When "Private" Is No Longer Private: Protecting Personal Information in an Ever Changing Digital Landscape

Research Project for Emerging Issues / Advanced Topics Course
Diploma in Investigative and Forensic Accounting Program
University of Toronto

Prepared by: Miranda Lahtinen

June 26, 2015

Prepared for: Professor Leonard Brooks

Acknowledgements

The author wishes to acknowledge the generous contributions of the following individuals:

Alex Cameron LL.B, LL.M, LL.D, for providing helpful insight into privacy infringement from a lawyer's perspective.

Ken Froese,FCPA, FCA•IFA, FCFI, *Sarah E. MacGregor, CPA, CA•IFA, CFE*, and *Pamela Morley, CPA, CA•IFA, CFE* for providing constructive insight from the perspective of an IFA working in private and/or public sectors.

Tim Ticknor, for providing useful input on how privacy legislation could impact investigations.

Charles Smedmor, CPA, CA, CFE, who acted as the author's mentor, for overseeing the development of this research paper, and establishing the connection with Mr. Froese.

The author would also like to recognize the generous support from the offices of the Diploma in Forensic Accounting (DIFA) Program at University of Toronto:

- *Leonard J. Brooks, FCPA, FCA*, Director, DIFA; and
- *Debby Keown*, Program Officer, DIFA.

Executive Summary

The introduction of personal computers and the introduction of the internet have greatly changed the way data can be gathered, analyzed, and shared. Today almost everyone has access to a computer, smart phone, or gaming system that can be connected to the internet. This technology has become so integrated with our way of life, that the exchange of information, sometimes personal information, has become almost commonplace.

As a result of growing concerns surrounding access to private information, the Canadian government, along with the governments in other countries, has enacted special legislation around privacy concerns. Technology, however, continues to change at an ever increasing rate that is not compensated for in the legislation. As a result, breaches in security and privacy infringement have become a growing concern and will continue to do so as the digital landscape changes.

Although the original intent of this report was to review the impact of privacy protection legislation on investigative forensic accounting (IFAs) engagements and investigations, at the time this report was written, it was discovered that privacy legislation has had little impact on IFA engagements or investigations. This may result from the way that an IFA is hired since consent for the collection of information has usually already been granted as part of the engagement with an individual's lawyer.

Table of Contents

Figures

1. Summary of Acronyms Used

AITA – Access to Information Act

APEC – Asia Pacific Economic Cooperation

APPA – Asia Pacific Privacy Authorities

CA – Chartered Accountant

CASL – Canada's Anti-Spam Law

CFE – Certified Fraud Examiner

CHRA – Canadian Human Rights Act

CPA – Certified Professional Accountant

CRA – Canada Revenue Agency

CRTC – Canadian Radio Television and Telecommunications Commission

CSA – Canadian Standard Association's

DFAIT – Department of Foreign Affairs and International Trade

DIFA – Diploma in Forensic Accounting

ECPA – The Electronic Communications Privacy Act

ESDC – Employment and Social Development Canada

EU – European Union's

FAMG – Forensic Accounting Management Group

FCA – Fellow Chartered Accountant

FCFI – Fellow Certified Forensic Investigator

FCPA – Fellow Certified Professional Accountant

FINTRAC – Financial Transaction and Reports Analysis Centre of Canada

FTC – Federal Trade Commission

Google – Google Inc.

GPEN – Global Privacy Enforcement Network

HRDC – Human Resources Development Canada

IFA – Investigative Forensic Accountant

IRS – Internal Revenue Service

ISO – International Organization for Standardization

ISP – Internet Service Provider

LL.B – Bachelor of Law degree

LL.D – Doctorate of Law degree

LL.M – Masters of Law degree,

MFIPA – Municipal Freedom of Information Act

OBA – Online Behavioural Advertising

OECD – Organisation for Economic Co-operation and Development's

OPC – Office of the Privacy Commission of Canada

OPHIP – Ontario Personal Health Information Protection Act

OPP – Ontario Provincial Police

PA – Privacy Act

Patriot Act – USA PATRIOT ACT

PCMLTFA – Proceeds of Crime (Money Laundering) and Terrorist Financing Act

PIPEDA – Personal Information Protection and Electronic Documents Act

Privacy Legislation – Privacy Protection legislation

PSC – Public Service Commission

PwC – PricewaterhouseCoopers

SIN - Social Insurance Number

SIR – Social Insurance Register

TBS – Treasury Board of Canada Secretariat

U.S. – United States of America

UN – United Nations Organization

USD – United States dollar

2. Research Objectives

As the world has become increasingly connected, concerns regarding the security of electronic personal data have developed and grown. In response, governments across the globe have established varying levels of legislation regarding the collection and use of such data.

This research paper will study the development of privacy legislation, both in Canada and abroad, and explore whether this has had an impact to Investigative Forensic Accounting (herein referred to as "IFA") engagements and investigations.

It should be noted that the ideas, views and interpretations presented in this paper should not be considered legal advice and are solely those of the author. The ideas and suggestions presented in this document are for discussion purposes only. Prior to relying on the cases and issues outlined in this paper, the author recommends that readers seek legal counsel and that this report is carefully examined and reviewed by legal professionals on a cases by case basis.

3. Research Scope

This research paper will focus on the development of Canadian privacy protection legislation ("privacy legislation"), areas where there have been breaches of the applicable legislation and regulations, and the possibility of implications on IFA engagements and investigations. It will also offer a brief comparison of Canada's privacy legislation with the legislation established in both the United States of America and the European Union.

To understand privacy legislation in both Canada and abroad legal text books, on-line legislation, and on line articles on government websites were consulted, along with the annual Privacy Commissioner reports. Research of case law was conducted to identify cases related breaches in privacy legislation. Finally, interviews were conducted with practicing IFA and members of the legal and private sector communities to investigate how they adjusted to the opportunities and challenges associated with privacy legislation.

The specific documents reviewed and relied upon in preparing this research paper are referenced in each section and outlined in the attached bibliography.

4. Introduction

Discussion surrounding the increased use of personal data and the protection of private information has been increasing at an exponential rate since the introduction of early computing machines in the 1940s. Intended to improve efficiency, early computers were large, cumbersome, and prohibitively expensive. They were typically locked in self-contained rooms with limited access to the outside world. Until that point, access to personal information was largely restricted to physical paper copies which limited the analysis and sharing of data. As such, privacy violations were unusual and largely restricted to internal breaches within a given organization. (Barabara McIssac, 2007)

With the introduction of personal computers in the late 1980s and early 1990s, individuals and systems began to connect – at first locally by early networks within companies, then globally with the introduction of the Internet – and the landscape of how information was being collected, transferred, and used changed as a result.

Today, many people own, or have access to, a personal computer, and to a lesser extent, a tablet, smart phone, smart television, or gaming system all of which are connected to the Internet. All of these devices transfer and process data, but this transfer has become so commonplace and natural that it is rarely ever considered or questioned. High-tech online databases allow information to be analyzed, processed and dissected at ever-increasing speeds, and offer the ability to identify specific individuals with greater accuracy, most of the time without the individual's knowledge or consent. (Barabara McIssac, 2007)

Since appropriate access to information is an ever growing concern, an IFA should stay abreast of the federal, provincial, and municipal legislation that could result in engagements and/or impact their investigations. As such an IFA must be able to determine if more information has

been obtained or reviewed than is relevant to her or his investigations, and she or he should understand the protocols for reporting and investigating instances where there have been infringements on individual privacy and private personal information.

5. Federal Privacy Legislation in Canada

The Canadian government became concerned about the security of personal information as early as the 1970s as personal computers were being introduced. Since then, several Federal legislative initiatives were developed and implemented including (Holmes N. , 2008):

- An amendment to the *Canadian Human Rights Act* (CHRA) in 1977 to include the first Federal public sector privacy protection
- The *Privacy Act* in 1983 along with the *Access to Information Act* (ATIA) from Bill C-43, in response to the Council of Europe's enactment of the *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* in 1980
- A commitment in 1984 by the Government of Canada to the Organisation for Economic Co-operation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Appendix A) which led to the development of the Canadian Standard Association's (CSA) *Model Code for the Protection of Personal Information* (Appendix B)
- The *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 2000 in response to the European Union's (EU) enactment of Directive 95/46/EC in 1995. If Canada failed to implement privacy legislation protecting the transfer of private information Article 25 of the Directive would have prevented Canada from conducting business with the European Union.

The Privacy Act [1]

Established in 1983, the Privacy Act is a data protection law that applies to approximately 250 federal government departments and agencies. Comprised of three components (see list below), it has been referred to as "the information handler's code of ethics" – although it is interesting to note that Section 8 of the act specifies thirteen areas where personal information may be disclosed without the consent of the individual. (Bernal-Castillero, 2013):

1. Grants an individual the legal right to access personal information held about his or her by the federal government (Sections 12 to 17);
2. Imposes obligations on the federal government with regard to how it collects, maintains, uses, and discloses personal information under its control (Sections 4 to 11); and
3. Establishes an independent ombudsman, the Privacy Commissioner, to resolve problems and oversee compliance with the legislation (Sections 29 to 40).

The Personal Information Protection and Electronic Data Act (PIPEDA)[2]

Established in 2000, and put into effect over three stages from 2001 through 2004, PIPEDA was created to support and promote electronic commerce: [3]

- In 2001 it was only concerned with the interprovincial and international trade of personal information as it pertained to the federally regulated private sector

[1] The consolidation of the *Privacy Act* R.S.C., 1985, c. P-21, is published by the Minister of Justice and is available on the website: http://laws-lois.justice.gc.ca.

[2] The consolidation of the *Personal Information Protection and Electronic Documents Act* S.C., 2000, c. 5, is published by the Minister of Justice and is available on the website: http://laws-lois.justice.gc.ca.

[3] "PIPEDA is limited in its scope to commercial activities because the provinces of Canada have exclusive jurisdiction over matters of private property and civil rights. The federal government therefore chose to regulate this area on its general power to regulate trade and commerce." (Holmes N. , 2008)

(broadcasting, telecommunications, banking, interprovincial transportation, and airline industries);

- It was expanded in 2002 to cover personal health information; and
- In 2004 it was further expanded to include all organizations located within the province even if they collect, use or disclose information only within that province.

In addition to the privacy principles established by the CSA (Appendix B), PIPEDA included rules governing the collection, use and disclosure of personal information by organizations in the private sector, as well as employees of federally regulated organizations during the course of commercial activities (Section 4.1).

At the time of this report only Alberta, British Columbia and Quebec have legislation that supersedes PIPEDA for both personal and personal health information. Other provinces, such as New Brunswick, Ontario, and Newfoundland and Labrador, whose legislation pertains solely to personal health information, are still regulated by PIPEDA with respect to the private sector, and interprovincial and international transactions. (Personal Information Protection and Electronic Documents Act, 2014).

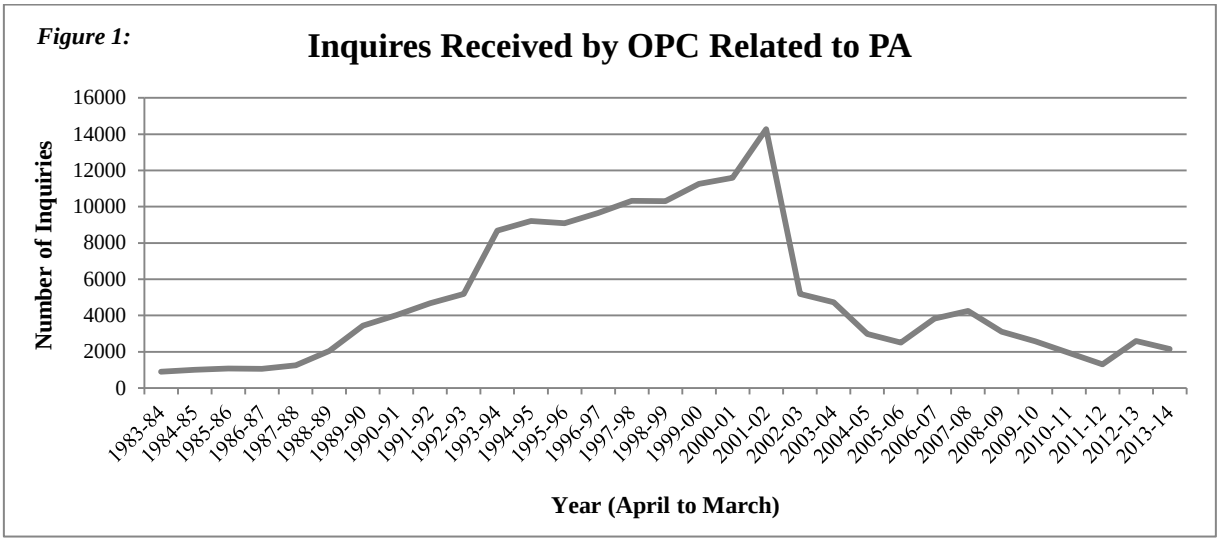
The Privacy Commissioner

In response to a federal government task force report on privacy and computers in 1977, the Government of Canada created the Office of the Privacy Commission of Canada (OPC) under the Human Rights Commission to review and investigate complaints from the general public regarding breaches in personal privacy (Holmes N. , 2008).

Annually, the OPC releases a report which includes the privacy issues that were reported, the inquiries that were received, a summary of the findings, and any research that was conducted by the OPC under both the Privacy Act and PIPEDA. One of the interesting outcomes of these reports has been that the public appears to be more concerned with the security and use of their personal information than the processes by which this information was collected, stored or disposed.

The following figures provide a summary of the inquiries and complaints received by the OPC since its inception.

