School of Computing

Blekinge Institute of Technology

Security of Personal Information In Cloud Computing

Identifying and mitigating against risks to privacy in the deployment of Enterprise Systems Applications on the Software as a Service platform.

By: Paul Denys

Thesis submitted for completion of Master of Science (60 credits)

Main field of study: Computer Science

Specialization: Informatics

School of Computing

Blekinge Institute of Technology

SE-371 79 Karlskrona

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science (60 credits) in Computer Science with specialization in Informatics. The thesis is equivalent to 10 weeks of full time studies.

Contact Information:

Author: Paul Denys

E-mail: pldenys@gmail.com

University advisor: Hans Kyhlbäck, senior lecturer, PhD

E-mail: hans.kyhlback@bth.se

School of Computing
Blekinge Institute of Technology
SE-371 41 Karlskrona

Internet : www.bth.se/com
Phone : +46 455 38 50 00
Fax : + 46 455 38 50 57

ACKNOWLEDGEMENTS

I would like to acknowledge several individuals for their assistance and support during my research without whom it would have been harder to write this thesis.

First and foremost, I wish to thank my supervisor Hans Kyhlbäck from Blekinge Institute of Technology for his support, criticism and direction which resulted in a much more consistent thesis project. Thank you for your criticism and taking the time to answer questions and reviewing the thesis at several stages during the process.

I would also like to thank Harpreet Dhillon, Eugene McGarrigle and Stephen Parr who took the time to review the thesis, offer their comments and suggestions for improving it.

I would also like to thank my family for their support and understanding during the research process, which took a lot of time and resulted in less time devoted to their needs.

Paul Denys
Calgary, 12 October 2012

ABSTRACT

The emergence and subsequent growth of Cloud computing has brought with it a great deal of change in the manner in which the world undertakes to compute and store information. This new technology has brought with it immense possibilities as far as processing of information and the pooling of resources is concerned. This potential has also been noticed by the public sector, as Governments all over the world have undertaken to introduce what has come to be known as e-Government, the provisioning of Government services and communications via Web based applications, rather than the traditional means of in person contact and paper based collection of personal information. While the move to Web based Government has been occurring for the last 20 or so years, a new development in this area is the introduction of Cloud computing and Cloud-based computing platforms, most notably Software-as-a-Service (*SaaS*) in the provisioning of these services. The computing and efficiency potential of this technology cannot be disputed, yet it's important to recognize that taking advantage of this computing power does come at a price. That price being significant threats to personal privacy and security of personally identifiable information. This thesis will make it easier for government agencies to make informed decisions about whether or not to migrate data and applications into the cloud. The identification and analysis of potential risks to data security and personal information has drawn together key information from a multitude of both academic and industry sources to make such a decision plausible.

Keywords: privacy, cloud computing, personal information, security.

TABLE OF CONTENTS

INTRODUCTION

The emergence of new technologies in the last decade has opened up a world of new opportunities to enable cloud-based computing which gave rise to mobile computing meaning computing that is not tied to a specified location. It has enabled solutions that are making it possible to provide extensive and flexible computing needs without the necessity of purchasing software or hardware or of employing an army of Information Technology (IT) professionals to: maintain, upgrade and secure it.

These solutions are very competitive to the traditional approach to computing because they have a tendency to be much cheaper and offer greater flexibility for users. While these developments have definitely changed the way that Corporations and Governments approach their computing needs, it has also exposed some definite shortcomings; most notably in the area of data security. It is the threat to the security of the data which has a direct and profound impact on the protection of personal information and privacy of identifiable individuals. This thesis will focus on the Software-as-a-Service (*SaaS*) platform in the provisioning of Cloud Computing services for Government, also referred to as e-Government. It will examine the risks to the security of personal information in the application of Enterprise Application Software (EAS) in the Cloud Computing environment. It will also suggest ways to mitigate against those risks to enhance the security and integrity of personal information that is stored or migrated into the cloud for computing.

BACKGROUND

With the growth of cloud computing and an increasing number of applications offered on the platform of Software as a Service (*SaaS*) there has been an increasing amount of personally identifiable information uploaded into "the cloud" for processing and storage. What are the threats to the security of personal information in the cloud?

A couple of methods have been used to analyze or affect the level of security to personal information offered within the cloud. For several years, Dr. Anne Cavoukian, the Privacy Commissioner of Ontario has been promoting the concept of Privacy by Design (PbD), (Cavoukian, 2010). This is a process by which, systems are designed to contain provisions for the protection of privacy and personal information at the outset. The concept proposes to build systems which have the protection of privacy as a default, rather than retrofitting them at later stages. Another approach to this problem has been undertaken by David Tancock, Siani Pearson, and Andrew Charlesworth. They proposed the creation of a "Privacy Impact Assessment (PIA) Tool for Cloud Computing" (Tancock, Pearson & Charlesworth, 2010), which would be an automated application that would analyze data input with regards to a project and rely upon a pre-set body of knowledge from those jurisdictions that currently require the completion of Privacy Impact Assessments (PIAs)[1] to determine the level of risk associated with certain undertakings.

Our current state of knowledge on the subject matter of security of personal information in cloud computing is quite limited. Because the "Cloud" is a relatively immature concept and technological solution, very little is known about its exact operation, how it "behaves" and the level of security that it affords to data stored and processed within. Given the limited knowledge we have about the technology, we must examine the current legal framework for ensuring that the security of personally

[1] Government of Canada. Privacy Resources. "Privacy Impact Assessments (PIAs) are used to identify the potential privacy risks of new or redesigned federal government programs or services. They also help eliminate or reduce those risks to an acceptable level". http://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp *Accessed: 2012-10-08.*

identifiable information stored in the cloud is sufficient to prevent privacy breaches from occurring.

AIMS and OBJECTIVES

This project will undertake to identify and assess the potential risk to privacy in the use of **Enterprise Systems Applications** (**ESA**) associated with *SaaS* (Mell & Grance, 2011) in the implementation of e-Government solutions and suggest ways to mitigate those risks. The project will analyze and identify the prevailing security threats and suggest ways to mitigate against those threats thereby affecting the level of security of personal information in cloud computing. To accomplish the task, an analysis of the current knowledge about *SaaS* and web 2.0 will be undertaken. A detailed analysis and critical assessment of potential privacy risks, legal frameworks associated with privacy protection and cloud computing in general will be undertaken. Finally, risks to the security and privacy of personal information in the *SaaS* and Cloud environment as well as strategies to mitigate against those risks will be mapped.

RESEARCH QUESTIONS

To assist in the task of meeting the aims and objectives set forth in the previous section I have proposed the following research questions, which will act as a guide as we navigate through the thesis and the often complex realities of the cloud. ***What are the threats to the security of personal information in SaaS "cloud-based" applications for Enterprise Application Systems (EAS) eGovernment initiatives? What are the shortcomings of the methods currently used to identify and mitigate the risks to privacy in applications used in the public sector? Does the deployment of EAS on the cloud using the SaaS platform offer adequate safeguards and does it minimize the risks associated with the SaaS platform?***

By answering these questions, I will facilitate a better understanding of the risks associated with the processing and storage of personal information in the cloud. It will also yield suggestions for mitigating the risks prior to undertaking projects which utilize cloud-based technologies for the implementation of eGovernment initiatives.

RESEARCH METHODOLOGY

This project will utilize the literature based approach, utilizing both academic and industry specific publications to arrive at the answers to the research questions that have been posed. Through an extensive and detailed review of literature on the subjects of: information security, privacy protection, cloud computing, eGovernment, EAS and data security and privacy protection legal frameworks across several jurisdictions, the conclusion will resolve the questions arriving at a recommendation on the subject of the: Security of Personal Information in Cloud Computing.

