information listed. This list includes: solicitor-client privilege (or in civil law by the professional secrecy of lawyers and notaries), confidential commercial information, information that could reasonably be expected to threaten the life or security of another individual.

Section 9(4) provides that section 9(3) does not apply if the individual needs the information because an individual's life, health or security is threatened.

Section 9(5) requires that an organization, which decides not to give access to personal information regarding an investigation of a breach of an agreement or breach of Canadian or provincial law, shall notify the Commissioner in writing.

Section 10 of the PIPEDA is unique in all the Privacy Statutes in that an organization must give access to personal information in an alternative format to an individual with a

sensory disability and who requests it.

In Québec, sections 27 to 41 of *An Act respecting the Protection of Personal Information in the Private Sector* govern access to personal information. Restrictions on access include: serious harm to the person's health, security investigation, affecting judicial proceedings or third party privacy.

Severance of personal information is required for all of the private sector Privacy Statutes but they are not the same. In BC, section 23(5) of the *Personal Information Protection Act* requires an organization, if it is able to remove specific information, to provide an individual with access to the personal information after the information is removed. This specific information is information regarding: solicitor-client privilege, confidential commercial information, investigation information and information whose disclosure could reasonably cause harm or breach another person's privacy.

Alberta, like BC, requires an organization to provide access to information. Section 24(1) of the *Personal Information Protection Act* requires an organization, if it is reasonable to sever specific information, to provide an individual with access to the personal information after the information is removed. Specific information is: commercial confidential information, information that reasonably could be expected to threaten the life or security of another or breach another individual's privacy, including an opinion about another individual.

Canada's PIPEDA in section 9(3) requires an organization, if specific information is severable from the record containing personal information, that the organization shall give the individual access after severing. The specific information is limited to: commercial confidential information or information that reasonably could be expected to threaten the life or security of another individual.

Québec is unique in Canada regarding severance, or as its *An Act respecting the Protection of Personal Information in the Private Sector* provides, deleting personal information. Only Québec permits deletion of personal information from nominative lists. A nominative list is a marketing list with individual's names, addresses, telephone numbers and email addresses. Section 17(2) of that Act requires persons conducting commerce in Québec who communicate personal information outside Québec, must give the opportunity for persons to refuse that personal information concerning them be used for the purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list. Section 24 requires that persons who engage in commercial or philanthropic prospection must notify the person of the right to have the personal information concerning that person be deleted from the nominative list that the person holds. Section 25 gives any person wishing to have personal information concerning that person deleted from a nominative list the right, at any time, to obtain that the information be deleted. Section 26 requires that the information holder, on receiving a request under section 25 must, with diligence, delete from the list any information relating to the person concerned.

11.0 Accuracy and Correction

All the Privacy Statutes require personal information that is under the custody or control of the public body or private organization to be accurate, complete and correct (in the event an error or omission is identified). In the public sector, Canada, Ontario and Québec go further with currency of the personal information. In section 6(2) of Canada's *Privacy Act*, section 40(2) of Ontario's *Freedom of Information and Protection of Privacy* Act and section 30(2) of Ontario's *Municipal Freedom of Information and Protection of Privacy Act*, personal information must be up to date as possible. In the private sector, keeping personal information up to date is required by section 71 of Québec's *An Act respecting the Protection of Personal Information in the Private Sector* and Canada's PIPEDA in Schedule 1 setting out Principle 6 (clause 4.6).

In the public sector, if the public body refuses to make a correction as requested, the head of the public body must annotate the information or describe or link the information, as the case may be, with the correction that was requested but not made. Except in Saskatchewan and Québec, the head of the public body must notify any other public body or any third party to whom that information has been disclosed either: (1) 1 year before the correction request for the provinces or (2) 2 years under section 12(2)(c) under Canada's *Privacy Act*.

Only 2 public sector jurisdictions—Alberta and Prince Edward Island--prohibit correcting a professional or expert opinion. In Alberta, in section 36(2) of the *Freedom of Information and Protection of Privacy Act*, the head of a public body must not correct an opinion, including a professional or expert opinion. In Prince Edward Island, in section 34(1.1) in the *Freedom of Information and Protection of Privacy Act*, the head of a public body shall not "correct or otherwise alter an opinion included in personal information, including a professional or expert opinion."

In the private sector, while all these private sector jurisdictions require correction, there is variation. In BC, section 24(1) and (2) of the *Personal Information Protection Act* allows the organization to determine if the request for correction is reasonable before making a correction as soon as reasonably possible; then for the organization to send the corrected personal information to each organization to which the personal information was disclosed by the organization during the year before the date the correction was made. Section 24(3) of that Act requires that if no correction is made under section 24(2), then the organization must annotate the personal information under its control with the correction that was requested but not made. Section 24(4) of that Act makes clear that when an organization is notified under section 24(2) of a correction of personal information, the organization must correct the personal information under its control.

In Alberta, like BC, the process is similar. Sections 25 and 26 of the Alberta *Personal Information Protection Act* require an organization to correct personal information that

has been reasonably shown to be incorrect. In Alberta, the organization must send a notification to other organizations that received the (now) correct personal information. Unlike BC, in Alberta there is no limitation that the correction notification must be made during the year. Unlike the other private sector jurisdictions, in Alberta in section 25(5), there is a positive duty on the organization to not correct or otherwise alter an opinion, including a professional or expert opinion.

In Québec, section 40 the *Civil Code of Québec*, requires that an organization must notify every person having received the information in the preceding 6 months and, where applicable, the person who provided that information.

In Canada, Clause 4.9.5 in Schedule 1 in the PIPEDA, requires an organization, after an individual successfully demonstrates the inaccuracy or incompleteness of personal information, to correct the information as required; where appropriate, the corrected information shall be transmitted to third parties having access to the information in question.

12.0 Protection

All across Canada, all the Privacy Statutes require a reasonable level of protection for records but are silent about the security level like that set out in the ARMA Principles®, levels for private, confidential, privileged, secret, or essential to business. None of the Privacy Statutes ban setting security levels. Security levels are reasonable protections for privacy. Consequently, it is a best practice that organizations consider setting security levels for the personal information they hold.

12.1 Reasonable Security

It is important to know the language of the jurisdiction that applies because of the variability of the wording of protection in the Privacy Statutes. Under the PIPEDA, safeguards must be maintained. No standards are prescribed for these safeguards. The

Schedule to the PIPEDA provides guidance on what are sufficient safeguards. One principle is that the safeguards will vary depending on the sensitivity of the information that has been collected; the more sensitive the information is, the more this information should be safeguarded by a higher level of protection.

But in BC and Alberta, unlike PIPEDA, there is no definition of "reasonable security".