Figure 1:



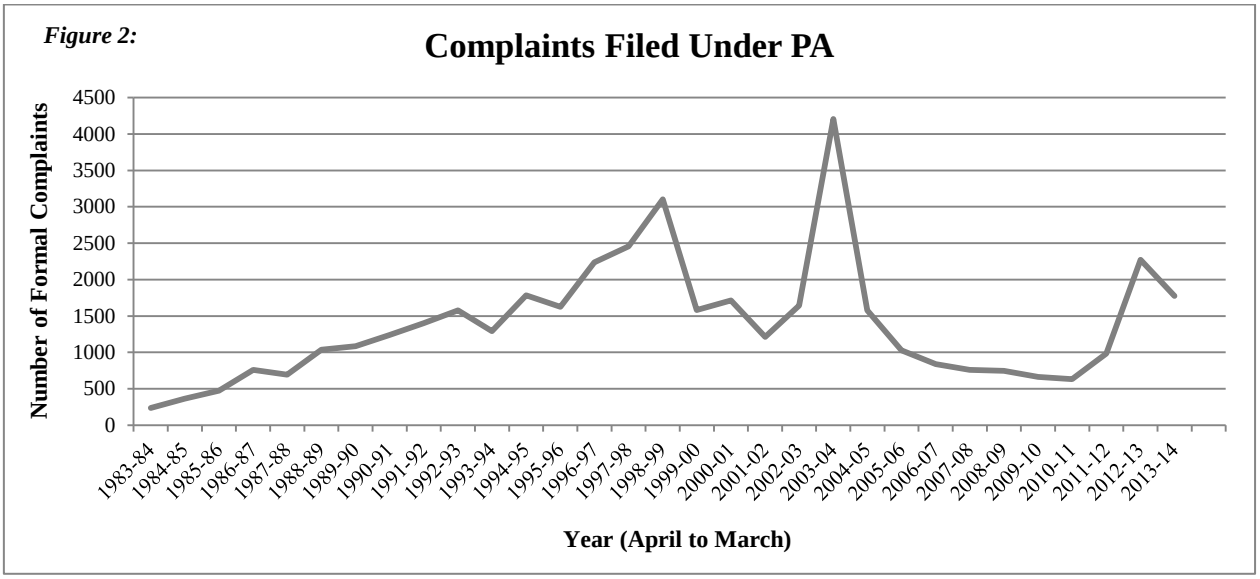
Source: OPC Annual Report on the PA to Parliament for the years 1983 to 2014

The notable peak in inquiries during the 2001-02 period illustrated in figure 1 are related to the events of September 11, 2001 and the resulting concerns surrounding the privacy of information.

In comparison, the number of complaints filed with the OPC had three notable peaks since its inception:

- The first peak in 1998-99 was the result of complaints surrounding the misuse of information collected from returning travelers through the customs declaration forms (E-311) which was compared against employment insurance claims, and delays in the release of personal information by the Cowansville (Quebec) Correctional Institute, National Defense, and Canada Revenue Agency (CRA);
- The second peak in 2003-04 was the result of:
    - Complaints against Health Canada from over 470 members of Canada's aboriginal communities around the consent form that was required to receive government-funded health benefits; and
    - More than 1,300 complaints filed against Correctional Services Canada (CSC) and the Joyceville Institution regarding delays in the release of personal information.
- The third peak in 2012-13 resulted from two significant data breaches involving Employment and Social Development Canada (ESDC) and the Department of Justice Canada. The Privacy Commissioner filed 1,159 of the 2,273 complaints as a result of the data breaches, while the remaining complaints resulted from a breakdown in employer-employee relationships within federal institutions and the sharing of personal information with third-party providers (i.e. telemarketing firms).

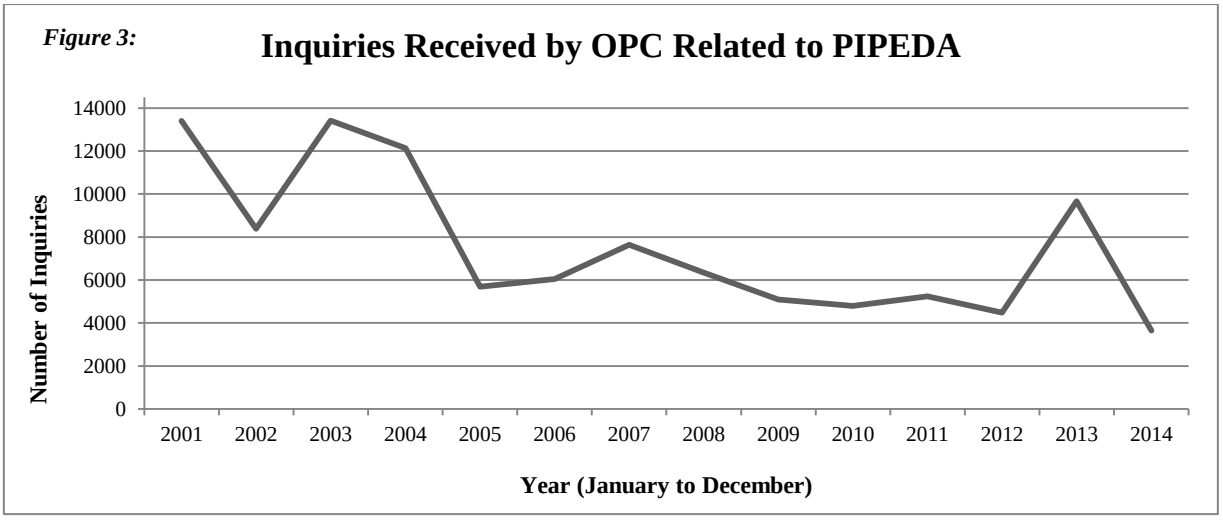
Figure 2:



Source: OPC Annual Report on the PA to Parliament for the years 1983 to 2014

Unlike the Privacy Act, the volume of inquiries and complaints filed and completed under PIPEDA have mainly decreased year over year as illustrated in Figures 4 and 5.

Figure 3:



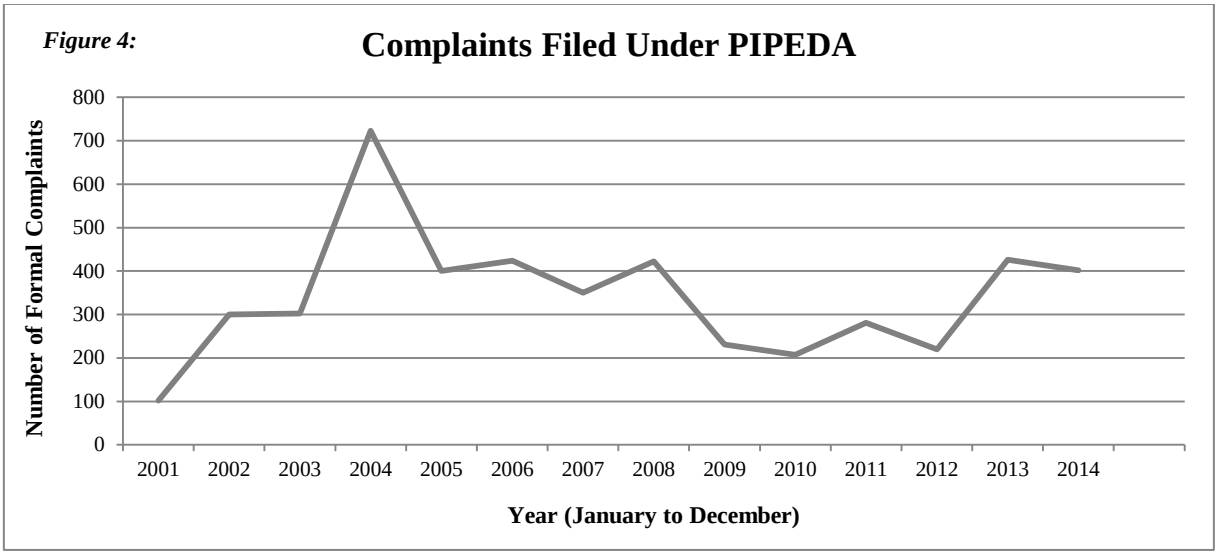
Source: OPC Annual Report on PIPEDA to Parliament for the years 2001 to 2014

The peak between 2001 and 2004 occurred as the Act came into effect and is largely related to the events of September 11, 2001. Following a notable decline, the number of inquiries peaked

again in 2013 resulting from investigations being conducted by the OPC in relation to Google and Apple.

With regards to the number of complaints filed with the OPC, there were two notable peaks since its inception. The first, in 2004, resulted from the implementation of a fast track process for completing investigations, and a one-time infusion of funds from the Treasury Board that was used to hire contract workers. The second, in 2013, resulted from a new marketing initiative from Bell Canada that prompted the OPC to conduct an investigation.

Figure 4:



Source: OPC Annual Report on PIPEDA to Parliament for the years 2001 to 2014

6. Privacy Infringement

As individuals and organizations are increasingly connected within an ever changing digital landscape, the data being exchanged becomes more vulnerable to breaches. These may occur as a result of:

- Unintended disclosure – such as information posted on a public website, or sent to the wrong party by email, fax, or regular mail;
- Hacking or malware – i.e. electronic entry through spyware;
- Payment card fraud – using skimming devices on point-of-service terminals, for example;
- Insider breaches – whereby information is intentionally shared by someone with legitimate access to that information; or
- Physical loss of equipment (i.e. laptops, smartphones, and portable memory devices, etc.) (Barabara McIssac, 2007)

Technology and Processes that Cause Concern Regarding Privacy

With the rapid advancement of technology, security systems on large scale networks and servers can quickly fall behind. In addition, most technology manufacturers are often so focused on releasing new products and developments quickly to gain an edge over their competition that concerns regarding security may not be adequately addressed before the product is released.

Some areas of potential concerns identified include (Barabara McIssac, 2007):

- *Single number identifiers*: Such as serial codes included in computers or software. Registering the products makes personal information available to manufacturers and software owners which may then be used to track user activity unknowingly;
- *Smart cards or devices*: The integrated circuit chips may hold encryption passwords, unlock secure doors, or financial information that permit "tap payment" capabilities;
- *Intelligent transportation systems*: Such as NEXUS passes for international travel, toll highway transponders, vehicle Global Positioning Systems (GPS), and OnStar services, all monitor an individual's movement;
- *Geographical information systems*: These database management systems facilitate the storage, retrieval, manipulation and analysis of spatial and temporal data related to the management of land, conservation, resources, emergency and disaster response, medical and health information, transportation, law enforcement, military systems and commercial systems;
- *Workplace monitoring*: Including video surveillance, telephone surveillance, computer monitoring, emails and voicemails, along with access cards and keypads all monitor employee movements within the company; and
- *Internet and online systems*: These systems allow for the extremely efficient and timely compilation and analysis of vast amounts of personal data at very low costs to a business.

Almost invisibly, these systems conveniently gather, display, retain, and analyze significant amounts of information that could be unknowingly used for other purposes. For example, the swiping of a pass card may give employees access to a secure floor, but it also gives the

company data which could be used to track employee movements throughout the day. Similarly, each time a provincial health card is used for a routine checkup or medical emergency that information can be used to monitor health service use, prescriptions and medical treatment for the individual and the population as a whole.

Security Breach of Privacy

Security breaches involving the theft or misuse of personal information appear in the media almost daily. Some recent notable events include:

- Adobe – July 2013[4] (but discovered in September 2013): attackers gained access to Adobe's servers and impacted 38 million individuals. The implication of this breach is that although Adobe claimed they had strong information security practices the breach still occurred and customers of Adobe may lose confidence in the company, its practices and potentially the products it sells.
- Health Canada – November 2013[5]: letters sent to 40,000 medical marijuana users resulted in a class action suit because the envelopes disclosed information that could identify individuals who were licensed to possess or grow medical marijuana. The implication of this breach is a loss of confidence in Health Canada and its ability to maintain sensitive confidential information and the potential impact to personal security from individual's that want to obtain access to the marijuana.

[4] See article, *Adobe Plans to Settle Breach Lawsuit*, for details of the breach and resolution, available at http://www.bankinfosecurity.com/adobe-plans-to-settle-breach-lawsuit-a-8174/op-1.

[5] See article, *Medical pot users seek class action against Health Canada*, for details of the breach, available at http://thechronicleherald.ca/metro/1292449-medical-pot-users-seek-class-action-against-health-canada.

- Canada Revenue Agency (CRA) - November 2014[6]: in response to a request made under the Access to Information Act, CBC was inadvertently sent an 18 page spreadsheet which detailed highly confidential information on the private lives of hundreds of Canadians, including many prominent citizens. The implication of this breach is the loss in confidence in the processes CRA implements to secure the vast amount of personal information that they have in their possession and their abilities to keep it secure. This breach also allowed a public forum, like the CBC, to gain access to highly confidential information and publish it under the "guise" that it was reported for journalistic reasons; to inform the public.
- United Stated Government - December 2014[7] : hackers apparently working for the Chinese state accessed personal information on four million federal employees from the Office of Personnel Management of the United States Government. It represented the largest security breach and second major intrusion from the same agency in the last year. This implication highlighted the fact that the Federal computer networks, who should maintain state-of-the-art defenses against security breaches, may have a system that is not secure.
- Samsung - December 2014[8]: a software flaw in the pre-installed predictive text technology used by 600 million of its Galaxy smartphones made them vulnerable to hackers during updates. Samsung released corrective patches at the start of 2015. The implication of this breach could include a loss of Samsung customers, a loss of

[6] See article, *Canada Revenue Agency privacy breach leaks prominent Canadians' tax details*, for details of the breach, available at http://www.cbc.ca/news/politics/canada-revenue-agency-privacy-breach-leaks-prominent-canadians-tax-details-1.2849336.