The analysis of both academic and industry related publications will enable a better and more complete understanding of the technology. It will also help to clarify which of the technological solutions pose the greatest threats to the security of personal information in the cloud.

THESIS OUTLINE

This thesis will identify potential risks to the security of personal information and examine ways to mitigate against those risks in the deployment of Enterprise System Applications on the Software-as-a-Service platform in the course of deploying e-Government solutions. First it will outline and define the concepts of the Cloud, e-Government, and Enterprise System Applications. A discussion of the security of personal information and privacy will follow, both on a high level of the concepts themselves and as they relate to Cloud Computing. This will include a detailed examination of the prevailing legal frameworks for the preservation of privacy in Canada, the U.S. and the E.U. Having laid the foundation for the legal basis for the

need to protect personal information and privacy, a discussion of the legal interpretations of the legislation will follow, to demonstrate the manner in which the legislation functions in practice. Following this, the thesis will tackle the identification and explanation of the potential threats to personal information and privacy in cloud computing. Because many, if not most, of the threats are common to multiple platforms of delivery of *SaaS*, the discussion will focus on the general threats associated with Cloud computing; however all of the threats identified are specifically tied to the *SaaS* platform among others. Once the threats have been outlined and discussed, a brief presentation of the view that Cloud computing offers adequate, if not greater, security will be presented and assessed. Strategies, and techniques to mitigate against the risks identified will be undertaken, which include the utilization of Privacy Impact Assessments and the Privacy by Design Frameworks will follow. Specific technological and systemic tools will also be discussed to truly address the risks identified previously and propose methods to minimize those risks to a manageable level. The final chapter will tie the concepts of cloud computing, Enterprise Systems Applications, and e-Government, as they relate to the privacy threats and risks identified and will summarize the most important findings of the project while drawing fundamental conclusions about the relationship between the need for protecting privacy and *SaaS*.

CHAPTER I

CLOUD COMPUTING

The National Institute of Science and Technology defines cloud computing as being a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011).[2] One of the ways in which cloud computing is able to compete with traditional modes of computing is to reduce the costs through the pooling and sharing of the available resources. Traditionally, if a corporate entity wanted to deploy a new database, they would acquire the hardware, software and staff with technical knowledge to launch and maintain the network. This would generally result in under usage of the network, at least in the initial stages of deployment and operation. In fact, Amazon discovered that their networks were being run at 10% capacity at any given time, to account for occasional spikes in the demand and usage of the network (Hof, 2006)[3] The corporation would have to front 100% of the costs associated with the roll out, even though it would take years to reach anything above the 10% utilization mark, especially since the system would continue to be upgraded and expanded throughout its life to prevent over utilization and account for times of increased demand on the resources.

As a result, cloud computing has filled a niche, offering a more cost-effective and neater solution for corporations, giving them the ability to roll out new networks without incurring substantial up-front expenses, and enabling further expansion to the system as needed. It remains competitive, because users only pay

---

2 The NIST (National Institute of Standards and Technology) Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf *Accessed 2012-04-01*.

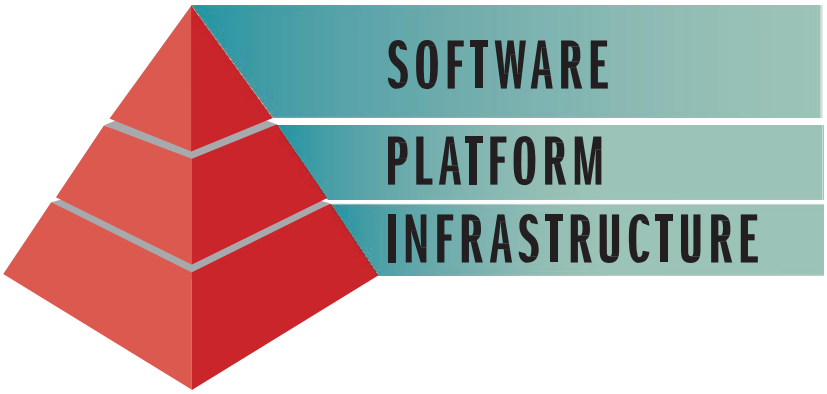
3 Business Week. Jeff Bezo's Risky Bet. http://www.businessweek.com/stories/2006-11-12/jeff-bezos-risky-bet *Accessed 2012-05-09*.

for what they are actually using. Through the pooling of resources, efficiency far greater than 10% could be reached.

There are several platforms for the delivery of cloud computing solutions, all of which give customers a certain degree of control over the type and size of investment that they wish to undertake. Ultimately, however, it must be said that adoption of web 2.0 technologies always carries with it a voluntary surrendering of much of the control over the infrastructure, servers, and, even to some extent, the applications and software to the provider. Brief descriptions of the platforms, and what each has to offer, both in terms of the advantages and possible disadvantages, follows below (Mell & Grance 2011):

1. ***Software-as-a-Service (SaaS)***. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a web browser, or program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities.
2. ***Platform-as-a-Service (PaaS)***. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created, or acquired applications, created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (including network, servers, operating systems, or storage), but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
3. ***Infrastructure-as-a-Service (IaaS)***. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications which may have limited control of select networking components (e.g., host firewalls).

The relationship between *SaaS*, *PaaS* and *IaaS* can be characterized as the building blocks of cloud computing, each one layered on top of another, thus creating what is often referred to as the 'Cloud computing stack' (see figure below) (Kepes, 2011).



In actuality, the layers themselves are not as clearly defined with the boundary between them, especially *PaaS* and *IaaS*, becoming increasingly blurred (Kepes, 2011). All of the layers are interdependent on each other, as each of them represents a different aspect of the Cloud - information, applications and infrastructure. The complexity and possibilities increase with each layer, from the most basic, *SaaS*, offering almost no control and enabling the utilization of existing 'out-of-the-box' applications. *PaaS*, which creates an environment and tools to develop applications for relatively low cost; to *IaaS*, which provides greater control over the infrastructure and resources, to either develop, or migrate data and applications created in a different environment (Barnatt, 2011).

This project will focus on *SaaS*, the most common platform being currently adopted by "public bodies" despite the many risks, given their limited involvement in software and application development as well as stringent licensing agreements that

limit their ability to place acquired software into a cloud environment (1105 Government Group Report on Cloud Computing, 2012)[4].

SaaS is the most basic iteration of Cloud Computing, making it easy to provision with virtually no up-front cost. The lack of control however, can be troubling, especially for agencies and public bodies that tend to have rigorous legislative and regulatory regimes to meet when it comes to external collection and hosting of data (Kepes, 2011), especially when 'external' could and usually means extraterritorial, thus subject to foreign legislation.

There are several models for the deployment of cloud services, all of which are possible in combination with the selected platform for the roll out (Mell & Grance, 2011); which essentially means that it's possible to implement *SaaS* in a public, private or hybrid environment.

> *1.* ***Private cloud***. The cloud infrastructure is provisioned for exclusive use by a single organization, comprising one or multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
>
> *2.* ***Community cloud***. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
>
> *3.* ***Public cloud***. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
>
> *4.* ***Hybrid cloud***. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that

4 http://docsfiles.com/pdf_1105_government_information_group_custom_report.html Survey results filtered to include only public sector respondents. Report is based upon responses from IT professionals representing 289 public bodies at the Federal and Municipal level.

> remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Cloud providers themselves have also begun to address the issues surrounding the applicability of the application of the cloud for various types of data. This has become especially important in light of the recoil effect, whereby many public agencies that had already adopted Web 2.0 as a solution to their computing needs abandoned the technology after implementation (1105 Government Group Report on Cloud Computing, 2012)[5]. A sharp decline in the use of the public cloud by Government agencies year-to-year has sparked what the 1105 Government Group refers to as the "shrinking of the public cloud", at least among public bodies, as the overall uptake of the public cloud - taking into account all deployment platforms, continues to grow. This is but one reason for the development of tools, such as Oracle's Cloud Candidate Selection Tool: Guiding Cloud Adoption, a practical guide, which for the first time takes a more serious approach at differentiating between public and private sector clients, nature of data to be uploaded into the cloud and the so called "Location Affinity" of the uploaded components, which determine the relative "independence" of the applications (Oracle White Paper, 2011).[6] This aspect is especially important for Government agencies, as they often maintain multiple databases which draw information from each other in order to function. The Oracle White Paper identifies this as a scenario, which may preclude the ability to adopt a cloud-based solution if any of those co-operating databases remain "off" the cloud. The guidelines also address the issues surrounding government regulations and data locality, which are of utmost importance to ensuring data security (Oracle White Paper, 2011).[7]

---

5 1105 Government Group Report on Cloud Computing, 2012. http://docsfiles.com/pdf_1105_government_information_group_custom_report.html A 13% drop was reported. *Accessed 2012-04-27*

6 *Accessed 2012-04-24.* http://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-candidate-tool-r3-0-1434931.pdf

7 Ibid. Accessed *2012-04-24*

e-GOVERNMENT.

The United Nations Department of Economic and Social Affairs prepared the e-Government Survey 2010, which defined the term as "the employment of the Internet and the world-wide-web for the delivery of government information and services to the citizens."[8] This relatively new phenomenon is said to have emerged in response to the search for greater efficiency in the manner in which governments spend public funds in the provisioning of services for the population. "The use of ICT in government structures is not new, but the concept of e-Government became widely used in the late 1990s when it became a policy strategy that focused on improving service delivery" (Waksberg-Guerrini & Aibar, 2010). This became much more pronounced following the economic and financial crisis of the mid-2000s, which has in large part been fuelling the adoption of cloud computing as a possible solution. It sought a way to create a more efficient and effective electronic framework for communication between Governments and Citizens. Three key driving forces have been identified for the adoption and proliferation of e-Government solutions (Waksberg-Guerrini & Aibar, 2007):

1) Efficiency (*Financial and Organizational Value*): financial gains, better empowerment, better organizational and IT architectures.
2) Democracy (*Political Value*): openness, transparency, accountability and participation.
3) Effectiveness (*Constituency Value*): reduced administrative burden, increased user value and satisfaction, inclusive public services.

It has become much more than a communication tool, as an increasing number of services are now available electronically which has made them much more accessible and easier to request, while becoming easier and less expensive to provide for governments. One issue that has arisen as a result of the move towards e-

8 United Nations. E-Government Survey 2010.
http://www2.unpan.org/egovkb/global_reports/10report.htm *Accessed 2012-04-01*

Government is the security of the personal information that citizens are providing via the electronic platforms created by governments; it is no longer a matter of being offered a choice to either request services online or in a traditional manner in person. In many instances, there is only one option for requesting the service, that being online. This raises the issue of individual consent to having ones personal information collected and used for a specific purpose and in a particular manner. While there is no doubt that the consent exists for the use of the personal information for a specified purpose, as the individual is providing their information in order to request a service, the lack of alternative means for requesting the services in question raises a concern as to the legitimacy of the consent to collect the information in the prescribed manner.

The concept of e-Government can bring with it mixed blessings, as the myriad of services that are being considered for, and launched using *SaaS* platforms have potentially far-reaching and intrusive consequences for the preservation of personal privacy of data subjects, if their data is not collected, stored or computed in an appropriate manner. Some of the most often cited business solutions for e-Government include: finance and accounts, human resources, procurement, inventory and material stock management, fleet management, project systems and real estate management as well as 'citizen's portals (Prakash & Gulla, 2008). In additional to this, many government bodies, at all levels, have utilized the web to "disseminate a wide range of sensitive information on personal, financial and medical aspects…hence IT departments in organizations should be aware that the security and privacy are not only critical for the availability and delivery of government services but also to build citizen confidence and trust in the online services and transactions" (Ebrahim & Irani, 2005). The aspect of building and strengthening citizen trust is of utmost importance, as the e-Government movement could potentially cause the loss of sensitive personal information of large numbers of individuals and end up failing miserably. Some high profile instances of privacy breaches and data compromise have dealt serious blows to continued efforts to migrate e-Government services onto the public cloud infrastructure.

> "The most publicized case in the UK involved the loss in October 2007 of personal data records for 25 million individuals and 7.25 million families receiving child benefits by Her Majesty's Revenue and Customs…More recent figures suggest the number of breaches is getting even worse with 7 in 10 UK organizations having experienced a data breach in the year to July 2009, up from 60% in the previous year" Other countries have had similar experiences" (Wright, 2011)

There are several distinct categories of delivery interaction models that fall within the general classification of e-Government, all of which have been extensively utilized in the traditional model of Government interactions. The traditional interactions have now been augmented by offerings of the computer age, increasing the frequency and speed with which these interactions can be carried out (Jeong, 2007).

- G2C (Government to Citizens)
- G2B (Government to Businesses)
- G2E (Government to Employees)
- G2G (Government to Governments)
- C2G (Citizens to Governments)

This digital interaction consists of governance, information and communication technology (ICT), business process re-engineering (BPR), and e-citizenship at all levels of government (city, state/province, national, and international) (Jeong, 2007). Recently, another category of e-Government interaction had emerged, sometimes referred to as "Government 2.0", which refers to the utilization of social media by government agencies (E-Government Survey, 2010). This tool is being utilized by an increasing number of institutions across the world at various levels and branches of government. This is not merely a communications tool however; it is also used to solicit and compile stakeholder involvement in various government initiatives. Government uses social media as a means to receive citizen input, and to conduct

citizen and stakeholder engagement prior to finalizing projects. Social media has been growing in importance to Government in that it can be utilized as a very ad hoc and quick tool to gauge citizen interest, displeasure and general attitude towards initiatives, plans and reactions to completed projects. A definite issue with the utilization of social networks to engage with citizens and carry on e-Government practices is the lack of public awareness regarding the impacts on their privacy that social networks wind up having.

> "Many users do not seem to realize that their free use of social networks has an indirect but steep effect through the exposure of their own personal data…do not realize which impact they have on the privacy of their friends and families when they publish information about them" (van Eecke & Truyens, 2010).

One of the most interesting aspects of social media is that it is a technological tool that is predominantly cloud-based and facilitates engagement between government and e-Communities, which are, for the most part, reflective of traditional communities. When the terms 'communities' and 'e-communities' are used in this context, it refers to the definition put forth by J. Preece, 2010, who understood them to mean communities consisting of:

- ***People***, who interact socially (in the e-Community) as they strive to satisfy their own needs or perform special roles as leading or moderating.
- A shared ***purpose***, such as interests, need, information exchange, or service that provide a reason for the community.
- ***Policies***, in the form of tacit assumptions, rituals, protocols, rules, and laws that guide people's interaction (in the e-Community at hand).
- ***ICT*** *(Technical Infrastructure),* to support and mediate social interaction and facilitate a sense of cohesion and togetherness.