12.2 Notify Breach of Personal Information

Of the 14 jurisdictions in Canada, only 5 have some level of duty to notify the head of the public body of a privacy breach: (1) British Columbia, (2) Alberta, (3) Newfoundland and Labrador, (4) Nunavut and (5) Canada.

In British Columbia, section 30.5(2) of the *Freedom Of Information And Protection Of Privacy Act* requires that members of a public body or a public body service provider, if they know that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body, must immediately notify the head of the public body. The BC private sector *Personal Information Protection Act* does not have breach notification requirements.

In Alberta, in contrast, under the *Freedom of Information and Protection of Privacy Act* the duty to notify of a breach of personal information is not as comprehensive compared to British Columbia. But the time limit to notify breach is the same: immediately. This is found in section 9(i) of the Freedom of Information and Protection of Privacy Regulation (Alta. Reg. 186/2008) under the *Freedom of Information and Protection of Privacy Act*. This section 9(i) requires that anyone must notify the public body in writing immediately if the person becomes aware that any of the conditions set out in a researcher agreement have been breached. Research agreements permit disclosure of personal information for research or statistical purposes.

In the Alberta private sector, under the *Personal Information Protection Act*, section 34.1(1) requires that an organization having personal information under its control must, without unreasonable delay, provide notice to the Privacy Commissioner for a breach of personal information as prescribed by regulation. The time to report is arguably longer than "immediately" being, "without unreasonable delay".

In Newfoundland and Labrador, section 64(3) of the *Access to Information and Protection of Privacy Act, 2015,* requires that a public body head must inform the individual the personal information is about, at the first reasonable opportunity, if that personal information is lost, stolen or breached. Section 64(3) of the same statute requires the public body head to inform the Privacy Commissioner of a breach of personal information, where the head reasonably believes that there has been such a breach. Section 64(5) of that statute gives the Privacy Commissioner the discretion to recommend that the public body head, at the first reasonable opportunity, notify the individual who is the subject of the information that is subject to the breach.

Nunavut's public sector statute has requirements for the content of the notification and timing of notification. Division E of the *Access to Information and Protection of Privacy Act*, requires a public body to report a material breach of personal information to the Privacy Commissioner "as soon as reasonably possible". Nunavut requires the public body to inform the individual of a breach of that individual's personal information as soon as reasonably possible if it is reasonable in the circumstances to believe that the breach of privacy creates a real risk of significant harm to the individual.

Finally, in Canada, sections 10.1 to 10.3 of the *Digital Privacy Act* sets out notification requirements. The *Digital Privacy Act* amends the PIPEDA. Section 10.1 of the *Digital Privacy Act* requires that an organization report any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The organization reports to the individual that the breach is about and also reports to the

Privacy Commissioner of Canada. The report timing is to make notification as soon as feasible after the organization determines that the breach has occurred. Section 10.2 extends this "as soon as feasible" notification to other organizations, if those organizations, when given notice, may be able to reduce the risk of harm, mitigate that harm, or satisfy a condition set by regulation. To date, no regulation has been deposited under the *Digital Privacy Act*.

Unlike any other of the Privacy Statutes that require notification of breach of personal information, section 10.3 of the *Digital Privacy Act* requires an organization to both keep and maintain a record of every breach of security safeguards involving personal information under its control as required by regulation. No retention period is specified. To date, no regulation has been deposited under the *Digital Privacy Act*.

Table 3 shows the range of timing of the notification of a breach of personal information for those Privacy Statutes that have this requirement:

TIMING OF REPORTING BREACH	**JURISDICTION**
"immediately"	BC & Alta public sector
"without unreasonable delay"	Alta private sector
"first reasonable opportunity"	Newfl. & Lab public sector
"as soon as reasonably possible"	Nunavut public sector
"as soon as feasible"	PIPEDA via *Digital Privacy Act* (Canada))

Table 3: Timing of Reporting Required for Breach of Personal Information

The word "immediately" is used in 2 of them, "reasonable" in 3 of them, while 1 uses "feasible". No time limit is specified by any jurisdiction, only a general duty to notify based on the facts.

As a result of this diversity of the timing of reporting, organizations need to closely read the applicable statute in order to determine what time standard applies to them in order to

comply with the law.

13.0 Use And Disclosure, Storage Inside Or Outside Canada

The Privacy Statutes govern use and disclosure of personal information and storage of same inside or outside Canada.

13.1 Use

In the public sector, a public body's use of personal information is only permitted as allowed by the Privacy Statutes. Three principles apply. First, the information must be used for purposes consistent with the purposes for which it was collected or compiled. Second, the individual the information is about has identified the information and consented for its use. Third, use is otherwise permitted by the statute.

In the private sector Privacy Statutes, use of personal information is permitted by an organization with the consent of the individual or, in limited circumstances, without the individual's consent. A similar approach is taken with disclosure. Storage of personal information in Canada is dealt with expressly in only 1 private sector jurisdiction: Alberta. There is no outright prohibition in Alberta for storing private sector personal information outside of Canada.

Regarding use, BC in section 14 of the *Personal Information Protection Act* provides that an organization may use personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that: (1) meet the purposes the organization disclosed to the individual, (2) meet the purposes for information collected before the Act came into force or (3) otherwise permitted under this Act.

In Alberta, in section 16 of the *Personal Information Protection Act* provides that an organization may use personal information only for purposes that are reasonable and in doing so, only to the extent that is reasonable for meeting the purposes for which the information is used.

In Québec, section 13 of *An Act Respecting The Protection Of Personal Information In The Private Sector* permits use of personal information only for purposes for which it was collected unless the individual has consented or otherwise permitted by the Act. Also, section 12 of that Act provides that subsequent use must have the individual's consent subject to the time limit prescribed by law or by a retention schedule set by regulation.

Canada's PIPEDA in Clause 4.2.4 in Schedule 1, provides that when personal information that has been collected is to be used for a new purpose, the new purpose must be identified prior to using the personal information. The new purpose requires the consent of the individual before it can be used, unless the new purpose is required by law. PIPEDA has limited circumstances where the organization can use the personal information without the knowledge or consent of the individual the information is about.

Section 7(2) lists those circumstances:

- the organization has reasonable grounds to believe the information could be useful in an investigation of a violation of law;
- the organization uses the information regarding an emergency that threatens the life, health or security of an individual;
- the information is in a witness statement and used regarding an insurance claim;
- the information was produced by the individual in the course of the individual's employment;
- the information is used for statistical, scholarly study or research;
- the information is publicly available and specified in the regulations;
- the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- to obtain consent would compromise an investigation a breach of an agreement or breach of Canadian or provincial law; and
- the collection is solely for journalistic, artistic or literary purposes.

13.2 Disclosure

In each of the public sector Privacy Statutes, exceptions to disclosure are provided as set out above in this Report's section on Access.