[7] See article, *Chinese breach data of 4 million federal workers*, available at http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

[8] See article, *Samsung Galaxy: What you need to know about reported security risk*, for details of the breach, available at http://abcnews.go.com/Technology/samsung-galaxy-reported-security-risk/story?id=31825944.

business reputation and a loss of belief in the security of personal information contained on the smart phone.

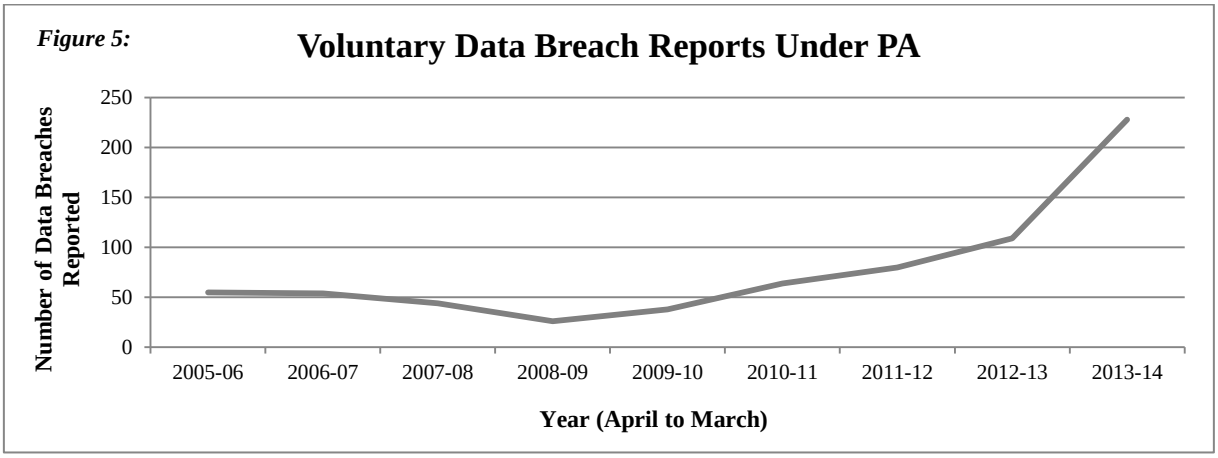
- Internal Revenue Service (IRS) – May 2015[9]: criminals used stolen data to access detailed tax information on 104,000 tax payers and use this information to file fraudulent returns. The implications of this breach are similar to the breach experienced by CRA in that the American population may loss confidence in the systems offered online by the IRS and the IRS' ability to secure the vast amount of personal information that they have in their possession.

Security Breaches Reported by the OPC

Under the Privacy Act and prior to the release of Treasury Board of Canada Secretariat (TBS) guidelines on privacy practices, there were 55 voluntary reported incidents of security breaches in 2005-06 (Figure 5). By 2008-09 that number fell to twenty-six. Although the decline could be attributed to improved processes at the OPC, it is also possible that since the requirement to report errors is voluntary that government agencies may have chosen to not report errors or mistakes to the OPC and correct them internally.

[9] See article, *Cyberattack Exposes I.R.S. Tax Returns*, for details of the breach, available at http://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html?_r=0.

Figure 5:



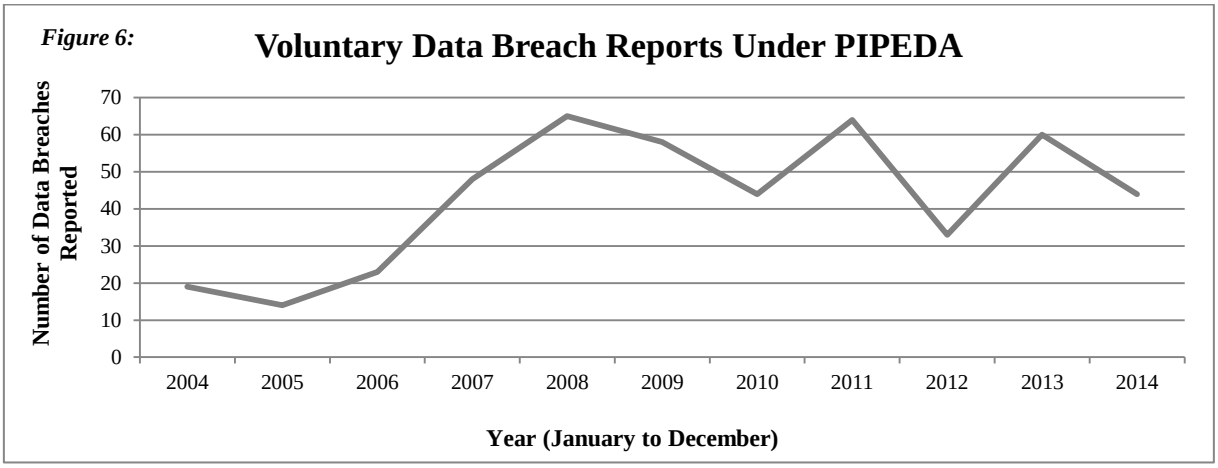
Source: OPC Annual Report on the PA to Parliament for the years 2005 to 2014

By 2013-14, the number of voluntarily reported security breaches rose sharply, likely as the natural result of changes to the TBS *Directive on Privacy Practices*[10] which came into effect in May 2014 and required government institutions covered by the Privacy Act to report all material data and privacy breaches to the OPC and the TBS.

The OPC also monitors and investigates security breaches reported under PIPEDA. As with the Privacy Act, the reporting of breaches was initially minimal (19 incidents in 2004 and 14 in 2005), and occurred only on a voluntary basis. Unlike the Privacy Act, however, the reporting of privacy and security breaches year over year has been sporadic (Figure 8). In 2008, the number of voluntarily reported breaches reached a peak at 65 incidents then declined until 2011 where it peaked again at 64 voluntarily reported breaches. By 2012 the number of reported breaches was almost half that value at 33 breaches then almost doubled in 2013 when 60 breaches were voluntarily reported.

[10] The full Directive on Privacy Practices can be found at http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309.

Figure 6:



Source: OPC Annual Report on PIPEDA to Parliament for the years 2004 to 2014

Since the reporting of privacy breaches is not mandatory under PIPEDA, it is not unexpected that number of reported incidents would vary year over year. To improve the reporting requirements the OPC has been working to develop standardized guidelines. However unlike the reporting requirements under the Privacy Act, as of 2014 there is no obligation for entities covered under PIPEDA to report data and privacy breaches.

Ways to Protect Personal Information

The increase in privacy infringement has prompted the development of systems and software which could be purchased by individuals and corporations to help protect their information. Examples of these systems include:

- *Anonymizers* – Software which remove the user's personal identity (such as a blocked phone number or anonymous email repliers);
- *Anonymous Payment Mechanisms* – Programs which protect the identity of the buyer in electronic transactions (such as PayPal, Digi cash or gift cards);

- *Pseudonymizers* – Software that uses a combination of anonymizers and aliases to allow individuals to establish relationships with vendors or suppliers without releasing personal information (such as Lucent's personalized web assistant);
- *Privacy Labels* – Programs that enable a web page to carry a machine readable label signifying its compliance with a particular privacy policy (such as. TRUSTe, CA web trust or BBBonline);
- *Privacy Icons* – Simple visual cues of a website's privacy policy that users must click on to signify their acceptance prior to proceeding (such as Mozilla and Disconnect privacy icons[11]);
- *Data Exchange Technology* – Programs, such as Open Profiling Standard (OPS), that create a profile to allow individuals to select the personal information that is released each time a web page is accessed. This technology was initiated by Netscape, FireFly Network, Inc. and VeriSign, Inc. in May 1997[12];
- *Trusted Third Party* (TTP) – Independent third party services are services that are trusted by both the user and the service provider. The third party is expected to keep personal information private but can release it when certain conditions are met (such as TRUSTe privacy services[13]);
- *Pressure from business partners* – For example, to gain part of the advertising budgets from IBM and Microsoft, companies and advertising agencies wishing to work with them must develop and implement policies to protect the privacy of their consumers; and

[11] See article, *New Visual Icons Introduced to help People Easily Understand Online Privacy Policies*, for complete details of the creation of privacy icons, available at http://www.marketwatch.com/story/new-visual-icons-introduced-to-help-people-easily-understand-online-privacy-policies-2014-06-23.

[12] See article, *Open Profiling Standard*, for details, available at http://www.farces.com/wikis/ie/chap-07/open-profiling-standard/.

[13] Services provided by TRUSTe include TTP compliance. Visit their website for further details at https://www.truste.com/.

- *Electronic Commerce Insurance* – Internet liability insurance cover breaches related to: system failures; theft; loss or misuse of data; loss of financial funds and/or a network shutdown. While this is not a solution for privacy infringement, it limits the risks faced by users (examples include Brokers Trust Insurance Group Inc. Technology, IT and Ecommerce insurance coverage for commercial insurance[14]) (Barabara McIssac, 2007).

[14] Refer to Brokers Trust Insurance Group Inc. website for information related to commercial technology, IT and ecommerce insurance products, available at http://www.brokerstrust.ca/technology.php.

7. IFA Engagements and Investigations

There are two sections under the Privacy Act that may provide engagements for an IFA or potentially impede her or his investigation. First, Section 8 covers thirteen areas where personal information may be disclosed without the consent of the individual. This could lead to the perception of breaches in privacy, resulting in complaints that must be investigated. Second, the Exemption Sections (18 to 28) could hinder investigations because the information required to conduct the investigation may be restricted, or the client is unable to obtain the information due to the exemption rule.

As with the Privacy Act, there are sections of PIPEDA that may impact an IFA engagement and/or investigation. Section 7 or Part I (similar to section 8 or the Privacy Act) covers the collection, storage, or disclosure of personal information without an individual's consent. Since the reason this data was original provided may have little to no relation to the reason it is being gathered or disclosed, it may lead to perceptions that an individual's privacy is being infringed upon, and could prompt complaints and investigations.

Under Section 8 of PIPEDA individuals may request access to their information because of concerns surrounding the accuracy of information being stored is accurate. Individuals may also request to discover what could potentially be released in the event of a security breach. Understanding the process of how information is stored and disclosed by an organization, along with their expected timelines for release of the disclosure, can assist an IFA during an investigation if information needs to be requested. It may also help an IFA understand that clients may perceive that their privacy is being infringed if the process takes longer than expected, or the client has been declined access without being provided the reason for it.

During an investigation, an IFA must ensure that the collection of data follows a systematic approach so as not to compromise the gathering and collecting of electronic evidence. Computer forensics may be applied:

- Where digital information forms the basis of an investigation; or
- To identify potential violations of government regulations and legislation, or corporate policies that may result in civil litigation actions (Rufus, 2014).

When gathering computer forensic information, there are legal considerations that an IFA must bear in mind:

- To whom does the data belong;
- Does the IFA have legal authority to collect the data; and
- Are there corporate policies (and practices) that must be considered prior to collection?

If an IFA is involved in a civil case, a subpoena would grant the required authority, while in a criminal case, a search warrant would grant the required authority. If the investigation relates to an organization, then corporate policies, such as the policy on personal use of company-owned computers and cell phones and the personal use of company email must be considered. Also, adherence to privacy legislation (the Privacy Act and PIPEDA) that relates to confidential personal information must be observed as improper access to data stored on electronic devices may constitute a breach of federal or provincial laws.

Once the investigation or information gathering is complete, an IFA must ensure that the confidential information gathered and then used during the investigation is secured safely and not accessible to third parties who might misuse the information or tamper with it. When the engagement ends, the IFA must store her or his working file for an adequate amount of time to

ensure if there are further disputes or a request for access to the information relied on that it is available. If the confidential information must be disposed of, the IFA must ensure that the information is properly destroyed and cannot be retrieved.

Interviews of professionals working in the field of privacy protection

The following individuals were interviewed to gain a practical understanding of the privacy legislation and any potential impacts that it may have on IFA investigations and engagements (see interview questions in Appendix C).

- *Alex Cameron, LL.B, LL.M, LL.D,* and Partner with Fasken Martineau DuMoulin LLP[15] provided a lawyer's perspective
- *Tim Ticknor* a Detective Constable with the Ontario Provincial Police (OPP) in the Anti-Rackets Branch, Corruptions Unit[16] provided a law enforcement's perspective from the public sector
- *Ken Froese, FCPA, FCA•IFA, FCFI,* Senior Managing Director with Froese Forensic Partners Ltd.[17], *Sarah E. MacGregor, CPA, CA•IFA, CFE,* Partner with PricewaterhouseCoopers LLP (PwC) Investigation & Forensic Services[18], and *Pamela Morley, CPA, CA•IFA, CFE,* Senior Forensic Accountant with the Forensic Accounting Management Group (FAMG[19]) provided IFA perspectives from the private and public sectors.

[15] Information related to Fasken Martineau DuMoulin LLP Privacy and Information Protection services can be found at http://www.fasken.com/en/privacy-information-protection/.

[16] Information related to the Anti-Rackets Branch of the OPP can be found at http://www.opp.ca/ecms/index.php?id=186#2.

[17] Information related to Froese Forensic Partners Ltd. can be found at http://www.froeseforensic.com/.

[18] Information related to PwC's Investigations & Forensic Services can be found at http://www.pwc.com/ca/en/risk/forensic-services/index.jhtml.

[19] Information related to FAMG can be found at http://www.tpsgc-pwgsc.gc.ca/ggj-famg/index-eng.html.

All five interviewees were asked the same questions in the hopes that the responses would be consistent and comparable. Each interviewee was asked:

- To confirm the privacy legislation that was applicable to their respective field;
- To explain how the legislation related to her or his work;
- Whether the legislation restricted his or her work; and
- Whether the legislation imposed any limitations with regards to the access of information needed in the course of their duties.