The definition was used to explain what makes an e-community. In the context of my thesis, I see a definite correlation between what constitutes an e-Community with what we would understand to be an 'interest group' which is also a form of community. As members of an interest group also interact, on multiple levels, one of which would be social, they share a common interest or reason for action and often have internal protocols or tacit assumptions, whether codified or not. The method for their interaction is increasingly ICT based. The use of social media enables the government to reach e-Communities, which are representative of our traditional understanding of communities, which in turn are often organized along the lines of common interests or needs. The shift to e-Government has also been referred to by some scholars as a "transition towards a new form of network organization at the core of the public administrations that might be conceptualized as a virtual state or, as a network administration" (Waksberg-Guerrini & Aibar, 2010)

ENTERPRISE SYSTEM APPLICATIONS (ESA)

A common definition of ESA states that "Enterprise applications are about the display, manipulation, and storage of large amounts of often complex data and the support or automation of business processes with that data (Fowler, 2002). Enterprise System Applications are widely utilized in the software industry today, and are often subjected to a 3-dimension model of assessment, focusing on: "Process, Management and Technique" (Yang & Liu, 2010). Some of the unique features of Enterprise software are that it is generally required to conform to management patterns, business processes, and enterprise culture, yet at the same time offering flexibility to the Enterprise to tailor the end product to the required or desired specifications (Yang and Jiang, 2011). ESA software implementation is nonetheless considered to be "high-risk", by academics and enterprises alike (Yang & Liu, 2010). They do, however, offer corporations more control, input, and customizability of the application to fit the required purpose, at least in the design phase. Theoretically, this should mean that this is the perfect mechanism for ensuring that privacy protection controls are implemented right at the start of the design process, taking care of compliance and security issues. This is not always the case, as an equally important

issue is the method of deployment and the infrastructure of the cloud-based platform that is chosen.

While the application itself can and should have security features built-in, the platform and architecture delivering it must also offer protection to prevent architecture weaknesses from being exploited, as will be discussed in the section on threats to privacy in cloud computing. The application is only going to be as safe and secure as the deployment infrastructure permits, which could mean that adopting public cloud *SaaS* solutions could undermine the process of designing applications with adequate security features. The personal information may still be susceptible to "sniffing, spoofing, man-in-the-middle attacks, side channel and replay attacks [as] possible threat sources" (Catteddu & Hogben, 2009). There are also several barriers to the adequate implementation of security features into ESA, the first being the organization's internal culture as it relates to privacy concerns. If "executive sponsorship" and buy-in into a unified and coherent vision of software security is not achieved, then the entire effort will end up a resounding failure (Steven, 2006). Secondly,

> "Economists and software developers often have difficulty quantifying the value of security and privacy…because of this security and privacy are rarely designed as key components during system design, rather they become cumbersome operational 'bolt-on' features that often work orthogonally to a system's intended functional purpose" (Hurlburt et al, 2009)

This often results in very abstract views of the relationship and interconnectedness between security and privacy, which results in an all-or-nothing outcome of security over privacy or privacy over security or the suggestion that privacy and security are completely independent of each other. The desired outcome is a scenario which realizes and accepts the fact that both concepts exist separately but overlap (Hurlburt, Miller, Voas & Day, 2009). If the first two hurdles are overcome, unclear and frequently changing objectives can also have a detrimental effect on implementation

as well as the cross-platform and multi-system structure, technical resource limitations and unexpected risks that emerge during the design process (Yang & Jiang, 2011). It is also worth noting, that many of the techniques utilized to improve scalability end-up having negative effects on the Performance/Availability/Reliability (PAR) of the application (Jacobs, 2005):

1. The maintenance of session state in memory on the application's servers reduces reliability.
2. Best-effort catching of data reduces data consistency.
3. Web–based applications can have difficulty ensuring transactional integrity across read, edit and update of the data.
4. Session concentration, with a layering of machines, whereby smaller and slower machines must first be accessed which then in turn access fewer larger machines slows down response time.
5. Asynchronous communication results in one-way messages being sent back and forth which also slow down response time.

Once ESA has been deployed into a cloud environment there are further limitations as to the scalability of the architecture that may emerge - largely due to the multi-tenancy and pooling of resources, which has a tendency to "decrease the service providers ability to configure the system differently for different organizations" (Jacobs, 2005). As such, ESA cannot, and should not be viewed as a magical cure for the risks associated with cloud computing, especially in connection with a *SaaS* deployment model. All or most of the same risks still exist. They must be addressed, with the potential risks to privacy and data security being addressed prior to the design and deployment of the system; this can be accomplished through the use of privacy and risk impact assessments. The goal of the risk assessment and implementation of mitigation strategies and mechanisms aims at fulfilling legal and regulatory obligations. After all "privacy mishaps can not only trigger scrutiny from domestic and international regulators but also have a significant and lasting impact…which can haunt companies indefinitely" (Knutson, 2007).

CHAPTER II

SECURITY OF PERSONAL INFORMATION AND PRIVACY

Protection of privacy rights have come a long way since the groundbreaking essay "The Right to Privacy" by Warren and Brandeis written in 1890 (Axelrod, Bayuk & Schutzer, 2009). The basic principles have remained unchanged; the process and societal acceptance has evolved. The rights have become codified and are respected in much of the Western world. Since the first legislation formally entrenching privacy rights in the 1970s, much more has been achieved in the realization of the importance of these rights in enabling people to partake in the exercise of democracy. Privacy has been defined as (Yael Onn et al. 2005):

> "The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose"

Although no universal definition exists, and many different variations exist, this definition contains a very important aspect that is of utmost importance in the quest to discover what privacy is; the element of control over our personal 'domain'. There are a multitude of different types of threats to one's privacy that are specifically linked to cloud computing and internet usage. The control over the extent to which our personal domain can be accessed by others is a key element of privacy legislation in North America and the EU, which will be discussed in more detail later in this paper.

When we think of privacy, it's important to point out that there are generally three different aspects to privacy (Krekke, 2004):

1. Territorial Privacy: referring to the close physical area surrounding a person.
2. Privacy of the Person: which include 'undue interference', physical searches and information violation.
3. Informational Privacy: control over the manner in which personal data can be collected, stored, processed or selectively disseminated.

It is possible to compromise a person's privacy through the violation or encroachment on any of the three listed aspects to privacy. At the same time, it is unlikely that complete privacy and lack of dissemination of personal information can be prevented in all aspects of privacy given social interaction as well as engagement with government - especially through e-Government initiatives, where a frequent barrier to adoption is the lack of, or perceived lack of, "adequate security and privacy" (Ebrahim & Irani, 2005)

The first significant type of threat is in the form of data-mining by Internet Service Providers (ISP's) and online cloud-based service platforms, such as social networking sites, internet browsers and search engines, and collaboration sites.

> "Google for instance, leverages its cloud infrastructure to collect and analyze consumer data for its advertising network…EPIC has called for Gmail, Google Docs, Google calendar and the company's other Web applications to be shut down until appropriate privacy guards are in place" (Chow et al., 2009)

I have listed data-mining first, because this is the most common type of privacy threat that all internet users are subjected to on a daily basis. Most people do not approach this as a serious privacy threat, because consumers have become

conditioned to accept this practice as a 'necessary evil'; being able to take advantage of internet-based services and applications, especially those offered to users free of charge (Gunnarsson & Ekberg, 2003). This is however, one of the most fundamental and far-reaching threats to one's personal privacy; it's very systematic, it occurs on several different levels and is often packaged, marketed, and resold to any-and-all interested parties. The dangers with this type of practice come when data mined is later correlated with other sources of information about specific individuals or populations, thereby creating very detailed profiles of individuals which could lead to the creation of surveillance profiles consisting of internet browsing patters, online shopping habits, political and religious affiliations, travel patterns etc. (Fayyad, Piatetsky-Shapiro & Smyth, 1996)

> "The actual data mining task is the automatic or semi-automatic analysis of large quantities of data to extract previously unknown interesting patterns such as groups of data records (cluster analysis), unusual records (anomaly detection) and dependencies (association rule mining). This usually involves using database techniques such as spatial indexes. These patterns can then be seen as a kind of summary of the input data, and used in further analysis or for example in machine learning and predictive analytics".