13.3 Storage Inside or Outside Canada

Regarding storage in Canada, in the public sector, 3 jurisdictions require storage in Canada with some exceptions: (1) BC, (2) Nova Scotia and (3) Québec. There is no outright prohibition in these 3 jurisdictions for storing public sector personal information outside of Canada.

In BC, section 30.1 of the *Freedom Of Information And Protection Of Privacy Act* requires that a public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, subject to some limited exceptions where storage outside Canada is permitted: (1) consent from the individual the information is about, (2) if information is stored or accessed from another jurisdiction for the purpose of disclosure allowed under this Act and (3) if information is disclosed regarding payment to the government or public body under the Act.

In Nova Scotia, sections 9-11 of the *Personal Information International Disclosure Protection Act* require that a public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, subject to some limited exceptions.

In Québec, section 70.1 of the *Access to Documents Held by Public Bodies and the Protection of Personal Information* requires that a public body, before releasing personal information outside Québec by itself or another party on its behalf must ensure that the information receives protection equivalent to that afforded under this Act. If not, the public body must refuse to release the information.

Canada's *Privacy Act* is silent about storage of personal information outside of Canada. To date, there is no case law from Canadian courts that gives direction on the application of the *Privacy Act* to personal information stored outside of Canada.

The Treasury Board of Canada Secretariat (TBS) is responsible for preparing policy instruments concerning the operation of the *Privacy Act* and its regulations. This includes issuing directives and guidelines related to the *Privacy Act*. The TBS' Policy on Privacy Protection gives direction to government institutions to ensure compliance with the *Privacy Act*. Part of the TBS' Policy on Privacy Protection is the Taking Privacy into Account Before Making Contracting Decisions, Guidance Document (Guidance Document).[xvi]

The Guidance Document states:

> **Why this document was developed**
> It is not uncommon for a federal government institution to contract out the management of a program or service involving personal information about Canadians to a company based in Canada, the U.S., or another country. When information is stored or accessible outside of Canada, however, it can be subject not only to Canadian laws but also to the laws of the other country.
>
> One such law is the *USA PATRIOT Act*. The Act permits U.S. law enforcement officials to seek a court order allowing them to access the personal records of any individual for the purpose of an anti-terrorism investigation without informing individuals or agencies that such disclosure has occurred. In theory, as a result of government contracting activities, U.S. officials could access information about Canadians through U.S. firms or their affiliates, even if the data is located in Canada.
>
> Although the risk of U.S. authorities using the *USA PATRIOT Act* in this way is minimal, it nevertheless exists. This has highlighted the need for special considerations with respect to government contracts involving personal information in order to mitigate such privacy risks.

As noted in the TBS' Guidance Document, it is permissible for Canadian government

institutions to store public sector records outside of Canada.

In Alberta, section 13.1 of the *Personal Information Protection Act* requires that a private sector organization that uses a service provider outside Canada to collect personal information about an individual for or on behalf of the organization with the consent of the individual, must notify the individual.

Canada's PIPEDA is silent about storage of personal information outside of Canada. To date, there is no case law from Canadian courts that gives direction on the application of the PIPEDA to personal information stored outside of Canada by either the private sector or the public sector. The Office of the Privacy Commissioner takes this position regarding transfer, processing or storage of personal information outside of Canada:

- The *Personal Information Protection and Electronic Documents Act (*the *Act)* does not prohibit organizations from outsourcing their operations across international borders;

- It is important for organizations to assess the risks that could jeopardize the security and confidentiality of customer personal information when it is transferred to foreign-based third-party service providers. The measures by which personal information is protected by a foreign-based firm must be formalized with the organization by using contractual or other means.

- No contract or contractual provision can override the laws of a country to which the information could be subject once the information has been transferred.

- Organizations must be transparent about their personal information handling practices. A company in Canada that outsources personal information processing to a company that operates in another country should notify its customers that the information may be available to the government of that country or its agencies under a lawful order made in that country.

- With regard to the issue of customer consent, the Office has taken the position that the sharing of information with a third-party service provider constitutes a "use" for the purposes of the *Act*. Organizations obtain customer consent for the use of personal information for the provision of services or products when individuals first apply for the service or product. Although service providers may change over time, if the purpose of the current provider's use of the personal information has remained the same, organizations are not required to obtain renewed customer consent for the information use.[xvii]

14.0 Retention

The Privacy Statutes have a wide range of records retention periods required for personal information:

- No retention requirement at all;
- Minimum 1 year after use;
- Minimum 2 years after use;
- As required by a retention policy or schedule; or
- As long as necessary.

As is apparent, there are no harmonized record retention requirements among the Privacy Statutes.

14.1 No Retention Requirement

Saskatchewan is the only jurisdiction that does not set a records retention requirement for personal information in the public sector.

14.2 Minimum 1 year After Use

The "1 year after use" requirement--so that an affected individual has a reasonable opportunity to obtain access to that privacy information (under provincial and territorial public sector legislation)-- is the most common among the Privacy Statutes. These jurisdictions are:

- BC[xviii];
- Alberta[xix];
- Ontario[xx];
- Nova Scotia[xxi];
- Newfoundland and Labrador[xxii];
- Yukon Territory[xxiii];
- Northwest Territories[xxiv]; and
- Nunavut[xxv].

There is a variation of this "1-year after use" rule. That is, to retain the record containing

personal information for 1 year after use but then to destroy it unless the organization has a legal or business purpose to retain longer. Two of the Privacy Statutes have this requirement. Both of them are in the private sector. They are:

- BC[xxvi]; and
- Alberta[xxvii].

A final variation of this "retain-1-year-after-use" rule is found in only 1 jurisdiction: Prince Edward Island. Section 33(b) of the *Freedom of Information and Protection of Privacy* Act provides that this 1 year rule can be shortened to any time frame with written consent of the individual, the public body, and the body that approves the records retention and disposition schedule for the public body, if different from the public body.

14.3 Minimum 2 years After Use

Under Canada's *Privacy Act*, section 6(1) requires that a government institution that has used personal information for an administrative purpose shall retain it as prescribed by regulation so that the individual to whom it relates has a reasonable opportunity to obtain access to the information. The Privacy Regulations (SOR/83-508) under the *Privacy Act* prescribe a minimum 2-year retention of personal information after use. Section 4(1) of the Privacy Regulations provide for this 2 year retention for personal information used for an administrative purpose unless the individual consents to its disposal and where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his or her rights under the Act.

Section 7 of the Privacy Regulations also provides for this 2-year retention following the date on which a request for access to personal information is received by the institution under paragraph 8(2)(e) of the Act that provides for disclosure to an investigative body for law enforcement purposes.