A lawyer's perspective:

A prominent lawyer in the field of privacy protection, Mr. Cameron has been involved in cases related to breaches under the Privacy Act, PIPEDA, and most privacy protection legislation at the provincial level. As such he is "very mindful of the need for consent (either express or implied), and the need to safeguard personal information (Cameron, 2015)". According to Mr. Cameron, while privacy legislation could have the same potential impact on both the private and public sectors, it is likely that the private sector may experience more infringements since the legislation is less comprehensive in that area.

In Mr. Cameron's view, "[privacy legislation] has rarely limited an investigation, although many times careful consideration needs to be given to limiting the collection, use, and disclosure of personal information to that which is necessary for the purpose of the investigation (Cameron, 2015)". Normally, implied consent with regards to the collection of information which could be crucial to a case is given when a client engages a lawyer. According to Mr. Cameron, "in rare cases where an infringement has occurred, the information would normally still be used in the investigation and any legal proceedings, and the courts

would admit the evidence. [The use of this information] might then give rise to a separate liability for invasion of privacy (Cameron, 2015)".

With regards to investigations, access to personal information is perhaps one of the larger impacts of the Privacy Act and PIPEDA. Although limited in scope, both of those forms of privacy legislation provide situations whereby information could be collected without an individual's knowledge or consent. Information collected during an investigation, however, does not fall under any of these exceptions as outlined in PIPEDA. As a result, an injunction would need to be obtained before any data collection could occur. When a third party (such as law enforcement) is unwilling to disclose information without consent from the individual in question, a subpoena or court order could be obtained to allow the necessary data to be collected.

According to Mr. Cameron, updates to PIPEDA should include extending the list of exemptions to include the collection, use, and disclosure of information during an investigation. Obtaining injunctions and subpoenas, which are required under the current legislation, has the potential of alerting individuals of possible investigations before they are conducted, given them time to potentially alter any information or data that could be obtained.

A law enforcement perspective:

Being a government employee, Mr. Ticknor has to comply with the Privacy Act, PIPEDA, and as the *Municipal Freedom of Information Act (MFIPA)* when conducting investigations. Part of his role is to ensure that the information gathered or disclosed during an investigation is done according to the law otherwise it may not be admissible and could compromise the collection of information going forward.

According to Mr. Ticknor, there is greater risk of privacy breaches in the private sector. Unlike their counterparts, the public sector has received detailed training and people who are responsible for reviewing and approving information requests to ensure that no breach of security occurs (Tim, 2015).

As with Mr. Cameron, Mr. Ticknor must also obtain production orders or warrants in order to obtain the necessary information during investigations. The current privacy legislation has also impacted his work with lawyers and accountants it provides limitation on the amount and type of information that they are required to disclose. A memorandum of understanding, or a waiver signed by the client permitting full disclosure could improve the working relationship, but it may also compromise the information that is obtained by alerting individuals that they may be the subject of an investigation.

According to Mr. Ticknor, one of the largest contributing factors with respect to privacy infringement is the lack of public knowledge. He maintains that "people need to be educated on the various legislations so as not to breach them (breaches usually occur through people trying to be helpful but not knowing the boundaries)." (Tim, 2015)

An IFA working with the OPP perspective:

Ms. Morley is a Senior Forensic Accountant with the Forensic Accounting Management Group (FAMG), the Government of Canada that provides support to investigations conducted by law enforcement. Similar to Mr. Ticknor, as a government employee Ms. Morley must comply with both the Privacy Act and PIPEDA when conducting investigations. She must also comply with the *Ontario Personal Health Information Protection Act* (OPHIP), the *Municipal Freedom of Information Act* (MFIPA), sections of the *Canada Evidence Act* and sections of the

Criminal Code of Canada. Since Ms. Morley works mainly with law enforcement, they ensure that all issues of privacy infringement are addressed prior to the information being provided to Ms. Morley's team for investigation. (Morley, 2015)

There are times during an investigation when the information provided to Ms. Morley has been "cleansed" of personal information that does not directly pertain to an investigation. Ms. Morley advised that "if the individual was not named in the Production Order, then their names are redacted (Morley, 2015)." At the same time, when Ms. Morley prepares reports for the OPP certain personal information must be removed in order to reduce the possibility of privacy infringement.

During an investigation, if Ms. Morley was provided with more information than was required, she would ignore the information and not include it in her reports (Morley, 2015). Since she did not obtain the documents directly she does not have to worry about whether the documents were obtained via appropriate judicial channels. Also, since Ms. Morley works primarily with law enforcement there is minimal impact, if any, to her engagement and investigations by the privacy legislation in place. (Morley, 2015)

<u>An IFA working in the private sector perspective</u>:

Ms. MacGregor is a Partner with PricewaterhouseCoopers LLP (PwC) Investigations & Forensic Services practice working in the Forensic Services Group. Based on her experience, Ms. MacGregor is not aware of whether the public or private sector is impacted more by privacy legislation (MacGregor, 2015). Ms. MacGregor has been involved in engagements where an investigation into the leakage of confidential information has occurred but has not specifically worked on an engagement involving a breach of privacy legislation directly (MacGregor, 2015).

During the course of an engagement, Ms. MacGregor must consider the implication of both the Privacy Act and PIPEDA from the acceptance to the conclusion of the engagement. Ms. MacGregor indicated that privacy legislation has not limited the acceptance of any engagement but has caused her to "consider the necessity of information to be obtained in the course of [her] work to ensure [she] is not obtaining sensitive information (MacGregor, 2015)." When she is working on an engagement she will use the best information that is made available to her and if there is information missing, or she was unable to obtain access to, she would reference this limitation in her report and provide a detailed listing of the information she has relied on (MacGregor, 2015).

If Ms. MacGregor was faced with additional information in an engagement that was not considered relevant to the investigation, she understand that there might be unnecessary risks relating to privacy infringement and would "communicate with the client and with legal counsel to ensure there is no expectation gap in terms of the information required, provided and would be relied upon (MacGregor, 2015)." If Ms. MacGregor viewed that the information received was important to the investigation, she would consult with legal counsel before accepting or proceeding with the engagement.

Finally, Ms. MacGregor believes that the largest risk of infringement of privacy legislation during an investigation can occur during the collection of relevant and necessary information in order to successfully conduct an investigation. Ms. MacGregor advised that 'there could be sensitivities in the information required and provided that could result in infringement, therefore it is important to consult legal counsel to ensure all requirements are followed (MacGregor, 2015)."

A second IFA working in the private sector perspective:

Mr. Froese is the Senior Managing Director of Froese Forensic Partners Ltd., and works with former police officers, eDiscovery and digital forensic specialists as well as forensic accountants and valuators. In the course of Mr. Froese's work, he has to consider the implication of privacy protection legislation not only in Canada but globally as his firm provides services internationally.

Mr. Froese believes that the private sector is impacted most often in relation to privacy infringement as "the private sector is much larger and has applied much fewer resources to privacy, especially in smaller businesses. They are thus more vulnerable to privacy breaches due to the lack of awareness of the legislation, and also due to less robust file servers and websites where information may be stored (Froese, 2015)."

Mr. Froese believes that the impact to an engagement as a result of privacy legislation has been mainly a restriction on the access to information from "financial, communication and other institutions and it has reduced the use of pretext calls (which were quite limited in any event) (Froese, 2015)." In order to address this restriction during an engagement, Mr. Froese "clearly sets out what we can and can't do, what requires a consent and the related documentation required to accompany the consent such as appropriate photo ID (Froese, 2015)." Since Mr. Froese is also licensed as a private investigator, the impact on engagements is reduced, but not eliminated, as this credential allows him the ability to share personal information in order to gain access to information (Froese, 2015).

If information is provided during an engagement that is outside the relevance and requirements of an engagement, Mr. Froese obtains legal advice on how to address the information received.

If the information received was deemed to be crucial to the results of an engagement then Mr. Froese would again obtain legal counsel on to what extent the information, not requested but received, could be used (Froese, 2015).

Finally, Mr. Froese believes that the largest risk area for infringement on privacy legislation occurs when determining the use of personal information that was obtained according to legislated requirements but would be included in a report that will be made available to the public. Mr. Froese advised that one must consider what information is essential to the report, what information is actually personal and should not be made available to the public and should names or bank account numbers be removed or deleted in order to protect the individual's privacy (Froese, 2015). "Often in conducting interviews in investigations we get far more personal information concerning other employees, contractors, etc. than is ultimately required, but it provides a profile/background that helps direct the investigation. As well, when we contract for surveillance we have had issues where the video goes beyond public spaces to someone walking into and out of home; other persons may be in the video; etc. Depending on the use of the video, there needs to be care taken in ensuring evidence used doesn't violate privacy legislation (Froese, 2015)."

A Review of Privacy Commissioner Findings

Reports produced through the Office of the Privacy Commissioner of Canada (OPC) were consulted to see if there were any potential impact on privacy in relation to IFA engagements and investigations. Careful review of their findings did not reveal any infringements that were cause by an IFA or the result of a forensic investigation. Most of the privacy impacts that were investigated were the result of the actions of an individual or organization and not as a result of the investigations being conducted.

A selection of the more interesting findings under both the Privacy Act and PIPEDA are included below:

Under the Privacy Act:

- A complaint filed with the OPC against the Canada Mortgage and Housing Corporation in 2001-02 (Radwanski, 2001) led the OPC to request that other agencies change their practices since the requirement to provide tax information (which is regulated under the *Income Tax Act*) was an infringement to the Privacy Act.
- In 2002-03 (Marleau, 2003), the unauthorized disclosure of a complainants social insurance number to a private investigator of an insurance company by an employee of Human Resources Development Canada (HRDC) lead to the discovery of a larger infringement involving approximately 40 other client files accessed by the same employee on the Social Insurance Register (SIR) system. The larger concern was that managers working at HRDC were not monitoring the activities of employees and the SIR system which allowed the release of private information without consent. HRDC mitigated risks by implementing measures to significantly enhance the security of personal information contained in the SIR system and began monitoring employee's access to SIR in order to prevent further infringements on under the Privacy Act.
- In 2005-06 (Stoddart, Annual Reports to Parliament 2005-2006: Report on the Privacy Act, 2006), the Public Service Commission (PSC) disclosed personal information related to three auditors in an audit report that was released to the media. It was found that since the institution that was audited was small in nature, the views expressed in the report could easily be linked to the individuals that conducted the audit and therefore infringed on the individuals privacy (Stoddart, Annual Reports to Parliament 2005-2006: Report on the Privacy Act, 2006). To

rectify this, PSC now requires that all audit reports be reviewed by the Access to Information and Privacy Branch of the PSC prior to releasing the reports to the media to ensure the report does not include information that is subject to the Privacy Act (Stoddart, Annual Reports to Parliament 2005-2006: Report on the Privacy Act, 2006).

- In 2008 (Stoddart, Annual Reports to Parliament 2007-2008: Report on the Privacy Act, 2008), an employee of the Department of Foreign Affairs and International Trade (DFAIT) disclosed personal information related to a Canadian citizen being held in a foreign jail. The issues were that all DFAIT employees had access to the computer system and no audit trail capabilities were available to monitor who accessed which records. Further, there were no access restrictions in place (Stoddart, Annual Reports to Parliament 2007-2008: Report on the Privacy Act, 2008). To mitigate the risk of further disclosure of personal information, DFAIT agreed to rectify the security deficiencies of the computer system, ensure the system would have audit trail capabilities and restrict access to the system (Stoddart, Annual Reports to Parliament 2007-2008: Report on the Privacy Act, 2008). DFAIT also agreed to develop guidelines and trainings on the proper sharing of personal information between departmental and ministerial offices (Stoddart, Annual Reports to Parliament 2007-2008: Report on the Privacy Act, 2008).
- In 2014 (Therrien, Transparency and Privacy in the Digital Age: Annual Report to Parliament 2013-14: Report on the Privacy Act, 2014), a USB key containing personal information of Canada Pension Plan Disability appellants went missing while in the control of a Justice of Canada lawyer working in an office of Employment and Social Development Canada (ESDC). This was a second breach of its kind. The OPC found that neither ESDC nor Justice Canada had established meaningful business practices from the formal privacy and security policies it had in place at the time which resulted in careless actions of its employees (Therrien, Transparency and Privacy in the Digital Age: Annual Report to Parliament 2013-14: Report on the Privacy Act, 2014). Both

the ESDC and Justice of Canada have agreed to improve internal policies and processes in an effort to better protect personal information that is under each departments control in order to minimize a breach of the PA (Therrien, Transparency and Privacy in the Digital Age: Annual Report to Parliament 2013-14: Report on the Privacy Act, 2014).

Under PIPEDA:

- In 2005 (Stoddart, Annual Report to Parliament 2005: Report on the Personal Information Protection and Electronic Documents Act, 2006), a hotel required a guest to consent to releasing personal information to any member franchise or hotel chain as a condition of service at the hotel based on new federal privacy laws. The OPC found that the hotel infringed on principle 4.3.3 of PIPEDA by requiring a guest to sign a consent form that not only provided her or his personal information but required her or him to consent to the release of her or his personal information for use other that its original intended purpose (Stoddart, Annual Report to Parliament 2005: Report on the Personal Information Protection and Electronic Documents Act, 2006). It was recommended that the hotel amend the consent form to request whether a guest would like to be contacted about other offers of the hotel instead of requiring the consent in order to meet the criteria established under PIPEDA (Stoddart, Annual Report to Parliament 2005: Report on the Personal Information Protection and Electronic Documents Act, 2006).
- In 2007 (Stoddart, Annual Report to Parliament 2007: Report on the Personal Information Protection and Electronic Documents Act, 2008), a couple was denied their insurance claim when they refused to sign a consent form that gave the insurance adjuster the ability to collect a wide range of personal information. The OPC found that the consent form infringed on principles 4.3.3 and 4.4.1 as the form allowed the adjuster to collect personal information that is not relevant to the claim the individual was filing (Stoddart, Annual Report to Parliament 2007: Report on

the Personal Information Protection and Electronic Documents Act, 2008). The insurance adjuster and the Canadian Independent Adjusters' Association worked to redraft the consent forms and develop separate claim forms for property claims and injury claims which would require different types of personal information (Stoddart, Annual Report to Parliament 2007: Report on the Personal Information Protection and Electronic Documents Act, 2008). These forms were reviewed by the OPC to confirm they complied with PIPEDA requirements (Stoddart, Annual Report to Parliament 2007: Report on the Personal Information Protection and Electronic Documents Act, 2008).