The process of Knowledge Discovery in Databases (KDD) relies upon several steps to arrive at a final conclusion or analysis of the data, with the practice of Data Mining being but one of the necessary steps. The process begins with the (1) *Selection* of data to be analyzed. Then the data is (2) *Pre-processed* which entails 'cleaning' the data to remove 'data noise' – or misleading information and accounting for missing data, and (3) *Transformed* (into a useful format which takes into account the data features and the goal of subjecting the data at hand to the KDD process before undergoing (4) *Data Mining* and resulting in a final (5) *Interpretation/Evaluation* (Fayyad, Piatetsky-Shapiro & Smyth, 1996). Data-mining is also closely related to tasks like data-dredging, data-phishing and data-snooping. These practices refer to data mining on a micro scale, meaning that it is applied to a small sample of a much larger population. The resulting analyses are generally

viewed as being unreliable in the quest to discover valid patterns. It is these practices that are of most concern to privacy, as they generally do not follow the established and accepted steps of KDD, cutting corners and leading to questionable applications and unreliable results.

SOCIAL NETWORKING & DATA COLLECTION

When one examines the 'terms of use' and privacy policies of services such as Facebook, Google and Youtube, it becomes quite clear that the evolution of these policies is heading in the direction of greater access to, and ability to use, personal information mined from users any way the provider sees fit. The latest changes to Facebook's privacy policy, currently referred to as the "data use policy" reads (Facebook, 2012):

> When you connect with an application or website it will have access to General Information about you. The term General Information includes you and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to "everyone."... Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.[9]

This category of threat to personal information is of significant importance in the provisioning of e-Government services through cloud computing enabled platforms. Increasingly, governments utilize social media platforms to communicate with the public, seek public input and engagement, and contract-out services to cloud-based

9 Facebook. http://www.facebook.com/full_data_use_policy *Accessed 2012-04-07*

third parties to administer on behalf of government. While there is a definite benefit in utilizing social networking platforms to engage individuals that historically have been difficult to reach, it must also be noted that the ease with which information can be solicited from individuals by Government and the impossibility of guaranteeing anonymity or even a dedicated use for the information when utilizing these platforms is also of concern. In essence, by taking advantage of social networks to seek out input and engage the population, Governments have entered into de facto information sharing agreements with the social networks. As the term implies, in order for information sharing to take place, there needs to be an exchange of information between the Government agency and the social network provider.

In this instance, the exchange takes place in the form of joint usage of the collected information. The risk to privacy occurs when we realize that social networking sites cross reference collected information. As we can see from the excerpt above, the default settings are increasingly leaving data vulnerable to mining and cross-referencing.

Another category of potential privacy threats comes from hacking, which may include techniques such as (Gupta, Klavinsky & Laliberte, 2002):

1. Network enumeration: Discovering information about the intended target.
2. Vulnerability analysis: Identifying potential ways of attack.
3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.[10]

Ultimately, we must remember that personal information has become *the* commodity on the internet these days. It winds-up being collected, both directly and indirectly from data subjects, stored and used in many different ways by an army of users,

10 Security Through Penetration Testing: Internet Penetration. InformIT. http://www.informit.com/articles/article.aspx?p=25916. March 2002. *Accessed 2012-04-10*

producing a “panopticon beyond anything Bentham ever imagined” (Ausloos, 2012). Furthermore, it is also very difficult, if not impossible, to predict all of the negative or potentially intrusive consequences that can result from the collection, use, disclosure and mining of personal information (Ausloos, 2012). Governments must be incredibly diligent in the manner in which they engage in the gathering, storage, and computing of PI (Personal Information) so as not to increase the risks to privacy of the data subjects while trying to save a buck or two. This is especially true when services are out-sourced to the cloud, which poses many of the traditional and several “unique”, threats to the integrity and security of the information. The importance of the preservation of our privacy rights cannot be stressed enough, given that:

> “Privacy is an important right that feeds into other rights; for instance, a lack of privacy can undermine family life, confidential services and free press. Totalitarian regimes know to their cost that citizens need a private space to develop, or organize around, a dissenting thought; that is why personal privacy is anathema to such regimes” (Pounder, 2009)

The fact that personal information has become a very sought after product results in a need for Government’s to exercise a great deal of caution when handling or employing the cloud for the collection and processing of personal information especially because of the high potential for the disclosure of such information as a result of the threats to the security and integrity of said personal information which will be discussed in great detail in the upcoming sections.

CHAPTER III

LEGAL FRAMEWORK

The primary legal framework that will be examined in this thesis is that of Canada, at both the Federal and Provincial levels. However, many references and comparisons will be made throughout to the legal environment for privacy protection in the United States of America (USA) as well as the European Union (EU). Because no solution exists in a vacuum, and extensive data flows exist between Canada and the USA, as well as the US and the EU, it will be important to map out the similarities and differences between approaches in each of the countries or territories listed.

The interplay between Canada and the USA is especially important as far as the realities of CSPs (Cloud Service Providers) locations in North America are concerned. The majority of web 2.0 providers are based out of the United States, which inherently means that any data that is stored in the USA is also subject to US laws. This is especially troublesome when one considers the far-reaching effects of the USA PATRIOT Act; the official title of which is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001"[11]. The PATRIOT Act was enacted as counter-terrorist legislation which intended to allow US authorities to gain access to information held by US companies about both national and international entities. Some of the purposes that were stated during the enactment of the legislation read:

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;

11United States Department of Treasury. Financial Crimes Enforcement Network (FinCEN). The Patriot Act. http://www.fincen.gov/statutes_regs/patriot/index.html *Accessed: 2012-04-14*

- To require all appropriate elements of the financial services industry to report potential money laundering;
- To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.[12]

Of note is the second provision, which seeks to "subject to special scrutiny foreign jurisdictions", which has, in essence, resulted in a great deal of panic as to the security of data stored by US firms, whether cloud-based or not, as well as to firms that are subsidiaries of parent companies that are US based. In fact, the interpretation of the issue of jurisdiction by US courts has led to a reality whereby all companies that have US ties are subject to the PATRIOT Act. An analysis of the jurisdictional question has yielded the following results for EU based corporations with US ties or parent companies (Bodle, 2012): The Patriot Act applies to customer data held by any company located in:

- the EU which has a US parent company;
- the USA;
- the EU and using the services of a US subsidiary for data processing;
- the EU which uses any third party to store or process data in the USA i.e. a hosting company.[13]

The analysis and interpretation is based upon decisions that have been handed down by US courts, which means that the same application of the PATRIOT Act will be

12 Ibid. *Accessed: 2012-04-14*

13 Bodle, Irene (2012) EU Data Protection Law and the Patriot Act in the Cloud. Web Analytics World http://www.webanalyticsworld.net/2012/03/eu-data-protection-law-and-the-patriot-act-in-the-cloud.html *Accessed: 2012-04-14.*

invoked with regard to data that originated in Canada. There are several sections of the PATRIOT Act which have caused particularly high alarm among Canadian corporations and government agencies, most notably: Section 2702, "voluntary disclosure of customer communications or records''; and Section 2703, "required disclosure of customer communications or records".[14]

Both of the sections deal with instances where the PATRIOT Act is invoked, with the voluntary disclosure by the service provider being immune from prosecution for breaching of US Privacy Laws. In the instance of Section 2703, when the provider is compelled to disclose customer data, they are also immune from liability and forbidden from informing the originator of the data about the disclosure.[15] These regulations are in stark contrast to Canadian and EU Privacy Laws, as well as the Safe Harbor Framework negotiated and signed between the USA and the EU prior to the passing of the US PATRIOT Act in 2001. This is a far cry from the 1973 Fair Information Practices code that was issued by the Department of Health, Education and Welfare (HEW) in reaction to the "growing public distrust of computerized recordkeeping systems" which called for (Axelrod, Bayuk & Schultzer, 2009):

1. No personal data record keeping systems whose very existence is secret
2. A way for individuals to find out what information about them is being stored
3. A way for individuals to prevent alternate uses of their personal information without consent
4. A way for individuals to correct or amend identifiable information about them
5. Assurance of the reliability of data created, stored, used or disseminated as well as 'reasonable" precautions to prevent the misuse of data