14.4 Required by Retention Policy or Schedule

While this is closet to common RIM practice, retention required by retention policy or schedule is contained in only 3 jurisdictions: Manitoba, New Brunswick and Québec.

In Manitoba, section 40(1) of *The Freedom of Information and Protection of Privacy Act* requires that a public body that uses personal information about an individual shall, in the absence of another legal requirement to do so, establish and comply with a written records retention policy concerning the retention of the personal information. Section 40(2) also requires the personal information be retained for a reasonable period of time so that the individual the information is about has a reasonable opportunity to obtain access to it. Section 40(2) further requires that the policy comply with any additional requirements set out in the regulations. To date, the regulations under *The Freedom of Information and Protection of Privacy Act* are silent about retention.

Like Manitoba, New Brunswick has a retention policy requirement. In section 41(1) of New Brunswick's *Right to Information and Protection of Privacy Act*, a public body that uses personal information about an individual to make a decision that directly affects the individual shall have and follow a written record retention policy, subject any other New Brunswick law. The condition that the retention policy is subject to another New Brunswick statute is similar to Manitoba, except that Manitoba does not limit the condition to a statute. In Manitoba, the retention policy is subject to "another legal requirement to do so"; this legal requirement could be not only a Manitoba statute, but also a regulation, Order in Council or Ministerial Order.

Section 41(2) of New Brunswick's *Right to Information and Protection of Privacy Act* uses the same wording as section 40(2) of Manitoba's *The Freedom of Information and Protection of Privacy Act*: the written policy must retain personal information for a reasonable time period so that the individual to whom the information relates has a reasonable opportunity to obtain access to it and that this policy complies with any

additional requirements set out in the regulations. To date, like Manitoba, the regulations under New Brunswick's *Right to Information and Protection of Privacy Act* are silent about retention.

In Québec, Article 7 of the *Archives Act* requires all public bodies to have an up-to-date retention schedule. This schedule must set out the periods of use and medium of retention of its active and semi-active documents, as well as stating which inactive documents are to be preserved permanently, and which are to be disposed of. This statute goes further. Articles 8 to 11 create a process for specified public bodies to obtain approval for their retention schedules, and future modifications, by the Bibliothèque et Archives nationales.

For the private sector in Québec, section 12 of *An Act respecting the Protection of Personal Information in the Private Sector* provides that records regarding personal information are to be retained for a time limit prescribed by law or by a retention schedule established by government regulation. To date, there is no retention schedule established by regulation.

Finally in Québec, Article 20(3) of *An Act to Establish a Legal Framework for Information Technology* requires that records must be destroyed according to the retention schedule established under the *Archives Act*.

14.5 As Long As Necessary

The final retention pattern is also the most indefinite: retain personal information "as long as necessary". That could be 1 year after use or even less than 1 year after use. That also could be decades of retention. The only one of the Privacy Statutes to embody this pattern is found in Canada's PIPEDA. Section 8(8) of the PIPEDA provides that, despite clause 4.5 of Schedule 1, "an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have".

Clause 4.5.2 of the Schedule states:

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

The Part to which section 8(8) refers to is limited to Part II of PIPEDA. Part II is Protection of Personal Information in the Private Sector.

15.0 Disposition

The Privacy Statutes use the word "disposition" but not in the way "disposition" is normally used in the RIM profession. In the RIM profession "disposition" is understood as destruction, permanent retention or transfer to an archives. The Privacy Statutes frame disposition, unlike in the RIM profession. Instead, they only refer to reasonable security.

Regarding records management, the word "disposition" or "destruction", as the case may be, is referred to in the Privacy Statutes in these jurisdictions:

- BC (public and private sector)[xxviii];
- Alberta (public and private sector)[xxix];
- Saskatchewan (public sector)[xxx];
- Manitoba (public sector)[xxxi];
- Ontario (public sector and municipal sector)[xxxii];
- Québec (public and private sector)[xxxiii];
- New Brunswick (public sector)[xxxiv];
- Nova Scotia (public sector)[xxxv];
- Prince Edward Island (public sector)[xxxvi];
- Newfoundland and Labrador (public sector)[xxxvii];
- Yukon[xxxviii];

- Northwest Territories[xxxix];
- Nunavut[xl]; and
- Canada[xli].

Whether it is "disposition" or "destruction" used in the Privacy Statutes, there is no prohibition in the Privacy Statutes for organizations applying RIM-focussed disposition. It is preferable to apply the RIM profession's common use of disposition since it is more complete than simply reasonable security.

16.0 Special Features

There are special features of the Privacy Statutes that are unique to information and privacy law and that can be classed into 7 categories:

1. Personal Information Banks (PIBs).
2. Privacy Impact Assessments (PIAs).
3. RIM policies/procedures/practices/schedules.
4. Manuals.
5. Cloud computing.
6. Social media.
7. Terrorism.

16.1 Personal Information Banks (PIBs)

Some of the Privacy Statutes require personal information banks (PIBs) to be created, maintained, kept current and published for the public's access. Typically, a PIB is a list of records with personal information that is organized or accessed in 1 of 4 ways. First, is the name of the individual. Second, is the number used to identify the individual. Third, is the symbol used to identify the individual. Or fourth, is another particular used to identify the individual.

Another common requirement for the PIB is that the personal information in each PIB

must be under the custody or control of the public sector organization.

PIBs are generally accessible to the public without the need to make an access request under the legislation; PIBs are available usually without paying a fee.

The jurisdictions that require PIBs of public sector bodies are:

- BC[xlii];
- Alberta[xliii];
- Nova Scotia[xliv];
- Newfoundland and Labrador[xlv];
- Ontario[xlvi]; and
- Canada in the *Privacy Act*[xlvii].

PIBs form part of standard RIM practice in order to comply with the Privacy Statutes. As a result, PIBs are commonly cited in a public body's classification plan and retention schedule. The Privacy Statutes have no PIB requirement in the private sector.

16.2 Privacy Impact Assessments (PIAs)

Like PIBs, Privacy Impact Assessments (PIAs) are unique to information and privacy law. A PIA is an assessment that a public body undertakes to see if its proposed program or practice complies with the privacy legislation.

Unlike PIBs, only 3 jurisdictions require PIAs: BC, New Brunswick and Newfoundland and Labrador. These 3 jurisdictions only require PIAs in the public sector, not the private sector.

In BC, PIAs are mandated for limited use. Not all programs or practices involving personal information are required to first have a PIA. Sections 69(5) to (5.2) of the *Freedom Of Information And Protection Of Privacy Act* require a Ministry head to

submit to the Minister a PIA regarding a proposed program or practice regarding a common or integrated program or activity or a data-linking initiative. In turn, that Minister must submit that PIA to the Information and Privacy Commissioner for review and comment.