- In 2009 (Stoddart, Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act, 2010), in attempts to collect an outstanding debt, a funeral home disclosed an individual's bankruptcy to their siblings in hopes that they would settle the outstanding debt. The OPC found that the funeral home had infringed on principle 4.3 of PIPEDA when it released personal information about an individual to a third party, namely the siblings of the individual (Stoddart, Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act, 2010) . The funeral home did not have *"carte blanche"* to disclose whatever information it wished in order to pursue the collection of a debt (Stoddart, Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act, 2010). The funeral home attempted to circumvent PIPEDA by clarifying that the bankruptcy was public knowledge since it appeared in a public record of filed bankruptcies but the OPC advised that the information in the public domain, collected under a statutory authority may only be used without consent if related directly to the purpose for which it appears in the registry (Stoddart, Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act, 2010). Calling the siblings and telling them about the bankruptcy in hopes to

collect the outstanding debt is in breach of PIPEDA (Stoddart, Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act, 2010).

- In 2014 (Therrien, Privacy Protection: A Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act, 2015), a complaint was filed against Google Inc.'s (Google) use of online behavioural advertising (OBA). When the complainant conducted a Google search for a medical condition, every website visited for the next month would display advertisements related to the condition he had searched. The OPC found that Google had infringed on principles 4.3 and 4.3.6 of PIPEDA in that Google targeted its online advertising based on sensitive health information of the complainant and was not following the OPCs OBA Guidelines (Therrien, Privacy Protection: A Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act, 2015). The OPC requested that Google comply with PIPEDA and align its online advertising policies with the OBA Guidelines (Therrien, Privacy Protection: A Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act, 2015). Google responded that the compliance issue was related to third party advertisers using the remarketing tool provided by Google. Google allows for remarketing for sites that are medical related but require that they comply with Google's privacy policy and the requirements of the remarketing program policy (Therrien, Privacy Protection: A Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act, 2015). The OPC felt that Google was not monitoring the remarketing tool and advertising streams enough to determine potential infringements of privacy and required that Google amend its systems, processes and remarketing tool to ensure that it remained compliant with PIPEDA and the OPC's OBA Guideline (Therrien, Privacy Protection: A Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act, 2015) s. Google is working to strengthen

its public interest-based advertising policies to restrict health related advertising, will develop internal training to keep staff abreast of privacy legislation requirements, increase the monitoring of remarketing advertising and upgrade its automated systems to remain compliant with PIPEDA (Therrien, Privacy Protection: A Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act, 2015).

Case Law Related to Privacy Infringement and the Outcomes

A review of the existing case law found no cases that were related to an infringement on privacy legislation by an IFA. The search included the Federal Court of Canada, Federal Court of Appeal, the Supreme Court of Canada, Court of Appeal, the Supreme Court of Canada, Cour of Appeal for Ontario, and Superior Court of Justice through CanLii.

Several cases exist which discuss how the Privacy Act and PIPEDA have been infringed upon, and discuss the use of forensic accountants to conduct investigations, but none have resulted in the infringement of privacy legislation by an IFA. This could be in relation to the fact that an IFA's engagement is through a lawyer or with a client and consent is given to the IFA to collect the needed information to conduct an investigation. Although an IFA must understand privacy legislation and how it might infringe on an investigation, the direct impact on the work itself appears to be is minimal if any.

8. Revisions and Updates of Privacy Legislation

Enacted in 1985, the Privacy Act has remained unchanged for more than 20 years despite feedback from numerous reports and government committees between 1987 and 2009.

In June 2006, the Privacy Commissioner (Ms. Jennifer Stoddard) presented *Government Accountability for Personal Information: Reforming the Privacy Act*, which outlined a comprehensive set of proposals for changes to the Act. In April 2008, an addendum was issued outlining 10 quick fixes, and a further revision in May of 2009 added 2 more (Appendix D). Currently none of these proposals have been enacted. (Bernal-Castillero, 2013).

In June 2009, the Access to Information, Privacy and Ethics Committee issued a response report, *The Privacy Act: First Steps toward Renewal*[20], endorsing the reforms that the Privacy Commissioner had suggested. In November 2013, when Ms. Stoddard addressed the Library of Parliament on *The Necessary Rebirth of the Privacy Act*, no reforms or in-depth reviews had been scheduled (Szabo, 2009). Based on the website for the Office of the Privacy Commission at the time this report was written, no review had been scheduled or conducted.

Revisions and Updates to PIPEDA

At the end of 2006 The House of Commons Standing Committee on Access to Information, Privacy and Ethics initiated the first and only review of PIPEDA, which was completed by February 2007. The review was conducted in compliance with section 29's requirement that a review occur five years from the date of enactment (Part I came into effect in January 1, 2001)

[20] A summary of the responses made by the Access to Information, Privacy and Ethics Committee have been included at Appendix E.

but the Committee felt that since the entire Act was not in effect until January 1, 2004, only a limited review was needed. (Bernal-Castillero, 2013)

The report presented by the Committee entitled, *Statutory Review of the Personal Information Protection and Electronic Documents Act*, provided 25 recommendations (Appendix F) which would harmonize the older federal legislation with the newer provincial privacy legislation established in Alberta, Quebec, and British Columbia. While the Committee agreed that fine-tuning of PIPEDA was in order, it did not advocate for any major changes to the legislation. (Wappel, 2007)

In 2010, the 40th Parliament introduced Bill C-29, but it did not proceed past the 2nd reading due to the dissolution of the Government in March 2011. The Bill was later reviewed, improved, and reintroduced as Bill C-12 in September 2011 but again did not proceed as a result of the dissolution of Government in September 2013. Finally, in April 2014 a current version of the Bill was brought before the Senate as Bill S-4.

Short-titled the *Digital Privacy Act,* the Bill S-4 goes beyond just amending PIPEDA. Expanding on the focus of its predecessor Bills C-29 and C-12, it included observations from the 2012 Privacy and Social Media study released by the House of Commons Standing Committee on Access to Information, Privacy and Ethics, and recommendations made by the Privacy Commissioner in her May 2013 position paper, *The Case for Reforming the Personal Information Protection and Electronic Documents Act*. (Lithwick, 2014)

As of June 2015, Bill-S4 is still before the government, and a second 5 year review of PIPEDA has not been initiated.

Additional Legislation Related to Privacy Protection

Enacted in December 1998, the *DNA Identification Act*[21] regulates the collection and storage of biological samples for Deoxyribonucleic Acid (DNA) analysis from anyone convicted of a designated offence (generally involving violence). It created a National DNA Data Bank and allows the National DNA Data Bank to share this information on a case by case basis with foreign jurisdiction in accordance with paragraph 8(2)(f) of the Privacy Act.

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*[22], enacted in June 2000, facilitates combatting the laundering of criminal proceeds and combatting the financing of terrorist activities as well as establishes the Financial Transaction and Reports Analysis Centre of Canada (FINTRAC). This Act requires that organizations subject to the Act undertake compliance activities which include client identification, record keeping activities and reporting certain transactions to FINTRAC.

The *Public Safety Act, 2002*[23], enacted May 2004, amended PIPEDA by allowing private sector organizations to collect personal information, without consent, for the purposes of disclosing this information to the government, law enforcement and national security agencies.

Bill C-37, *An Act to Amend the Telecommunications Act*[24] also known as the *"Do-Not-Call List Legislation"*, enacted in November 2005, allowed the Canadian Radio Television and Telecommunications Commission (CRTC) to establish a national bilingual do-not-call list where individuals not wishing to receive unsolicited calls could register their number. Telemarketers who call numbers on the national registry would be subject to monetary fines.

[21] This Act is available at http://laws-lois.justice.gc.ca/PDF/D-3.8.pdf.

[22] This Act is available at http://laws-lois.justice.gc.ca/PDF/P-24.501.pdf and https://www.priv.gc.ca/resource/topic-sujet/pcmltfa-lrpcfat/index_e.asp.

[23] This Act is available at http://laws.justice.gc.ca/PDF/P-31.5.pdf.

[24] This Act is available at http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=c37&Parl=38&Ses=1.

The *Act to amend the Criminal Code (identity theft and related misconduct)*[25], came into force in January 2010 and amended the *Criminal Code* to make the obtaining, selling or possessing of another person's "identity documents", such as a birth certificate or a driver's licence, a criminal offence. The Act also expanded a number of existing Criminal Code provisions dealing with matters such as the theft or forgery of credit cards, mail theft and forging documents (Stoddart, Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act, 2010).

The *Canada's Anti-Spam Law* (CASL)[26], was enacted in 2010 and came into force July 1, 2014. It regulates the sending of commercial e-emails and other forms of communications such as commercial text messages and regulates other harmful practices such as electronic address harvesting and spyware. CASL amended PIPEDA by providing the OPC greater discretion to refuse or discontinue complaints. It also permits the OPC to share information with domestic and international counterparts.

Enacted in December 2014 Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*,[27] also known as the *Protecting Canadians from Online Crime Act*, makes it illegal to distribute intimate images without consent and remove barriers to getting such pictures scrubbed from the internet. The Act also provides the police and other authorities with new tools to preserve records of computer use and electronic emissions, track and trace various online activities of suspects, make it easier to get court approval for electronic surveillance and expand lawful access for a wider range of investigating agencies (Therrien, 2014).

[25] This Act is available at http://laws-lois.justice.gc.ca/PDF/2009_28.pdf.
[26] This Act is available at http://laws-lois.justice.gc.ca/PDF/E-1.6.pdf.
[27] This Act is available at http://laws-lois.justice.gc.ca/PDF/2014_31.pdf.

The *Global Cross Border Enforcement Cooperation Arrangement*[28] will come into effect in October 2015 following its acceptance by 55 of the world's data protection authorities in 2014. It is aimed at fostering more coordinated approaches to addressing cross-border privacy issues. It meets an urgent need for data protection authorities to share confidential information, thereby enabling greater collaboration and more joint investigations. Findings and outcomes of investigations could, in many instances, be issued faster – leading to clearer and stronger messages to organizations and the public (Therrien, Privacy Protection a Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act, 2015).

[28] Details of this Agreement are available at https://www.priv.gc.ca/information/conf2014/arrangement_e.asp.

9. Comparison of Privacy Protection Legislation

Legislation in Canada

While the Privacy Act and PIPEDA are federal legislation, each province and territory also has its own public-sector and/or private-sector legislation (Appendix G). In the provinces of Quebec, Alberta, and British Columbia, which possess legislation comparable to PIPEDA, the provincial legislation supersedes the federal Act. Other provinces, such as Ontario, New Brunswick, and Newfoundland and Labrador, have only passed privacy legislation related to personal health information that is comparable to PIPEDA, in which case they are still regulated by PIPEDA with respect to the private sector, and interprovincial and international transactions.

With the enactment of PIPEDA, Canada met the requirements needed to continue to conduct business with the European Union which established its own privacy legislation in 1998. Canada and the United States signed the *Statement on the Free Flow of Information and Trade in North America* which recognized the importance of the free flow of information between the two countries. Also, the Privacy Act and PIPEDA do not prohibit the Canadian public-sector or private-sector from transferring personal information to the United States or abroad as long as the organizations involved are compliant with the law's requirements.

Legislation in the United States

Unlike Canada, privacy legislation in the United States focusses mainly on protecting an individual's personal privacy from the government (the public-sector) and has limited legislation addressing the private sector (Levin & Nicholson, 2005). Also, instead of one central federal

law for the whole country, the United States has many overlapping laws, including (Levin & Nicholson, 2005):

- *The Privacy Act of 1974*. Like the Canadian Privacy Act, it is a federal omnibus Act which only applies to data collected and processed by the federal government.
- *The Electronic Communications Privacy Act of 1986* ("ECPA"). Requires government officials to request a "Title III" order to receive permission from a federal judge to obtain electronic communications including emails or Internet Service Provider (ISP) logs of personal information;
- *The Privacy Protection Act of 1980*. Protects free speech and First Amendment rights and prohibits the government from searching or seizing materials held by an individual who intends to broadcast it to the public by some form of public communication (such as newspaper, radio broadcast or electronic format) without court authorization/order; and
- *The Right to Financial Privacy Act.* Protects the confidentiality of personal financial records from the government by restricting enforcement agency (like police or military) access to bank records without court authorization/order.