14 US Department of Treasury. FinCEN. USA PATRIOT Act 2001. http://www.fincen.gov/statutes_regs/patriot/index.html *Accessed: 2012-04-15.*

15 US Department of Treasury. FinCEN. USA PATRIOT Act 2001. http://www.fincen.gov/statutes_regs/patriot/index.html *Accessed 2012-04-15* *Accessed: 2012-04-15*

The EUROPEAN UNION

The European Parliament and Council adopted the Data Protection Directive (95/46/EC) in October of 1995 (Amended in November 2003).[16] The Directive set out a regulatory framework for the protection of individual privacy while at the same time seeking to achieve a balance by way of a relatively unhindered movement of the data within the EU. The Directive set out strict limits on the collection and use of personal data, and required each member state to establish an "independent national body" responsible for the protection of the data.[17] It placed upon member states the duties to:

- Protect fundamental rights and freedoms to protection of privacy with respect to processing of personally identifiable data.
- Lawful processing of data, including specified and declared purposes for the collection, and processing of the data and inability to process for purposes incompatible with the stated purpose.
- Data collected can only be processed if the data subject has given consent for the processing. The collection cannot be excessive in relation to the original purpose for the collection.
- The controller must inform the data subject of their right to access and correct their data. In the event of indirect collection, the controller must inform the subject of the purpose for the collection and processing of the data. The controller must also provide their identity to the subject.(EurLex, 23/11/1995)[18]

---

16 Summaries of EU Legislation. European Parliament and Council Directive of 24 October 1995. http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm *Accessed: 2012-04-15*

17 Summaries of EU Legislation. European Parliament and Council Directive of 24 October 1995. http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm *Accessed: 2012-04-15*

18 EurLex. *Official Journal L 281, 23/11/1995 P. 0031 – 0050.* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *http*://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:31995L004 6:en :HTML *Accessed: 2012-04-16*

The European Parliament and Council have also adopted the Directive on Privacy and Electronic Communications in July of 2002.[19] This directive dealt with the processing of personal information and protection of privacy in the electronic communications sector. The directive placed the following duties upon providers of electronic communications providers:

- ensuring personal data is accessed by authorized persons only;
- protecting personal data from being destroyed, lost or accidentally altered;
- Ensuring the implementation of a security policy on the processing of personal data.[20]

The Directive dealt with matters related to the management of subscriber databases, and placed a burden on the providers to enable subscribers to withdraw, verify or correct their personal information free of charge. The Directive also addressed data-retention concerns, requiring providers to purge data when no longer required for the purposes of providing the service or billing matters. The Directive understood purging to mean the deletion of the data or anonymization of the data unless the data subject has given their consent for alternate uses of their personal information. Confidentiality of communications, and unsolicited communications were also addressed by prohibiting 'eavesdropping' on electronic communications, and requiring providers to get recipients to "opt-in" before targeted, unsolicited,

19 Summaries of EU Legislation. European Parliament and Council Directive 2002/58/EC. July 2002. http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm *Accessed: 2012-04-16*

20 Ibid. *Accessed: 2012-04-15*

communications could begin. The Directive addressed the issue of "cookies", which are hidden information exchanged between an Internet user and a web server, and are stored in a file on the user's hard disk. The Directive indicated that users must give their consent for information to be stored on their terminal equipment, or that access to such information may be obtained.[21]

In October of 1998, the European Commission's Directive on Data Protection went into effect and sought to: "prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection".[22] This measure severely limited European companies' abilities to transfer personally identifiable data of European Union residents outside of the EU. The Safe Harbor Framework was developed as a streamlined process for US-based companies to be able to get certified as having met the standards set out by the European Parliament and Council as to the protection of privacy provisions contained in the Data Protection Directive of 1998. Companies could receive certification if they adhered to the seven principles of the Framework, on condition of recertifying on a yearly basis:

- **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
- **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.

---

21 Ibid. *Accessed: 2012-04-15*

22 U.S.-EU Safe Harbor. http://export.gov/safeharbor/eu/index.asp *Accessed: 2012-04-15*

- **Security** - Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for.
- **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement** - There must be effective means of enforcing these rules.[23]

While the Safe Harbor Framework set out certain guidelines and best-practice parameters, to enable compatibility between the US and European Union Privacy legislation, it has been widely criticized for a lack of enforcement due to widespread non-compliance of the corporations seeking certification (Connolly, 2008). It is nonetheless often cited as a benchmark for ensuring adequate privacy protection provisions before the transfer of personally identifiable information to the US. The Framework has also been cited by other jurisdictions that were not a party to the agreement, as guidelines that would also establish compatibility between Canadian and US privacy legislation provisions. Since the inception of the USA PATRIOT Act, the Framework's effectiveness has gone largely into desuetude as the provisions of the PATRIOT Act for access to and processing of personal information and its extensive surveillance provisions, largely incompatible with European privacy legislation (Whittaker, 2011)[24].

23 U.S.-EU Safe Harbor. http://export.gov/safeharbor/eu/index.asp *Accessed: 2012-04-15*

24 Whittaker, Zack (2011). ZDNet. "Google admits Patriot Act requests; Handed over European data to U.S. authorities" http://www.zdnet.com/blog/igeneration/google-admits-patriot-act-requests-handed-over-european-data-to-us-authorities/12191 *Accessed: on 2012-05-05*. Google has publically admitted being compelled to turn over EU data, stored in a European based data centre to US intelligence, having first used the Safe Harbor Framework to transport the data to the US. Recently, Microsoft has also admitted to having had complied with Patriot Act requests for information about EU based data.

CANADA

The Canadian Privacy Legislation Framework is composed of both federal and provincial laws which seek to achieve fairly "uniform" privacy coverage across the country. Federally, Canada has enacted the ***Privacy Act (1983) and the Personal Information Protection and Electronic Documents Act*** (PIPEDA - 2000). In addition to these statutes, Canada has a system whereby Provinces can enact their own legislation, which supersede the federal legislation on condition the provincial law is found to be "substantially similar" to its federal counterpart (Privacy Sense Net, 2012)[25].

To date, three provinces have enacted legislation that meets this threshold, Quebec, which has enacted two statutes, the: Act respecting access to documents held by public bodies and the protection of personal information (Governments - Public bodies) and the Act respecting the protection of personal information in the private sector (Corporations - Private sector)[26]; British Columbia (BC) and Alberta have enacted legislation dealing with the public and private sectors as well, similar in both name and content: The ***Freedom of Information and Protection of Privacy Act*** (referred to as FIPPA in BC and FOIP Act in Alberta) which applies to public bodies and The ***Personal Information Protection Act*** (PIPA) which applies to the private sector. FOIP and FIPPA came into being in the mid-1990s, while PIPA followed in 2003, in BC and 2004 in Alberta, respectively. Because of the substantial similarities between the legislation, I will focus primarily on the federal legislation and that of Alberta as that is the legislation I am most familiar with and able to offer greater insights into its actual utilization, beyond the theoretical framework[27]. In addition to the public and private sector legislation in Canada, several access and information regimes have also been enacted dealing with personal health information. In Alberta, this legislation is referred to as the *Health*

---

25 Sense Net. http://www.privacysense.net/privacy-legislation/canadian/ *Accessed: 2012-05-03*

26 Sense Net. http://www.privacysense.net/privacy-legislation/canadian/quebec/ *Accessed: 2012-05-03*

27 ***FOIP in the Clouds***. Presented at the **2012 Municipal Information Systems Association** (**MISA**) **Prairies Spring Conference**. Paul Denys. FOIP Officer for Privacy, the City of Calgary, Alberta, Canada.