Under the BC *Freedom Of Information And Protection Of Privacy Act*, the key terms "common or integrated program or activity" and "data-linking initiative" are strictly defined. As a result, they have a narrow application. Schedule 1 of the *Freedom Of Information And Protection Of Privacy Act* defines "common or integrated program or activity" to mean a program or activity that provides service(s) through a public body and one or more public bodies or agencies. As well, Schedule 1 defines "data-linking initiative" to mean a "new or newly revised enactment, system, project, program or activity that has, as a component, data linking" between 2 or more public bodies or 1 or more public bodies and 1 or more agencies.

Similarly, in BC for a public body with a proposed program or practice regarding a common or integrated program or activity or a data-linking initiative, sections 69(5.3) to (5.5) of the *Freedom Of Information And Protection Of Privacy Act* require that the public body must, before engaging in that program, activity or initiative, conduct a PIA in accordance with the Minister's directions. Then the public body must submit a PIA to the Information and Privacy Commissioner for review and comment.

Similar to BC, in New Brunswick, proposed programs or practices from a Ministry or public body regarding linked/matched information databases, research, or volume or bulk basis of personal information first require a PIA. Unlike BC where the party proposing the program or practice must conduct the PIA, in New Brunswick, section 77 of the *Right to Information and Protection of Privacy Act* requires the Privacy Assessment Review Committee to conduct an assessment of these proposed programs or practices. This Committee, in turn, may have its work reviewed by the Integrity Commissioner.[xlviii]
In Newfoundland and Labrador, section 72 of the *Access to Information and Protection*

of Privacy Act, 2015 requires a government department or branch of the executive government to submit to the Minister a PIA during the development of a program or service to conduct a PIA, if the preliminary assessment showed that a PIA was not required. Then the Minister must submit the PIA to the Information and Privacy Commissioner for review and comment.

Unlike BC and New Brunswick, Newfoundland and Labrador has a broader application for a PIA; it requires a PIA for any government program or practice affecting the protection of personal information, not just a common or integrated program or service, data-linking or research.

While in general, the mandatory use of PIAs is limited in the Privacy Statutes, it is a best practice for an organization to conduct a PIA to determine the level of privacy compliance and to reduce risks of future investigation, audit or litigation. A good rule of thumb for RIM professionals to apply is that the greater the risk, the greater is the need for a PIA.

Using technology such as social media, cloud computing, mobile devices, Bring Your Own Device to work, Bring your Own Cloud to work and video surveillance increases risk. Conducting a PIA for the use of these technologies can reduce risk.

For example, the Information and Privacy Commissioner for BC has a helpful guidance document "Conducting Social Media Background Checks" which recommends that an organization or public body conduct a PIA.[xlix] The PIA should assess:

- what privacy law applies;
- purposes for using social media to collect personal information;
- that there is legal authority to collect and use personal information; if so, to notify the individual about whom the background check will be about and the legal authority for collecting it;
- if there are other, less intrusive measures to the background check, that meet the

same purposes;

- what types and amounts of personal information are likely to be collected in background check, including third party personal information;
- what risks are there with collection and use of the personal information regarding the background check, including risks of taking actions based on wrong information;
- that the proper policies and procedures are in use to manage risks related to the collection, use, disclosure, retention, accuracy, and protection of personal information; and
- that the information collected from the background check is retained and accessible in the event access is requested as to what decision was made regarding an employee or volunteer.[1]

16.3 RIM Policies/Procedures/Practices/Schedules

Half of the jurisdictions in the Privacy Statutes refer to RIM policies, procedures, practices or schedules.

In Saskatchewan, there are references to a records directory. Section 64 of *The Freedom of Information and Protection of Privacy Act* requires each Ministry to create a records directory and keep it reasonably up to date. The records directory must contain:

- a list of all government institutions;
- a general description of the categories of records in the possession or under the control of each institution; and
- the title and address of the appropriate officer for each government institution to whom applications for access to records should be sent.

The government is also required to make a copy of this directory available for inspection by the public, including in government offices, public libraries and municipal offices.

Also in Saskatchewan, there is a similar reference to a required records directory applying to local authorities. That reference is found in section 53 of *The Local Authority Freedom of Information and Protection of Privacy Act*.

In Manitoba, there is a requirement for a written records retention policy for personal information. Section 40(1) of *The Freedom of Information and Protection of Privacy Act* makes this requirement. Section 40(2) of that Act provides that the policy must require that personal information be retained for a reasonable period of time so that the individual the information is about has a reasonable opportunity to obtain access to it and to comply with any regulations. To date, no regulations have been deposited regarding the record retention policy.

In Ontario, in the public sector, there is a requirement to ensure preservation of records. Section 10.1 of the *Freedom of Information and Protection of Privacy Act* requires the head of every institution to ensure that reasonable measures for the records, in its custody or under the control, are developed, documented and put into place to preserve the records according to any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise. A parallel provision governing Ontario municipalities is set out in section 4.1 of the *Municipal Freedom of Information and Protection of Privacy Act*.

Also, for Ontario municipalities, section 34(1)(g) of the *Municipal Freedom of Information and Protection of Privacy Act* requires that, for personal information banks, public inspection of these banks is required, specifically the policies and practices applicable to the retention and disposal of the personal information.

In Québec, Article 7 of the *Archives Act* requires all public bodies to have an up-to-date retention schedule. That schedule must set out the periods of use and medium of retention of its active and semi-active documents, as well as stating which inactive documents are to be preserved permanently, and which are to be disposed of. This statute goes further

and creates a process in Articles 8 to 11 for specified public bodies to obtain approval for their retention schedules, and future modifications, by the Bibliothèque et Archives nationales.

For the private sector in Québec, section 12 of *An Act respecting the Protection of Personal Information in the Private Sector*, provides that records regarding personal information are to be retained for a time limit prescribed by law or by a retention schedule established by government regulation. To date, there is no retention schedule established by regulation.

Finally in Québec, Article 20(3) of *An Act to Establish a Legal Framework for Information Technology* requires that records must be destroyed according to the retention schedule established under the *Archives Act*.

In New Brunswick, section 41(1) of the *Right to Information and Protection of Privacy Act* requires that a public body must, subject to any other Act of the Legislature, establish and comply with a written policy concerning the retention of the personal information. Section 41(2) of that Act specifies that this policy must require that personal information be retained for a reasonable period of time so that the individual to whom the information relates has a reasonable opportunity to obtain access to it and to comply with any regulations. To date, no regulations have been deposited regarding the record retention policy.

In Newfoundland And Labrador, section 11 of the *Access to Information and Protection of Privacy Act, 2015* requires public bodies specified by regulation to have a publication scheme for their records, including a description and list of the records in the custody or under the control of the public body, including personal information banks. To date, there is no regulation specifying public bodies.