The United States has also enacted legislation to restrict private-sector access to personal information but has been very limited in scope (Levin & Nicholson, 2005):

- *The Fair Credit Reporting Act (1970)* (FCRA). Allows the Federal Trade Commission ("FTC") to regulate credit reporting in the private-sector by requiring Consumer Reporting Agencies to report credit information accurately and fairly, to correct any

errors in their reports, and to include a consumer's dispute of their credit record as part of the report;

- *The Financial Modernization Act (1999).* It is or more commonly known as the *Gramm-Leach-Bliley Act* (GLBA) and is administered by the FTC. It is the first Act to attempt privacy regulation for the financial sector by requiring financial institutions to implement a privacy policy and bring the policy to the attention of their customers, but it fails to provide guidelines or principles that the policy must adhere to;
- *The Identity Theft and Assumption Deterrence Act (1998).* It is also administered by the FTC and provides criminal sanctions for invasion of privacy (the unauthorized use of another person's identity for a felonious purpose), and deter identity theft (this act provides for penalties of up to fifteen years in prison and a maximum fine of $250,000USD); and
- *The Health Insurance Portability and Accountability Act of 1996* (HIPAA). Administered by the Office of Civil Rights in the Department of Health, it provides protection of personal health information that is held by healthcare providers, health plans, and healthcare clearinghouses. It requires that the patient's express consent must be obtained prior to disclosure in the government's attempt to eliminate the denial of employment based on medical information.

During the late 1990's the European Union was in the process of establishing privacy legislation that could impact continued business with the United States. To continue to conduct business with and within the EU, the United States needed to establish legislation which met the requirements of the EU principles. Since the United States felt that personal privacy could be regulated by market forces and constraints, it was not in a position to enact

new legislation. Instead, the United States entered into an agreement with the EU called *The Safe Harbor Agreement* which satisfied the requirements of the EU in relation to privacy and fundamental rights and freedoms of individuals of the EU.

After the events of September 11, 2001, the Department of Justice presented the *USA PATRIOT ACT ("Patriot Act"): Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism),* which was passed nearly unanimously by the Senate and enacted by Congress on October 25, 2001. Envisioned as a means to protect the public from terrorism, this Act gives the government greater access to private information under the guise of intercepting and obstructing terrorism in the United States, with limited judicial oversight. Perhaps realizing this, the pubic reinforced their concern that personal privacy was being further breached as it allowed more information to be analyzed, compiled, and disclosed, possibly without an individual's consent.

Legislation in the European Union

Europe has been the leader in the development of privacy legislation and the privacy of the individual in the digital age. The Council of Europe, which was established following World War II, addressed the issue of personal information as early as 1949. The efforts of the Council lead to the development of the 1980, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*, which provided basic privacy principles and a template for countries without data protection legislation (Levin & Nicholson, 2005).

These principles were adopted by the Organization of Economic Co-Operators and Development (OECD) the following year as the *Guidelines on the Protection of Personal*

Privacy and Transborder Flows of Personal Information (see Appendix A for principles). These guidelines were the first trans-Atlantic privacy protection agreement that would facilitate the flow of information and data internationally but were merely guidelines and not binding on OECD members. Therefore, it was not mandatory to follow these guidelines.

In 1998, the European Union established the Privacy Directive 94/46/EC ("Privacy Directive")[29] to increase privacy protection of data within the European Union based on the principles adopted by the OECD. The principles on which the Privacy Directive was established include personal data collection limitations, the quality of the data collected, purpose specification of the data to be collected and once it has been collected, use limitations of the data, security safeguards for the collection of and storage of data, openness, individual participation and accountability of the data collector. The Privacy Directive also helped to promote trade liberalization and to ensure that a single integrated market was achieved (Levin & Nicholson, 2005).

This was achieved by requiring that all member states enact similar legislation and enforced that the Privacy Directive was no exception. If a member state or country did not enact similar legislation, per Article 25 Principles under Chapter IV – Transfer of Personal Data to Third Countries, the EU could ban data transfers to third countries that do not have established "adequate levels of protection" of data privacy rights. Canada, in response to the Privacy Directive, enacted PIPEDA in order to maintain commerce with the EU. The United States on the other hand did not have adequate legislation in place to meet the requirements of Article 25.

[29] The EU Privacy Directive 94/46/EC can be found at *Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31, accessed by the author at* https://cdt.org/files/privacy/eudirective/EU_Directive_.html, on June 15, 2015.

Under Article 26 Derogations of Chapter IV, which allows the transfer of personal data "if the data controller enters into a contract that will provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals" (Levin & Nicholson, 2005), the United States was allowed to continue to exchange EU data with US companies by entering into a contract with the EU called *The Safe Harbor Agreement*. This agreement represents the EU's acceptance of the US Department of Commerce's privacy principles relating to the US protection of personal data applicable to European citizens for all US companies that register under the Agreement and conducts business within and outside the EU.

Compliance with the Safe Harbor Agreement requires that US companies "self-certify" to the US Department of Commerce or designated government body that they adhere to the privacy principles contained in the Agreement (Levin & Nicholson, 2005). This implies that US companies that want to conduct business with the EU should register under the Safe Harbor Agreement but are not mandated to register. Under Article 26, US companies can satisfy the requirements of the Privacy Directive with a direct contract with the EU or by complying with alternate legislation within the United States that meets the requirements of the Privacy Directive (for example financial institutions, insurance companies or consumer credit companies). The EU on the other hand, has imposed control over all business processing within the EU and internationally, both before and after personal data has been collected, and mandates that all businesses comply with the Privacy Directive.

Perceived Level of Privacy Protection between Canada, the United States and the EU

Based on the review conducted in the previous section, if the three groups were placed on a scale based on the perceived level of privacy protection, United States would be near the bottom (relying on mainly on self-regulating), the European Union (which is far more controlling and limited) would be on the other side, and Canada would be somewhere in the middle. In reality, the main concern should be whether any of this privacy legislation has remained current to changes in technology and still supports and protects personal privacy in global commerce.

Jurisdictional Challenges with Privacy Infringement

Another challenge that is faced when dealing with a privacy infringement is determining who has jurisdiction over the infringement. Domestic jurisdiction presents a challenge when trying to sort out if the infringement or breach falls within federal or provincial jurisdiction. Adding in the potential for an international jurisdiction, and the challenge becomes even more complex. The laws relating to jurisdiction over the internet and server locations were just developed at the beginning of the 21st century when PIPEDA came into force.

The advancements in technology and the growing reliance on said technology to communicate or engage in commerce activities makes it difficult to determine which jurisdiction would have responsibility. This is further compounded by the fact that most interactions occur over the internet which can be accessed from anywhere in the world. A vast amount of information is available in digital form, including personal information and corporate information, and growing exponentially every day that monitoring every interaction is almost impossible. Through the internet an individual, half a world away, could potentially infringe on another

individual's privacy by collecting, using or disclosing personal information that has been taken without her or his consent or even knowledge of its occurrence.

Determining who has legal access to this information, how can this information be gathered legally, which jurisdiction is authorized to access the information and can this information be used locally or globally during an investigation are challenges faced by government agencies like the OPC since the introduction of the internet. Some important considerations to make when determining jurisdiction rights of a privacy infringement might include the location of the internet servers, the location of the originating infringer and the location of any of the organizations that may be involved in the privacy infringement (Barabara McIssac, 2007).

For example, if the individual who is responsible for the infringement is physically located in Canada, or the servers are in Canada, then it the investigation may have to comply with the Canadian privacy legislation. But this gets more complex if the individual responsible for the infringement is located somewhere else on the globe but the person who they infringed upon was a Canadian individual. What determines which jurisdiction would apply? Could an analysis of the activities carried out and the contacts the infringer may have with residents or organization within Canada be used to determine jurisdiction? These are questions faced by privacy commissioners and other enforcement authorities globally.

An example of Canada's OPC's involvement in a cross-border infringement occurred in 2008 (Stoddart, Annual Report to Parliament 2008: Report on the Personal Information Protection and Electronic Documents Act, 2009) with the *Accusearch, Inc., d/b/a Abika.com, and X v. U.S Federal Trade Commission* case. This case involved the transborder flow of personal information between Canada and the U.S. Accusearch Inc. ("Accusearch"), a U. S. based website search service, was involved in selling consumer telephone records to third parties without authorization or consent from the

individuals impacted (defined as conducting business as a data-broker). Since the OPC had already been involved in investigating complaints filed against Accusearch between 2005 and 2007, it was granted the ability to file a brief during the appeal proceedings being conducted by the U.S. Tenth Circuit Court of Appeals (Stoddart, Annual Report to Parliament 2008: Report on the Personal Information Protection and Electronic Documents Act, 2009). The OPC felt that the Court's decision in this case might directly impact the privacy rights of Canadians and possibly any Canadian organization that conducts business with the U.S (Stoddart, Annual Report to Parliament 2008: Report on the Personal Information Protection and Electronic Documents Act, 2009). The OPC recognized that "recognition that Accusearch's practices and the resulting harms are illegal under the U.S. law would support international cooperation between Canadian and United States regulators by enhancing the consistency in approach between the two jurisdictions (Stoddart, Annual Report to Parliament 2008: Report on the Personal Information Protection and Electronic Documents Act, 2009)."

This growing need to coordinate and nationalize the control and regulation regarding the collection, use, storage, and disposal of personal information has resulted in the development of several international organizations. These organizations have been developed and established in order to monitor, assist with, and manage best practices with regards to privacy protection (a listing of said agencies, their mission and corresponding website has been provided in Appendix H).

Canada's Privacy Commissioners have been instrumental in assisting with the development of these organizations and sharing experiences and best practices with other countries as they adopt privacy protection legislation of their own. Jurisdictional challenges will continue to be a global priority it is recommended that IFAs remain abreast of the changing landscape of privacy legislation.

10. Conclusion

With the advancement of technology and the increased reliance on the internet for conducting work, engaging with friends, purchasing items or playing games, it has become commonplace to volunteer personal information without fully understanding the implications of how that information may be used.

The privacy legislation currently in place in Canada was enacted long before the use of technology became a way of life. The importance of protecting an individual's privacy from infringement was top priority and having the foresight to forecast where technology could advance and how it might impact an individual's privacy may have been beyond consideration at the time.

Despite rapid changes in technology and to the nature in how we communicate and do business around the globe, legislation relating to the privacy and security of personal information has remained almost stagnant or has been slow to reform. As a result, instances of security breaches and invasions of privacy have become more prevalent and will continue to grow as the digital landscape changes over time.

At the time this report was written, privacy legislation has had little impact in IFA engagements or investigations. This may result from the way that an IFA is hired. Since a significant portion of IFA work is obtained through a lawyer, where consent to gather information has already been granted by their clients, the potential of privacy infringement that is directly related to IFA activities may be minimal. That said, staying abreast of current privacy legislation and its reforms, will allow IFAs to act as consultants and adviser to their clients. Reviewing the current practices of a client, and discussing the weaknesses or potential

areas of non-compliance related to the privacy legislation could lead to further involvement and engagements in the event that a breach does occur.

Appendices

Appendix A – OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data – Part Two, Sections 7 to 14

Appendix B – The National Standard of Canada *Model Code for the Protection of Personal Information, CAN/CSA-Q830-96* – 10 Privacy Principles

Appendix C – Interview Questions – DIFA Program Advanced Topics Research Paper

Appendix D – Office of the Privacy Commissioner’s 10 “Quick Fix” Recommendations

Appendix E – Response to the Privacy Commissioner’s 10 “Quick Fix” Recommendations by the House of Commons Access to Information, Privacy and Ethics Committee

Appendix F – 25 Recommendations of Reform of PIPEDA Pursuant to the House of Commons Standing Committee on Access to Information, Privacy and Ethics’ Report, *Statutory Review of the Personal Information Protection and Electronic Documents Act*

Appendix G – Complete List of Provincial and Territorial Legislation Related to Privacy

Appendix H – International Organizations that assist with or manage best practices in privacy protection of which Canada is a member

Appendix A

OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data – Part Two, Sections 7 to 14[30] (Holmes N. , 2008)

Basic Principles of National Application

7. *Collection Limitation Principle:* There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
8. *Data Quality Principle:* Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
9. *Purpose Specification Principle:* The purposes for which personal data are collected should be specified not later than the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
10. *Use Limitation Principle:* Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except i) with the consent of the data subject or ii) by the authority of law.
11. *Security Safeguards Principle:* Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
12. *Openness Principle:* There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be

[30] The complete OECD Guidelines are available on the OECD website at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

13. *Individual Participation Principle:* An individual should have the right:
    a. To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. To have communicated to him, data relating to him i) within a reasonable time, ii) at a charge, if any, that is not excessive, iii) in a reasonable manner, and iv) in a form that is readily intelligible to him;
    c. To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
    d. To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
14. *Accountability Principle:* A data controller should be accountable for complying with measures which give effect to the principles stated above.

These guidelines were updated in 2013, over 30 years after the initial release, following an extensive review which determined that the landscape where personal data is collected and used has changed significantly from 30 years ago.

These changes to the landscape include (The OECD Privacy Framework 2013: Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines"), 2013):

- The volume of personal data being collected, used and stored;
- The range of analytics involving personal data, providing insights into individual and group trends, movements, interests, and activities;

- The value of the societal and economic benefits enabled by new technologies and responsible uses of personal data;
- The extent of threats to privacy;
- The number and variety of actors capable of either putting privacy at risk or protecting privacy;
- The frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate; and
- The global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

The OECD member countries include (as of 2013): Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

Appendix B

The National Standard of Canada *Model Code for the Protection of Personal Information, CAN/CSA-Q830-96* – 10 Privacy Principles

(Personal Information Protection and Electronic Documents Act, 2014)[31]

1. *Accountability:* An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. *Identifying Purposes:* The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. *Consent:* The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where appropriate.
4. *Limiting Collection:* The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. *Limiting Use, Disclosure and Retention:* Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.
6. *Accuracy:* Personal information shall be as accurate, complete and up-to-date as necessary for the purpose for which it is to be used.
7. *Safeguards:* Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

[31] Please refer to Schedule 1 of PIPEDA to view the complete description and requirements of all 10 privacy principles.