Information Act (HIA) and places stringent requirements upon the manner in which "custodians and affiliates" create and process health information, from the moment the information is collected, to when it is used, stored, and accessed (Tigerstrom, Nugent & Cosco, 2000).

The legislation is administered by "Privacy Commissioners" appointed by but independent of the government, which have the power to review decisions undertaken by public and private sector corporations and agencies in reference to the legislation. What is interesting to note, is that the privacy legislation at the provincial level in both British Columbia and Alberta is administered by an "Access and Privacy Commissioner" that has, what is referred to as, "order-making" powers. Commissioners have the ability to issue binding orders, much like judicial decisions; they also have the ability to issue fines for contravention of the legislation.[28]

The Federal Privacy Act of 1983 was largely based upon the eight Privacy Protection Guidelines issued by the Organization for Economic Co-operation and Development (OECD) in 1980[29]. The principles have had a profound effect on the development of Privacy Legislation in many states throughout the world and were enacted as a result of the "intensified investigative and legislative activities concerning the protection of privacy" of the 1970s[30]. The principles were considered to be the minimum acceptable standards which could be further augmented by national legislation and included:

1. **Collection Limitation Principle**: requiring that data collection be conducted in a lawful and fair manner with the knowledge and consent of the data subject.
2. **Data Quality Principle**: requiring that data be complete, relevant to the intended purpose, accurate and maintained up to date.

---

28 Queen's Printer BC. FIPPA Legislation. http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00 *Accessed: 20120-05-03*

29OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Information.http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html *Accessed: 2012-05-03*

30 Ibid. *Accessed: 2012-05-03*

3. **Purpose Specification Principle**: requiring that the purpose for the collection of the information must be specified at the time of collection and only used for that purpose or a consistent purpose.
4. **Use Limitation Principle**: requiring that data shouldn't be disclosed and can only be used for the authorized purpose, unless the data subject consents or legal authority exists.
5. **Security Safeguards Principle**: requiring that data collected must be protected from loss, unauthorized access, destruction, misuse or modification.
6. **Openness Principle**: requiring that there be a policy of openness with regard to developments, practices and policies regarding the data as well as the identity and location of the data controller.
7. **Individual Participation Principle**: requiring that the data subject have the right to access their information, and challenge that information if found to be erroneous.
8. **Accountability Principle**: requiring that data controllers be held accountable for complying with the principles.

The OECD principles have stood the test of time, and have been largely credited with being a pre-cursor to modern privacy legislation subsequently enacted in many Western democracies. One of the underlying purposes for the Guidelines was an attempt to unify and reduce differences between various national legislative frameworks with respect to privacy and the elimination of possible restrictions to the trans-border flow of personal data (due to those differences and the risks that this may entail).

The Canadian Privacy Act has remained substantially unchanged since its proclamation, yet continues to be relevant today, as the principles that were crafted at the time have remained as the basis for more modern legislation - most notably PIPEDA in 2000.

PIPEDA was founded upon ten principles, which in large part mirrored those that were formulated by the OECD and later were the basis for the Privacy Act

of 1983. The benefit of time and more experience with managing a privacy protection framework led to a more precise definition of the principles and greater prominence of those that had been previously amalgamated. The principles identified 30 years earlier have stood the test of time, showing that the rights that were formulated then for the first time are universal and true regardless of the technological reality that surrounds us. The ten principles of PIPEDA, often referred to as the "fair information principles" are: ***Accountability, Identifying Purposes, Consent, Limiting Collection, Limiting Use, Disclosure, and Retention, Accuracy, Safeguards, Openness, Individual Access, Challenging Compliance***[31].

Canada's Privacy Legislation was found to meet or exceed EU legislative requirements, which meant that the EU did not have to negotiate a Safe Harbor agreement with Canada, as the legislation was already compliant with European Council and Parliament Directives.

LEGAL INTERPRETATIONS

In Canada, as well as the EU, there is a common foundation upon which privacy legislation is built; a clear distinction drawn between "data stewards" and "data subjects". Canadian Privacy laws clearly state that the personal information collected belongs to the person who the information is about - not the agency or body collecting the data. One of the most basic principles of the FOIP Act is the right of individuals to control the manner in which their personal information is "collected, used or disclosed"[32]. Section 1 (n) of the FOIP Act defines personal information as being:

> "Personal information" means recorded information about an identifiable individual, including **(i)** the individual's name, home or business address or home or business telephone number, **(ii)** the individual's race, national or ethnic origin, colour or religious or political beliefs or associations, **(iii)** the

31 Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca/leg_c/leg_c_p_e.asp *Accessed: 20120-05-03*

32 Queen's Printer Alberta. The Freedom of Information and Protection of Privacy Act (FOIP Act) http://www.qp.alberta.ca/574.cfm?page=F25.cfm&leg_type=Acts&isbncln= 9780779762071 *Accessed: 20120-05-08*

> individual's age, sex, marital status or family status, **(iv)** an identifying number, symbol or other particular assigned to the individual, **(v)** the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, **(vi)** information about the individual's health and health care history, including information about a physical or mental disability, **(vii)** information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given, **(viii)** anyone else's opinions about the individual, and **(ix)** the individual's personal views or opinions, except if they are about someone else;

This very broad definition ensures that any data that is associated with a person becomes classified as being personally identifiable, and therefore falls under the stringent protection provisions of the FOIP Act. The Act also makes a distinction between custody of the data and control of the data, clearly establishing that "control" over records is of paramount importance, while "custody" is of secondary importance. This means that the public body is responsible for all records that it creates or has the right to manage, regardless of their physical location. This point is especially important when dealing with cloud providers, who are predominantly US-based. The public body continues to be responsible for the manner in which the records are administered, and the manner in which personal information is collected, used and disclosed by the 3rd party provider. Section 96 which defines records that the FOIP Act applies to, states that:

> **"**This Act applies to any record in the **custody** or under the **control** of a public body regardless of whether it comes into existence before or after this Act comes into force[33].

33 Queen's Printer Alberta. The Freedom of Information and Protection of Privacy Act (FOIP Act) http://www.qp.alberta.ca/574.cfm?page=F25.cfm&leg_type=Acts&isbncln= 9780779762071 *Accessed: 20120-05-08*. Section 96. Custody means the physical possession of the records, while control is the right to manage the records. As a result of 3rd party storage facilities and 3rd party vendor solutions that are undertaken by the public body, control over records created by or on behalf of the public body is of utmost importance.

One of the issues that arise is the difference in privacy protection legal frameworks that each party is bound by. Let's say that we take a Canadian municipality, which is deemed to be a "public body" under the Act and is subject to all of the provisions of said legislation, which then contracts-out certain services related to its operating programs to a 3rd party, cloud-based provider, from the US - as a result, several legal issues arise. Firstly, each party is subject to differing privacy protection provisions; secondly, the 'terms of service' agreements with cloud providers clearly state that the provider is subject to the legislation native to the location of their headquarters, with the result being that any disputes arising from the performance of the conditions of the contract shall be resolved by a court that has jurisdiction in the location where said headquarters are located. As an example, the Google Terms of Service for Business contain two points, one of which is a statement of fact, the other to which the customer must agree when accepting the agreement. In the preamble, the agreement states for the record that the agreement is being entered into by two parties, the provider – Google Inc. – and the customer:

> "This Google Apps for Business (Online) Agreement (the "Agreement") is entered into by and between Google Inc., a Delaware corporation, with offices at 1600 Amphitheatre Parkway, Mountain View, California 94043

> o 14.10 Governing Law.
> This Agreement is governed by California law, excluding that state's choice of law rules. FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA[34]

As a result, the customer agrees to abide by California law in the event that any legal disputes, concerning the performance of the contract, should arise. This includes

34 Google Apps Terms of Service – Premium Business.
http://www.google.com/apps/intl/en/terms/premier_terms.html *Accessed: 2012-04-27*

Privacy Legislation and the different requirements that are placed upon the provider by California State Privacy legislation versus the customer under provincial Privacy legislation in Canada. It would be quite an undertaking to compel a provider of services to appear before a jurisdiction "foreign" to them, and answer for breaching foreign laws that are not the "law of the land" in the location where the data is being stored and processed. This reality has resulted in a great deal of confusion for public bodies in Canada, and abroad, as to which legislation the provider is bound by.