In Canada, the PIPEDA provides for guidelines and procedures regarding records retention and destruction. In Schedule 1, Principle 4.5 Principle 5 —Limiting Use, Disclosure, and Retention provides:

> 4.5.2
> Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.
>
> 4.5.3
> Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

Finally, in Canada, there is reference to recordkeeping. Section 33 of the *Canada's Anti-Spam* Law provides for a due diligence defense from the high penalties for noncompliance if an individual, corporation, organization or public body, as the case may be, complies with Compliance and Enforcement Information Bulletin CRTC 2014-326 (June 19, 2012). This Bulletin provides guidance for the development of corporate compliance programs that may be used as part of due diligence defence. Specifically, this Bulletin sets out the components of a recommended written corporate compliance policy for recordkeeping:

> 9. Good record-keeping practices may help businesses (i) identify potential non-compliance issues, (ii) investigate and respond to consumer complaints, (iii) respond to questions about the business's practices and procedures, (iv) monitor their corporate compliance program, (v) identify the need for corrective actions and demonstrate that these actions were implemented, and (vi) establish a due diligence defence in the event of complaints to the Commission against the business.[li]

16.4 Manuals

In BC, there are references to manuals and policies/procedures in both the public and private sector, but not to RIM expressly. Section 70 of the *Freedom Of Information And Protection Of Privacy Act* requires a public body to make available to the public without a privacy request manuals, instructions or guidelines issued to the public body officers or employees used to interpret an enactment (statute or regulation) or administer a program or activity that affects the public. Section 5 of the *Personal Information Protection Act* requires an organization to develop and follow policies and practices to comply with this statute. As well, section 5 mandates a complaint process. Finally, section 5 requires an organization to make these available to the public upon request, without an access request.

In Alberta, like BC, there are references to manuals and policies/procedures in both the public and private sector, but not to RIM expressly. Section 89 of the *Freedom Of Information And Protection Of Privacy Act* requires the public body to make offices available where the public may inspect any manual, handbook or other guideline used in decision-making processes that affect the public by employees of the public body in administering or carrying out programs or activities of the public body. Unlike BC, there is no automatic right for the public in Alberta to obtain a copy of this information without an access request. Instead, in this Alberta statute, section 88(1) allows the public body to specify categories of records and that are available to the public without a request for access. Section 88(2) of this Act also permits the public body to charge a fee to provide access to this information, unless such records can otherwise be accessed without a fee.

In the private sector in Alberta, section 6(1) of the *Personal Information Protection Act* requires that an organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under the Act. Section 6(2) of this Act also requires that if an organization uses a service provider outside Canada to collect, use, disclose or store personal information, the policies and procedures must have

information about the countries outside Canada where the personal information is and the purposes for which this service provider has been authorized to collect, use or disclose personal information for the organization. Finally, section 6(3) of this Act requires that the organization must make written information about the policies and practices referred to in section 6(1) and (2) available on request.

In Saskatchewan, like BC and Alberta, there are references to making manuals available to the public. In section 65 of *The Freedom of Information and Protection of Privacy Act*, a government institution must provide access where the public may inspect any manual, handbook or other guideline used in government decision-making processes.

In Ontario, section 33 of the *Freedom of Information and Protection of Privacy Act* requires that manuals, directives or guidelines prepared by the institution, issued to its officers, be made available to the public. Section 35 of that Act requires that information to be generally available for inspection and copying by the public, either on the Internet or in the reading room, library or office designated by each institution for that purpose.

In these jurisdictions, there is no prohibition on using RIM policies, procedures, practices or schedules. What that means, is that the door is open for using RIM to protect and manage personal information.

16.5 Cloud Computing

Cloud computing is not found as a term in any of the Privacy Statutes. However, cloud computing is linked to storage of personal information outside of Canada. The principles set out in the section of this Report above "Use And Disclosure, Storage Inside Or Outside Canada" apply to cloud computing as well. In addition, some of the Privacy Statutes use the term "service provider". A "service provider" could include a cloud service provider.

16.6 Social Media

Social media is similar to cloud computing. The law regarding cloud computing can be applicable to social media. Like cloud computing, the use of the term "service provider" could include a social media service provider.

The only jurisdiction that refers to social media specifically is BC. Section 33.1(r)(i) of the BC *Freedom Of Information And Protection Of Privacy Act* provides that personal information may be disclosed inside or outside Canada if the information was disclosed on a social media site by the individual the information is about, was collected by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion and is disclosed for use that is consistent with the purpose of public engagement. Schedule 1 of that Act prescribes what social media sites are acceptable. Section 15 and Schedule 3 both in the Freedom Of Information And Protection Of Privacy Regulation (B.C. Reg. 155/2012) under that Act also prescribe social media sites. Together, 77 social media sites are prescribed. If a social media site is not prescribed, a public body cannot use that site to disclose personal information inside or outside Canada.

16.7 Terrorism

Part 1 of the *Anti-Terrorism Act, 2015* enacts the *Security of Canada Information Sharing Act*. The *Security of Canada Information Sharing Act* permits information sharing between Canadian institutions that have jurisdiction over national security threats, including terrorism. This includes personal information. Section 4 of this Act lists the principles to be used for information sharing, including that sharing protects Canada and Canadians.

17.0 Recommendations

The research results in this Report shows a need for a number of recommended changes for governments, business stakeholders in organizations and RIM professionals.

17.1 Governments

First, I recommend legislators in all jurisdictions enact more provisions mandating use of RIM policies and the like, and not only in privacy legislation. These RIM policies are effective tools that can be readily applied to meet the privacy goals in the legislation. These tools are especially useful when dealing with electronic records, where accessing electronic records can be difficult when the volume of electronic records is too large for easy indexing and searching for retrieval.

Second, I recommend that legislators harmonize retention requirements in the Privacy Statutes. Harmonization means that the same privacy retention would equally apply to all organizations and public bodies. Harmonization has a long-history in Canada. Since 1918, the Uniform Law Conference of Canada (ULCC) has worked diligently to research, write and recommend changes to Canadian federal, provincial and territorial laws.[lii] Over the years, many governments have acted on the ULCC's recommendations and enacted law.

Currently, the Privacy Statutes disclose 5 retention patterns that are not based in legal principle:

- No retention requirement at all;
- Minimum 1 year after use;
- Minimum 2 years after use;
- As required by retention policy or schedule; and
- As long as necessary.

The problem with this unprincipled approach is that it is confusing. As well, for organizations that conduct business across provincial borders, it is not only confusing but is difficult to comply with law, imposes regulatory burdens and increases costs to administer the law. For example, it requires changes and management to the organization's classification plan and retention schedule. It requires management of different retention periods and thus different dispositions for these records. These all increase costs. These all require training of staff to implement procedures in order to comply with the law.