8. *Openness:* An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. *Individual Access:* Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. *Challenging Compliance:* An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Appendix C

Interview Questions – DIFA Program Advanced Topics Research Paper

1. Please provide you full name:
2. Please provide your current title and name of the organization for which you work or where you had the most relevant experience:
3. Please provide a brief summary of your credentials and work experience:
4. The following is a list of privacy protection legislation ("privacy legislation") in Canada. Please indicate which legislation applies to your field of work or that you have encountered during your career:

   Federal Legislation:

   a. Privacy Act
   b. Personal Information Protection and Electronic Documents Act

   Provincial Legislation:

   a. Alberta's Personal Information Protection Act
   b. British Columbia's Personal Information Protection Act.
   c. Quebec's An Act Respecting the Protection of Personal Information in the Private Sector
   d. Ontario's Personal Health Information Protection Act.
   e. Any other Ontario legislation?
   f. New Brunswick's Personal Health Information Privacy and Access Act
   g. Newfoundland and Labrador's Personal Health Information Act
5. Please provide a brief description of how you have incorporated privacy legislation into your daily work routine?

6. In your experience, does a breach of privacy legislation occur more often in the public sector or in the private sector? Please explain.
7. Has there been a time/have there been times when privacy legislation, provincially or federally, has impacted your work? If so, can you describe the incident or summarize the incidents and explain how you how dealt with such an event/events.
8. How has privacy legislation limited the engagements you have accepted or the work you conduct/conducted for your current or previous roles?
9. How have you addressed previous situations where the personal information made available to you has limited the investigation you were conducting? What steps did you take/could you take to address such a limitation?
10. Consider a situation where you were provided with more personal information than required to conduct your work, whether the information was for the individual involved or for individuals who were not directly involved:
    a. What were the potential consequences of receiving this additional information?
    b. What did you see as your professional and ethical obligations when faced with this situation?
    c. If the information received infringed on privacy legislation but you knew using it is critical to the outcome of the investigation, how did you or would you have treated such a situation?
11. If you are required to work with law enforcement or legal counsel:
    a. Has privacy protection legislation limited the information you were able to receive;
    b. Has privacy legislation limited the investigation you conducted;

c. If possible, please provide an example of a time where you experienced and/or overcame such a situation;

d. If your answers to 11(a) and 11(b) were "no", please advise of how you would address such issues if presented to you.

12. If you are a lawyer involved in a case relating to privacy legislation infringement:

    a. In what circumstances could you envisage requiring the services of an investigative and forensic accountant (IFA);

    b. At what stage of the engagement would you require an IFA and

    c. What steps must you take to ensure you do not provide more information than required/permitted to the IFA?

13. In your opinion, has lawyer/client privilege affected the impact of privacy legislation in an engagement? If possible, please provide the context of how such a situation occurred.

14. In what ways could privacy legislation impact how an investigation is conducted? Please consider the various stages of an investigation

15. Have you been directly involved in a file or case that related to a breach in privacy legislation? Explain, to the extent you are able to:

    a. What the breach entailed;

    b. How you conducted the investigation or assisted with the investigation of this file or case; and

    c. What the ultimate outcome of the matter was.

16. Where, in your opinion, is/are the largest risk area(s) for infringement on privacy legislation when conducting investigations? Are there other areas of an investigation that could result in privacy legislation infringement? Please explain
17. How could the privacy legislation which affects your work be improved?
18. Knowing that access to certain information can critically impact an investigation, if you had an opportunity to change the privacy legislation in Canada:
    a. Which would you consider more important: having access to the necessary information for an investigation, or an individual's right to keep that information private?
    b. Who should make that decision – the government, society as a whole, or the individual, or a trier of fact?
19. Are you aware of any changes made in other jurisdictions regarding privacy legislation that you believe should be implemented in Ontario and or Canada? Briefly explain. (These changes can include international legislation with which you are familiar)

* * *

Please accept my thanks and appreciation for taking the time to answer the above questions. This experience has assisted with: the advancement of my education; my understanding of the impacts of privacy legislation in Canada; and my research paper for the Diploma in Forensic Accounting (DIFA) program at the University of Toronto.

Sincerely,

Miranda Lahtinen, CPA, CMA, CPM

Appendix D

Office of the Privacy Commissioner's 10 "Quick Fix" Recommendations (Stoddart, 2008)

Recommendation #1: Create a legislative "necessity test" which would require government institutions to demonstrate the needs for the personal information they collect.

Recommendation #2: Broaden the grounds for which an application for Court review under section 41 of the Privacy Act may be made to include the full array of privacy rights and protections under the Privacy Act and give the Federal Court the power to award damages against offending institutions.

Recommendation #3: Enshrine a requirement for head of government institutions subject to the Privacy Act to assess the privacy impact of programs or systems prior to their implementation and to publicly report assessment results.

Recommendation #4: Amend the Privacy Act to provide the Office of the Privacy Commissioner of Canada with a clear public education mandate.

Recommendation #5: Provide greater discretion for the Office of the Privacy Commissioner of Canada to report publicly on the privacy management practices of government institutions.

Recommendation #6: Provide discretion for the Privacy Commissioner to refuse and/or discontinue complaints the investigation of which would serve little or no useful purpose, and would not be in the public interest to pursue.

Recommendation #7: Amend the Privacy Act to align it with the PIPEDA by eliminating the restriction that the Privacy Act applies to recorded information only.

Recommendation #8: Strengthen the annual reporting requirements of government departments and agencies under section 72 of the Privacy Act, by requiring these institutions to report to Parliament on a broader spectrum of privacy-related activities.

Recommendation #9: Introduction of a provision requiring an ongoing five year Parliamentary review of the Privacy Act.

Recommendation #10: Strengthen the provisions governing the disclosure of personal information by the Canadian government to foreign states.

In May of 2009, the Privacy Commissioner recommended 2 additional "quick fixes" that should be included with her list of 10[32]. These included:

Recommendation #11: Introduce a provision for proper security safeguards requiring the protection of personal information.

Recommendation #12: Enshrine Treasury Board's breach notification guidelines into legislation.

[32] Privacy Commissioner of Canada, *Privacy Act Reform Recommendations*, The Office of the Privacy Commissioner, May 11, 2009, http://www.priv.gc.ca

Appendix E

Response to the Privacy Commissioner's 10 "Quick Fix" Recommendations by the House of Commons Access to Information, Privacy and Ethics Committee (Szabo, 2009)

Recommendation #1 Response: The Committee discussed whether section 4 of the Privacy Act is robust enough in its current form to give full effect to the rights underpinning the Act, but there were varying opinions on this issue. The Minister may wish to give it further study and consideration.

Recommendation #2 Response: The Committee discussed section 41 and whether access to the courts under it should be broadened by means of proposing amendments. It also discussed the relationship between this recommendation and recommendation #6, the proposal to give the Commissioner the discretion to refuse to investigate frivolous or vexatious complaints. The Committee recognizes the varying viewpoints of all who testified on this issue, and would suggest that the Minister give it further study and consideration. Discussion between the Minister and the Commissioner may help to determine whether these proposals should move forward, or be modified.

Recommendation #3 Response: The Committee discussed this recommendation and while it is sympathetic to the concerns raised by the Commissioner, does not consider this proposal to be a top priority for reform at this time.

Recommendation #4 Response: The Committee supports this recommendation and suggests that the Minister consider amending the Privacy Act accordingly.

Recommendation #5 Response: The Committee would support the proposal that more frequent latitude be given to the Commissioner to report to Parliament, subsequent to which her findings

could be discussed publicly. To the extent that the proposal would require legislative amendment to allow disclosure other than provided for under the Officer of Parliament model where reports must be tabled in Parliament first, the Committee would have concerns. The Committee also expressed concern about what would constitute a "matter of public interest" and how this would be determined.

Recommendation #6 Response: The Committee discussed this recommendation, and noted that the Minister's testimony had linked it with the second recommendation about concerning broadening the Court's powers with respect to the Privacy Act. The Committee recognizes the varying viewpoints of all who testified on this issue, and would suggest that the Minister give further study and consideration. Discussion between the Minister and the Commissioner may help to determine whether these proposals should move forward, or be modified.

Recommendation #7 Response: The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.

Recommendation #8 Response: The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.

Recommendation #9 Response: The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.

Recommendation #10 Response: The Committee is generally supportive of the Commissioner's recommendation, but there are some differing views on whether an exemption would need to be added to such an amendment for law enforcement purposes. The Committee suggests that the Minister consider an amendment and the form it would take.

Recommendation #11 Response: The Committee supports this recommendation and suggests that the Minister consider amending the Act accordingly.

Recommendation #12 Response: The Committee takes no position on this recommendation at the current time and agrees that it requires further study.

Appendix F

25 Recommendations of Reform of PIPEDA Pursuant to the House of Commons Standing Committee on Access to Information, Privacy and Ethics' Report, *Statutory Review of the Personal Information Protection and Electronic Documents Act*

Recommendation #1: The Committee recommends that a definition of "business contact information" be added to PIPEDA, and that the definition and relevant restrictive provision found in the Alberta Personal Information Protection Act be considered for this purpose.

Recommendation #2: The Committee recommends that PIPEDA be amended to include a definition of "work product" that is explicitly recognized as not constituting personal information for the purposes of the Act. In formulating this definition, reference should be added to the definition of "work product information" in the British Columbia Personal Information Protection Act, the definition proposed to this Committee by IMS Canada, and the approach taken to professional information in Quebec's An Act Respecting the Protection of Personal Information in the Private Sector.

Recommendation #3: The Committee recommends that a definition of "destruction" that would provide guidance to organizations on how to properly destroy both paper records and electronic media be added to PIPEDA.

Recommendation #4: The Committee recommends that PIPEDA be amended to clarify the form and adequacy of consent required by it, distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia Personal Information Protection Acts.

Recommendation #5: The Committee recommends that the Quebec, Alberta and British Columbia private sector data protection legislation be considered for the purposes of

developing and incorporating into PIPEDA an amendment to address the unique context experienced by federally regulated employers and employees.

Recommendation #6: The Committee recommends that PIPEDA be amended to replace the "investigative bodies" designation process with a definition of "investigation" similar to that found in the Alberta and British Columbia Personal Information Protection Acts thereby allowing for the collection, use and disclosure of personal information without consent for that purpose.

Recommendation #7: The Committee recommends that PIPEDA be amended to include a provision permitting organizations to collect, use and disclose personal information without consent, for the purposes of a business transaction. This amendment should be modeled on the Alberta Personal Information Protection Act in conjunction with enhancements recommended by the Privacy Commissioner of Canada.

Recommendation #8: The Committee recommends that an amendment to PIPEDA be considered to address the issue of principal-agent relationships. Reference to section 12(2) of the British Columbia Personal Information Protection Act should be made with respect to such an amendment.

Recommendation #9: The Committee recommends that PIPEDA be amended to create an exception to the consent requirement for information legally available to a party to a legal proceeding, in a manner similar to the provisions of the Alberta and British Columbia Personal Information Protection Acts.

Recommendation #10: The Committee recommends that the government consult with the Privacy Commissioner of Canada with respect to determining whether there is a need for further amendments to PIPEDA to address the issue of witness statements and the rights of persons whose personal information is contained therein.

Recommendation #11: The Committee recommends that PIPEDA be amended to add other individual, family or public interest exemptions in order to harmonize its approach with that taken by the Quebec, Alberta and British Columbia private sector data protection Acts.

Recommendation #12: The Committee recommends that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(c.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: "For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization shall disclose personal information without the knowledge or consent of the individual but only if the disclosure is […]"

Recommendation #13: The Committee recommends that the term "government institution" in sections 7(3)(c.1) and (d) be clarified in PIPEDA to specify whether it is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities.

Recommendation #14: The Committee recommends the removal of section 7(1)(e) from PIPEDA.

Recommendation #15: The Committee recommends that the government examine the issue of consent by minors with respect to the collection, use and disclosure of their personal information in a commercial context with a view to amendments to PIPEDA in this regard.

Recommendation #16: The Committee recommends that no amendments be made to PIPEDA with respect to transborder flows of personal information.

Recommendation #17: The Committee recommends that the government consult with members of the health care sector, as well as the Privacy Commissioner of Canada, to determine the extent to which elements contained in the PIPEDA Awareness Raising Tools document may be set out in legislative form.

Recommendation #18: The Committee recommends that the Federal Privacy Commissioner not be granted order-making powers at this time.

Recommendation #19: The Committee recommends that no amendment be made to section 20(2) of PIPEDA with respect to the Privacy Commissioner's discretionary power to publicly name organizations in the public interest.

Recommendation #20: The Committee recommends that the Federal Privacy Commissioner be granted the authority under PIPEDA to share personal information and cooperate in investigations of mutual interest with provincial counterparts that do not have substantially similar private sector legislation, as well as international data protection authorities.

Recommendation #21: The Committee recommends that any extra-jurisdictional information sharing, particularly to the United States, be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared.

Recommendation #22: The Committee recommends that PIPEDA be amended to permit the Privacy Commissioner to apply to the Federal Court for an expedited review of a claim of solicitor-client privilege in respect of the denial of access to personal information

(section 9(3)(a)) where the Commissioner has sought, and been denied, production of the information in the course of an investigation.

Recommendation #23: The Committee recommends that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner.

Recommendation #24: The Committee recommends that upon being notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner.

Recommendation #25: The Committee recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identity theft and fraud.

Appendix G

Complete List of Provincial and Territorial Legislation Related to Privacy[33]

Nova Scotia: Freedom of Information and Protection of Privacy Act, 1993, Part XX of the Municipal Government Act, 1998, Personal Information International Disclosure Protection Act, 2006 and Personal Health Information Act, 2013.

New Brunswick: Right to Information and Protection of Privacy Act, 2009 and Personal Health Information Privacy and Access Act, 2009.

Prince Edward Island: Freedom of Information and Protection of Privacy Act, 1988.