I recommend that the "1-year-after-use" retention period be enacted all across Canada. This "1-year-after-use" retention period is the most common retention period currently used by 8 of the 14 jurisdictions in Canada. This "1-year-after-use" rule would cut the current Gordian knot of retention, making retention easier to manage. This, in turn, would increase legal compliance and efficiency.

Third, I recommend that organizations and public bodies analyze the privacy statutes they are subject to and then use policies and procedures to fill in gaps between the privacy laws. RIM has many practical, effective tools to ensure legal compliance with the Privacy Statutes. Again, this is especially when managing electronic records and privacy.

17.2 Business Stakeholders in Organizations

First, I recommend that business stakeholders in organizations apply the Principle of Accountability from the ARMA Principles® to ensure compliance with the Privacy Statutes and that the organization is meeting its business goals and strategy. Part of this compliance function is auditability. The organization should maintain a RM Strategy Committee or Information Governance Committee, as the case may be, composed of business stakeholders, IT, RM and legal professionals. This Committee can be a very effective tool to ensure privacy law accountability by aligning strategy, reporting, training, technology, business integration and oversight.

Second, regarding the patchwork quilt of the law in in the Privacy Statutes, especially for the definitions of "personal information" and "record" and differences in duties to advise about privacy breaches, I recommend business stakeholders retain legal counsel experienced in privacy law to advise the organization on an ongoing basis. Questions and concerns about privacy commonly arise in organizations. For organizations with business operations across Canada or outside Canada, I recommend that policies and procedures, along with training of staff and management, be in place regarding the organization complying with the Privacy Statutes, especially storage of PI in and outside Canada, use of cloud computing and social media and combatting terrorism.

17.3 RIM Professionals

First, I recommend that RIM professionals apply the ARMA Principles® in their work to ensure that their organizations comply with the Privacy Statutes and also meet their organization's business needs. While the Privacy Statutes do not mention authenticity and reliability, I recommend that the ARMA Principle of Integrity can be applied to the organization's recordkeeping program so the records and information generated by or for the organization have a reasonable and suitable guarantee of authenticity and reliability. This is especially important for electronic records and to ensure their admissibility in legal proceedings affecting the organization.

While the Privacy Statutes do contain the Principle of Protection, the Privacy Statutes require the organization to ensure a reasonable level of protection but do not mention records and information that are private, confidential, privileged, secret, or essential to business continuity as do the ARMA Principles®. I recommend that RIM professionals enhance their organization's protection by applying these security levels to protect their organizations' records, especially electronic records.

Similarly like protection, for retention, the Privacy Statutes require that an organization maintain its records and information for an appropriate time. Unlike the ARMA Principle of Retention the Privacy Statutes do not expressly state that the organization must account for legal, regulatory, fiscal, operational and historical requirements. I recommend that RIM professionals account for legal, regulatory, fiscal, operational and historical requirements in their recordkeeping programs. This follows the life cycle of records and proper management of records, again, especially electronic records.

For the Principle of Disposition, this is uncertain. While the Privacy Statutes refer to disposition or disposal, the Privacy Statutes do not specify that an organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.

Second, I recommend RIM professionals take positive steps regarding transitory records. RIM professionals should take the lead and advise their public bodies or organizations and identify their transitory records. As well, RIM professionals should also advise on a transitory records policy that is practical, understood by staff and management and implemented. That includes explicitly stating that not all email is transitory; that not all email needs to be retained forever; that records professionals like records managers and archivists do not vet email or other transitory records for retention. RIM professionals should manage the authorized and routine destruction of transitory records in their organizations, unless transitory records exist in the custody or control of the public body or organization at the time of an access request and they are relevant to that request, those transitory records must not be destroyed. Instead, those transitory records must be kept on a legal hold until the access process is completed. The public body or organization must produce these transitory records unless there are exemptions in the relevant Privacy Statutes that prohibit disclosure. A further, and final best practice is for the public body or organization to determine if fees should be charged to the applicant making an information request to provide access to transitory records. The Privacy Statutes set out the rules for when a public body or organization may, and may not, charge fees to an

applicant. RIM professionals can advise their public bodies or organizations about managing this fee process.

Third, I recommend that RIM professionals advise their public bodies or organizations about records that can be routinely disclosed without a privacy request. Being proactive like this, saves time and money for all parties concerned: RIM professionals, their public bodies or organizations and potential privacy access applicants. For example, the Local Government Association of BC's Freedom of Information and Protection of Privacy Act Toolkit for Local Government Organizations has a helpful sample list of routinely available records that can be disclosed without a privacy request. [liii] These include records such as annual reports, budgets, manuals and policies and procedures. Lists like these can be customized to the specific needs of organizations, and made available on the organizations' websites or at their offices.

18.0 Conclusion

In conclusion, the research documenting this Report clearly shows how complex and varied the requirements are for personal information protection across Canada. It also demonstrates how Canada's Constitution influences how privacy rules and procedures are implemented and how often they are different jurisdiction to jurisdiction.

This Report also shows a need for harmonization in the Privacy Statutes to increase compliance.

The Privacy Statutes and RIM pair well together; they share similar policies and goals. Where there are gaps in the Privacy Statutes, the tools and practical insights of RIM can be used fill those gaps to ensure increased legal compliance, risk reduction and increased efficiencies in protecting personal information.

Further, as electronic technologies proliferate in all aspects of Canadian life, public bodies and organizations must adapt in order to comply with the Privacy Statutes. As use of these technologies continue to grow, Canadian public bodies and organizations should strongly consider putting more focus and weight on the importance of handling privacy matters in their work to ensure a balance between openness and accountability regarding personal information protection.

Appendix: Privacy Statutes Of Canada's Federal, Provincial And Territorial Governments

Click the following link to download the Appendix as an Excel file:
http://armaedfoundation.org/wp-content/uploads/2017/10/Rennie_Appendix_Privacy_Statutes_July_1_2017.xlsx

Notes

[i] See http://armaedfoundation.org/.

[ii] See US Privacy Shield website at and Federal Trade Commission website.

[iii] *Kazemi Estate v. Islamic Republic of Iran*, [2014] 3 SCR 176, 2014 SCC 62 (CanLII) at para. 35 per LeBel J.

[iv] See http://www.justice.gc.ca/eng/csj-sjc/just/05.html.

[v] Section 2(2) of the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31 and section 2(2) of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.

[vi] ISO/15489-1:2016, p. 2 and a similar definition incorporated into CAN/CGSB-72.34-2017, p. 6.

[vii] ISO/15489-1:2016, Section 5.2.2 Characteristics of authoritative records, pp. 4-5.

[viii] CAN/CGSB-72.34: 2017, p. 8.

[ix] *Saturley v. CIBC World Markets* 2012 NSSC 226 (CanLII).

[x] *R. v. Oler*, 2014 ABPC 130 (CanLII).

[xi] Elizabeth Denham, Information And Privacy Commissioner for BC, "Investigation Report F15-03 Access Denied: Record Retention And Disposal Practices Of The Government Of British Columbia" (October 22, 2015), pp. 14 and 53.

[xii] *Supra*, at pp. 3, 18.

[xiii] David Loukidelis, QC, "Implementing Investigation Report F15-03: Recommendations To The Government of British Columbia" (December 2015), pp.6-7.

[xiv] *Supra* at p. 8.

[xv] *Supra* at pp. 8-9.

[xvi] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13720

[xvii] See Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers, 2008 CanLII 58164 (PCC).

[xviii] Section 31 of the *Freedom Of Information And Protection Of Privacy Act, R.S.B.C. 1996, c. 165*.

[xix] Section 35 of the *Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25*.

[xx] Section 40(1) of the *Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F. 31* and section 5 in the regulations, General, R.R.O. 1990, Reg. 460.

[xxi] Section 24(4) of the Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5.

[xxii] Section 65 of the *Access to Information and Protection of Privacy Act, 2015, S.N.L. 2015, c. A-1.2*.

[xxiii] Section 34 of the *Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1*.

[xxiv] Section 44 of the *Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20*.

[xxv]Section 44 of the Access to Information and Protection of Privacy Act, S.N.W.T. (Nu) 1994, c. 20.

[xxvi] Section 35 of the *Personal Information Protection Act, S.B.C. 2003, c. 63*.

[xxvii] Section 35 of the *Personal Information Protection Act*, S.A. 2003, c. P-6.5.

[xxviii] Section 30 of the *Freedom Of Information And Protection Of Privacy Act, R.S.B.C. 1996, c. 165* and section 34 of the Personal Information Protection Act, S.B.C. 2003, c. 63.

[xxix] Sections 3(e), 35(b)(iii) and 38 of the *Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25* and sections 34 and 35 of the Personal Information Protection Act, S.A. 2003, c. P-6.5.

[xxx] Section 4(d) of The Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01.

[xxxi] Section 3(b), 41 and 44.1 of The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F.175.

[xxxii] Section 40(4) and 45(g) of the *Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F. 31* and sections 2(1), 30(4) and 34(1)(g) of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.

[xxxiii] Sections 63.1, 73, 81(4), 128 of the *An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, C.Q.L.R. c. A-2.1, section 10 of the *An Act respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R. c. P-39.1, sections 6, 17, 18, 20, 35, 44 and 45 of *An Act to Establish a Legal Framework for Information Technology*, C.Q.L.R. c. C-1.1, sections 7, 13, 18, 28 and 35 of the *Archives Act*, C.Q.L.R. c. A-21.1.

[xxxiv] Sections 3(b), 41 and 44.1 of the Right to Information and Protection of Privacy Act, S.N.B. 2009, c. R-10.6.

[xxxv] Sections 4(3)(c) and 24(3) of the *Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, c. 5 and section 464(c) of the Municipal Government Act, S.N.S. 1998, c. 18 (Part XX).

[xxxvi] Sections 3(e), 32(3)(b) and 35 of the *Freedom of Information and Protection of Privacy Act*, R.S.P.E.I. 1988, c. F-15.01.

[xxxvii] Sections 5(2)(b) and 64 of the *Access to Information and Protection of Privacy Act, 2015*, S.N.L. 2015, c. A-1.2.

[xxxviii] Sections 2(3) and 33 of the *Access to Information and Protection of Privacy Act*, R.S.Y. 2002, c. 1.

[xxxix] Sections 3(2)(e) and 42 of the *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20.

[xl] Sections 3(2)(e) and 42 of the *Access to Information and Protection of Privacy Act*, S.N.W.T. (Nu) 1994, c. 20.

[xli] Section 6(3) of the *Privacy Act*, R.S.C. 1985, c. P-21 and clauses 4.5.3 and 4.7.5 in Schedule 1 of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[xlii] Section 69 of the *Freedom Of Information And Protection Of Privacy Act, R.S.B.C. 1996, c. 165*.

[xliii] Section 87.1 of the *Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25*.

[xliv] Section 48 of the Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5.

[xlv] Section 111(3)(b) of the *Access to Information and Protection of Privacy Act, 2015, S.N.L. 2015, c. A-1.2*.

[xlvi] Sections 2(1) and 44-49 of the *Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F. 31* and sections 2(1), 34-38 of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.

[xlvii] Sections 9 to 18 of the *Privacy Act, R.S.C. 1985, c. P-21*.

[xlviii] Section 65.2(c) of the *Integrity Commissioner Act*, S.N.B. 2016, c. 53.

[xlix] (Updated May 2017) https://www.oipc.bc.ca/guidance-documents/1454.

[l] *Supra* at page. 4.

[li] Page 3 at http://crtc.gc.ca/eng/archive/2014/2014-326.pdf.

[lii] See http://www.ulcc.ca/.

[liii] See http://www.lgma.ca.

About the Author

Stuart Rennie, JD, MLIS, BA (Hons.) has a Vancouver, Canada-based boutique law practice where he specializes in records management, privacy and freedom of information, law reform, public policy and information governance law. He is a member of ARMA International and the Vancouver Chapter, and is a member of ARMA International's Content Editorial Board. Stuart is also an adjunct professor at the School of Library, Archival and Information Studies at the University of British Columbia in Vancouver. He is a frequent invited speaker at workshops and conferences, and a noted and published author. See: www.stuartrennie.ca/index.html .

The ARMA International Educational Foundation (the Foundation) is an education and research funding resource to be used by individuals and organizations for the advancement of knowledge in the field of information management. It is a US non-profit, 501(c)3 organization.

Mission

The ARMA International Educational Foundation supports education and research initiatives that promote the advancement of both information managers and the information management profession.

Purpose

Recorded information is the lifeblood of the modern organization, but rarely is it treated as a critical asset, primarily because there is little quality research to create the comprehensive body of knowledge required to support information management as a profession. The Foundation's purpose is to answer that need by soliciting funds for this research and then providing a vehicle through which conclusions can be tested, documented and communicated to the information management community.

If you found value in this publication, please consider making a financial contribution to the Endowment Fund of the Foundation. This can be accomplished by visiting the Foundation's web site, www.armaedfoundation.org , or by contacting: coordinator@armaedfoundation.org .

Additional information about the Foundation can be found at:

The National Database of Non-profit Organizations
http://www.guidestar.org/organizations/31-1556655/arma-international-educational-foundation.aspx

Comments about this publication and suggestions for further research are welcome at: coordinator@armaedfoundation.org