Newfoundland and Labrador: Access to Information and Protection of Privacy Act, 2002 and Personal Health Information Act, 2008.

Québec: Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, 1982, Act Respecting the Protection of Personal Information in the Private Sector, 1993 and An Act to amend the Act respecting health services and social services, the Health Insurance Act and the Act respecting the Régie de l'assurance maladie du Québec, 2008.

Ontario: Freedom of Information and Protection of Privacy Act, 1990, Municipal Freedom of Information and Protection of Privacy Act, 1990 and Personal Health Information Protection Act, 2004.

Manitoba: Freedom of Information and Protection of Privacy Act, 1997 and Personal Health Information Act, 1997.

[33] Information gathered from the Privacy Commissioner of Canada website: https://www.priv.gc.ca/resource/prov/index_e.asp.

Nunavut: In 2000, Nunavut adopted the laws in place in the Northwest Territories until the province is able to establish its own legislation. Therefore, Access to Information and Protection of Privacy Act, 1994.

Northwest Territories: Access to Information and Protection of Privacy Act, 1994.

Saskatchewan: Freedom of Information and Protection of Privacy Act, 1990, Local Freedom of Information and Protection of Privacy Act, 1990 and Health Information Protection Act, 2003.

Alberta: Freedom of Information and Protection of Privacy Act, 2000, Personal Information Protection Act, 2003 and Health Information Act, 2010.

British Columbia: Freedom of Information and Protection of Privacy Act, 1996, Personal Information Protection Act, 2003 and E-Health (Personal Health Information Access and Protection of Privacy) Act, 2008.

Yukon: Access to Information and Protection of Privacy Act, 1984.

Appendix H

International Organizations that assist with or manage best practices in privacy protection of which Canada is a member[34]

Asia Pacific Economic Cooperation ("APEC"): APEC is the premier Asia-Pacific economic forum. The primary goal is to support sustainable economic growth and prosperity in the Asia-Pacific region. *Mission:* APEC is united in their drive to build a dynamic and harmonious Asia-Pacific community by championing free and open trade and investment, promoting and accelerating regional economic integration, encouraging economic and technical cooperation, enhancing human security, and facilitating a favorable and sustainable business environment. APEC's initiatives turn policy goals into concrete results and agreements into tangible benefits. *Website:* http://www.apec.org/

Asia Pacific Privacy Authorities ("APPA"): Was formed in 1992 and is the principal forum for privacy authorities in the Asia Pacific Region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. *Website:* http://www.appaforum.org/

Commission for the Control of INTERPOL's Files: INTERPOL is the world's largest international police organization, with 190 member countries. The role of INTERPOL is to enable police around the world to work together to make the world a safer place. The Commission for the Control of INTERPOL's Files (CCF) is an independent monitoring body. It operates in line with a number of official rules and documents and has three main functions:

- Monitoring the application of the Organization's data protection rules to personal data processed by INTERPOL;

[34] All information has been gathered from each website provided.

- Advising the Organization with regard to any operations or projects concerning the processing of personal information; and
- Processing requests for access to INTERPOL's files.

Website: http://www.interpol.int/Commission-for-the-Control-of-INTERPOL's-Files

Council of Europe: The Council of Europe advocates freedom of expression and of the media, freedom of assembly, equality, and the protection of minorities. Duties of the Council of Europe include:

- Launching awareness campaigns on issues such as child protection and online hate speech;
- Helping member states to fight corruption and terrorism;
- Undertaking necessary judicial reform; and
- Offering legal advice to countries throughout the world.

Website: http://www.coe.int/en/

European Commission: The European Commission represents the interests of the EU as a whole. It proposes new legislation to the European Parliament and the Council of the European Union, and it ensures that EU law is correctly applied by member countries.

Website: http://ec.europa.eu/

Global Privacy Enforcement Network ("GPEN"): *Mission*: To connect privacy enforcement authorities from around the world to promote and support cooperation in cross-border enforcement of laws protecting privacy. It primarily seeks to promote cooperation by:

- Exchanging information about relevant issues, trends and experiences;

- Encouraging training opportunities and sharing of enforcement know-how, expertise and good practice;
- Promoting dialogue with organizations having a role in privacy enforcement;
- Creating, maintaining and supporting processes or mechanisms useful to bilateral or multilateral cooperation; and
- Undertaking or supporting specific activities.

Website: https://www.privacyenforcement.net/

International Organization for Standardization ("ISO"): Is an independent, non-governmental membership organization of 163 countries and the world's largest developer of voluntary international standards. *Website:* http://www.iso.org/

Organisation for Economic Co-Operation and Development ("OECD"): *Mission:* To promote policies that will improve the economic and social well-being of people around the world. It is focused on helping governments around the world to:

- Restore confidence in markets and the institutions that make them function;
- Re-establish healthy public finances as a basis for future sustainable economic growth;
- Foster and support new sources of growth through innovation, environmentally friendly 'green growth' strategies and the development of emerging economies; and
- Ensure that people of all ages can develop the skills to work productively and satisfyingly in the jobs of tomorrow.

Website: http://www.oecd.org/

United Nations Organization ("UN"): The UN is an international organization founded in 1945. The mission and work of the UN are guided by the purposes and principles contained in its founding Charter. The UN takes action relating to issues confronting humanity including (but not limited to) peace, security, human rights, terrorism and governance. The UN also provides a forum for its members to express their views and by doing so has provided a mechanism for governments to find areas of agreement and solve problems together.

Website: http://www.un.org/en/

Bibliography

Accounting, A. f. (2006). *Standard Practices for Investigative and Forensic Accounting Engagements.* Toronto: Chartered Accountants of Canada.

Barabara McIssac, Q. R. (2007). *The Law of Privacy in Canada: 2007 Student Edition.* Thomson Canada Limited and Carswell.

Bernal-Castillero, M. (2013, October 1). *Background Paper: Canada's Federal Privacy Laws.* Retrieved April 27, 2015, from Library of Parliament: http://www.parl.gc.ca

Cameron, A. (2015, June 21). Lawyer. (M. Lahtinen, Interviewer)

CPA Ontario Member's Handbook. (2015, March 20). Retrieved June 20, 2015, from Chartered Professional Accountants of Ontario: http://www.cpaontario.ca

Froese, K. (2015, June 18). Senior Managaing Director. (M. Lahtinen, Interviewer)

Gratton, E. (2013). *Understanding Personal Information: Managing Privacy Risks.* LexisNexis Canada Inc.

Holmes, N. (2000, December 11). *Privacy in a High-Tech World.* Retrieved April 25, 2015, from Library of Parliament: http://intraparl/36/map_sv_lib-e.htm

Holmes, N. (2008, September 25). *Canada's Fereal Privacy Laws.* Retrieved April 25, 2015, from Library of Parliament: http://www.parl.gc.ca

Levin, A., & Nicholson, M. J. (2005, February 2). Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground. *University of Ottawa Law & Technology Journal*, pp. 357-395.

Lithwick, D. (2014, June 11). *Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act.* Retrieved April 27, 2015, from Library of Parliament: http://www.parl.gc.on

MacGregor, S. (2015, June 18). Partner, Forensic Services. (M. Lahtinen, Interviewer)

Marleau, R. (2003, September). *Annual Report to Parliament 2002-2003.* Retrieved June 1, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Morley, P. (2015, June 10). Senior Forensic Accountant. (M. Lahtinen, Interviewer)

Personal Information Protection and Electronic Documents Act. (2014, July 1). Retrieved April 27, 2015, from Minister of Justice: http://www.laws-lois.justice.gc.ca

Privacy Act. (2015, February 26). Retrieved April 27, 2015, from Minister of Justice: http://laws-lois.justice.gc.ca

Radwanski, G. (2001, December). *Annual Report to Parliament 2000-2001.* Retrieved June 1, 2015, from Office of the Privacy Comissioner of Canada: http://www.priv.gc.ca

Rufus, R. J. (2014). *Forensic Accounting.* New Jersey, USA: Pearson Education, Inc. - Prentice Hall.

Stoddart, J. (2006, May). *Annual Report to Parliament 2005: Report on the Personal Information Protection and Electronic Documents Act.* Retrieved June 1, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Stoddart, J. (2006, June). *Annual Reports to Parliament 2005-2006: Report on the Privacy Act.* Retrieved June 1, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Stoddart, J. (2008, June). *Annual Report to Parliament 2007: Report on the Personal Information Protection and Electronic Documents Act.* Retrieved June 1, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Stoddart, J. (2008, December). *Annual Reports to Parliament 2007-2008: Report on the Privacy Act.* Retrieved June 1, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Stoddart, J. (2008, April 29). *Proposed Immediate Changes to the Privacy Act: Appearance before the Standing Committee on Access to Information, Privacy and Ethics.* Retrieved April 25, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Stoddart, J. (2009, August). *Annual Report to Parliament 2008: Report on the Personal Information Protection and Electronic Documents Act.* Retrieved June 1, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Stoddart, J. (2010, June). *Annual Report to Parliament 2009: Report on the Personal Information Protection and Electronic Documents Act.* Retrieved June 15, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Szabo, P. (2009, June). *The Privacy Act: First Steps Towards Renewal.* Retrieved April 27, 2015, from Library of Parliament: http://www.parl.gc.ca

The OECD Privacy Framework 2013: Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines"). (2013, July 11). Retrieved June 15, 2015, from The Organisation For Economic Co-operation and Development: http://www.oecd.org

Therrien, D. (2014, October). *Transparency and Privacy in the Digital Age: Annual Report to Parliament 2013-14: Report on the Privacy Act.* Retrieved June 15, 2015, from Office of the Commissioner of Canada: https://www.priv.gc.ca

Therrien, D. (2015, June). *Privacy Protection a Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act.* Retrieved June 15, 2015, from Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca

Therrien, D. (2015, June). *Privacy Protection: A Global Affair, Annual Report to Parliament 2014: Report on the Personal Information Protection and Electronic Documents Act.* Retrieved June 12, 2015, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca

Tim, T. (2015, June 10). Detective Constable, OPP. (M. Lahtinen, Interviewer)

Wappel, T. (2007, May). *Statutory Revies of the Personal Information Protection and Electronic Documents Act (PIPEDA): Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics.* Retrieved April 27, 2015, from Library of Parliament: http://www.parl.gc.ca

Articles

Adobe Plans to Settle Breach Lawsuit, retrieved June 20, 2015, from Bank Info Security: http://www.bankinfosecurity.com/adobe-plans-to-settle-breach-lawsuit-a-8174/op-1.

Canada Revenue Agency privacy breach leaks prominent Canadians' tax details, retrieved June 20, 2015, from CBC Canada: http://www.cbc.ca/news/politics/canada-revenue-agency-privacy-breach-leaks-prominent-canadians-tax-details-1.2849336.

Chinese breach data of 4 million federal workers, retrieved June 20, 2015, from Washington Post: http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

Cyberattack Exposes I.R.S. Tax Returns, retrieved June 20, 2015, from New York Times: http://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html?_r=0.

EU Privacy Directive 94/46/EC, retrieved June 15, 2015, from Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31, https://cdt.org/files/privacy/eudirective/EU_Directive_.html.

Highlights of the USA PATRIOT Act, retrieved June 7, 2015, from U.S. Department of Justice: http://www.justice.gov/archive/ll/highlights.htm.

Medical pot users seek class action against Health Canada, retrieved June 20, 2015, from The Chronicle Herald: http://thechronicleherald.ca/metro/1292449-medical-pot-users-seek-class-action-against-health-canada.

New Visual Icons Introduced to help People Easily Understand Online Privacy Policies, retrieved June 20, 2015, from Market Watch: http://www.marketwatch.com/story/new-visual-icons-introduced-to-help-people-easily-understand-online-privacy-policies-2014-06-23.

Open Profiling Standard, retrieved June 23, 2015, from Arts & Farces internet, Wikis: http://www.farces.com/wikis/ie/chap-07/open-profiling-standard/.

Privacy Act Reform Recommendations, retrieved June 5, 2015, from The Office of the Privacy Commissioner: http://www.priv.gc.ca.

Samsung Galaxy: What you need to know about reported security risk, retrieved June 20, 2015, from ABC News: http://abcnews.go.com/Technology/samsung-galaxy-reported-security-risk/story?id=31825944.

Additional Resources

Applying Canadian Privacy Law to Transborder Flows of Personal Information from Canada to the United States: A Clarification (September 2008). Retrieved June 15, 2015, from Industry Canada, available at https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf/$file/Clarification%20Statement%20-%20Transborder%20flow%20of%20personal%20information.pdf;

Global Data Privacy Directory (July 2014). Retrieved June 5, 2015, from Norton Rose Fulbright LLP, available at http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf;

International Data Protection and Privacy Law (August 2009). Retrieved June 5, 2015, from White and Case LLP, available at http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf;

The Safe Harbor: Privacy in the United States (May 2003). Retrieved June 5, 2015, from Fasken Martineau DuMoulin LLP, available at http://www.fasken.com/files/Publication/00cdee35-5943-4735-98b2-ca6ba483bcda/Presentation/PublicationAttachment/9ec7ac7a-dc59-4f82-880d-94deaa9144e9/SAFEHARBOUR.PDF;

Directive on Privacy Practices, retrieved June 20, 2015, from the Treasury Board of Canada Secretariat: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309

Global Cross Border Enforcement Cooperation Arrangement, retrieved June 20, 2015, from the Office of the Privacy Commissioner: https://www.priv.gc.ca/information/conf2014/arrangement_e.asp.

OECD Privacy Guidelines, retrieved June 17, 2015, from OECD: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Note: All Office of the Privacy Commissioner annual reports have been reviewed during the research of this paper but may not have been directly referenced in the body of the report. The reports are available at https://www.priv.gc.ca/information/02_05_b_e.asp.