This has been further reinforced by US Court interpretations, which have clearly stated that the determining factor for courts in the United States is not the origin of the data, but rather the "residency" of the data. If the data resides on the servers of a US-based provider, the residency of the data causes it to come under the jurisdiction of US law, such as the PATRIOT Act. Recent decisions out of the US have taken this interpretation of data residency a step further, by stating that even if the data does not physically reside inside the US, but is being stored by a company that is subject to US law or by a company that is a subsidiary of a parent company that is subject to US law, then the data residency of the information is deemed to be subject to US jurisdiction (Bodle, 2012). This interpretation has proven to be very problematic for both European and Canadian corporations and government agencies that have contracted, or were contemplating contracting the services of US-subsidiaries, in the hopes of taking advantage of a wider array of cloud-based services while at the same time avoiding the legal ramifications of "hegemonic" legislation like the PATRIOT Act which asserts paramountcy over all other legislation.

In most cases and examples of Canadian Access and Privacy laws, such as in Alberta, the FOIP Act is paramount over all other legislation unless the other legislation clearly states that its provisions or regulations are paramount over the

FOIP Act[35]. This sometimes results in situations where only certain provisions of other enactments prevail and take precedent over the FOIP Act[36].

Europe and Canada also share commonality in the application of privacy legislation. Privacy laws in Canada and the EU are 'sectoral' in nature; they apply to an entire sector, either the private or public sector and so are not specific to a single industry. This makes administration of the enactments easier, as all agencies or corporations that fall within either are bound by the same legal duties. This means that both individuals (consumers – data subjects) and the corporations or governments (data custodians) are all aware of the legal requirements that they must act within, and the level of privacy protection that is afforded them by the legislation. It 'evens the playing field' for both sides of the equation and makes compliance easier to achieve, as the corporations are not required to know and implement multiple pieces of legislation that they may be subject to, each one carrying with it potentially very different duties. In the US, this is not the case, as legislation is enacted for specific industries, placing detailed and often varying requirements upon each industry.

Furthermore, California law also specifies, in great detail the applicability and oversight of the provisions of each enactment. California, generally thought of as a leader in privacy protection and privacy legislation enactment in the US, has enacted many statutes which contain detailed and specific provisions for the protection of privacy, a small sample of which are listed below, (with brief explanations of their application). [37]:

---

35 Queen's Printer Alberta. The *FOIP Act*. http://www.qp.alberta.ca/574.cfm?page=F25.cfm&leg_type=Acts&isbncln=9780779762071 *Accessed: 2012-05-03* Section 5 of the Alberta FOIP Act states that: "If a provision of this Act is inconsistent or in conflict with a provision of another enactment, the provision of this Act prevails unless: a) Another Act, or b) a regulation under this Act, expressly provides that the other Act or regulation, or a provision of it, prevails despite this Act".

36 An example of such a situation is the **Emergency Management Act** of Alberta, which deals with administrative measures at times of crisis or disaster. Only Section 17 of the EMA prevails despite the FOIP Act, in all other respects, the FOIP Act prevails. http://www.qp.alberta.ca/documents/Acts/E06P8.pdf *Accessed: 2012-08-27*

37California Office of Privacy Protection. California State Privacy Laws. www.privacy.ca.gov/privacy_laws/index.shtml#privacy *Accessed: 2012-05-08*

- Computer Misuse and Abuse: Penal Code Section 502: criminalizes knowingly accessing and, without permission, the use, misuse, abuse, damage, contaminate, disruption or destruction of a computer, computer system, computer network, computer service, computer data or computer program.

- Electronic Eavesdropping by State Law Enforcement Officials: Penal Code Sections 629.50 – 629.98: The law sets out procedures for Sate officials to petition a Superior Court judge for authority to record, catalogue, maintain and report about recordings of all communications intercepted (except legally privileged communications). The law also requires the notification of the data subjects about intercepted communications and wiretapping activities, no later than 90 days after the termination of the activities or in the event of a denial of an application seeking wiretapping authority.

Ultimately however, unlike Canada and the EU, US law places the onus for the preservation of privacy upon the individual rather than the "data collector", which becomes problematic because few people possess the level of expertise needed to understand and apply privacy regulations affecting them through various types of private and public entities - especially given how dispersed they are throughout US Law.

> "The institution owns the data, not the customer-and information flow is largely impeded" (Langenderfer & Miyazaki, 2009)

The legislative differences among various jurisdictions are but one of the issues with data security and privacy protection, but it is of critical importance. This coupled with the fact that there as substantial and fundamental differences in the approach to "personal information" between the US and both Canada and the European Union;

and the fact that an overwhelming number of CSPs are US based leads to serious concern for the ability to ensure personal information remains protected and private.

RECENT LEGISLATIVE DEVELOPMENTS

The European Union has made recent modifications to its Privacy legislative framework, with the implementation of amendments to the 2002/58/EC e-Privacy Directive that took effect on 2012 May 26th, a year after it was officially announced; affectionately dubbed by some as the "Cookie Law". Cookies are used by the vast majority of websites to track certain data elements, which could in turn present risks to privacy. This is especially the case, given that traditionally cookies have been sent and retrieved by host domains automatically, without making users or visitors aware that this is happening. Cookies often contain what are referred to as 'tags' or 'trackers' and a typical website can set anywhere between 1 and 12 such cookies during each session. When we talk about sites that are supported through marketing ads, this number can increase exponentially to in excess of 500 cookies (O'Malley, 2012).

Much like in the culinary world, not all cookies are created equal. Some are perfectly innocent, remaining active only as long as a user remains logged onto a particular site while others can be much more malicious, collecting all kinds of information which is transmitted back and analyzed, even long after the user has left a particular domain. The cookies with trackers are of significant concern because they continue to be active behind the scenes, transmitting back information about movement within and between websites, as well as names, addresses and credit card numbers (Debussere, 2005). The European Union has become the first jurisdiction in the world to require individual consent before a cookie can be set. Site operators will be required to obtain consent from the user and inform the user of the fact that the website being visited is engaging in tracking. Once consent has been obtained, meaning the user has clicked on the consent button, the website will be required to provide a breakdown of the types of tracking that they engage in: Essential, Analytics, Customization and Advertising. Furthermore, the user will have the ability to look up the companies or entities that are conducting the tracking for each of the

listed categories and will have the ability to withdraw their consent from any or all of the individual companies (O'Malley, 2012).

While cookies are the subject of the legislation, the essence of the problem goes much deeper than just the 'cookie' itself. It is not so much the practice of setting a cookie as the practice of 'recalling' information from a cookie once it has been placed on a user's hard drive. Until now, there was no regulation on snooping in user's computers, which amounted to nothing less than sanctioned covert surveillance. While the directive applies to EU based entities and some have gone as far as suggesting that the law will not apply to extraterritorial companies and agencies that set and retrieve cookies. After all, what would be the means of ensuring compliance and enforcing potential breaches of the law?

While that remains unclear as the law hasn't been tested in the courts just yet, several interpretations that have arisen from law firms and researchers suggest that such an assumption would be a mistake! (Rashid, 2011). The Directive speaks of the use of equipment, located within the EU, over which the 'data collector' has at least partial control and has the intent of processing personal information (Debussere, 2005). While some providers have interpreted this to mean that they will not be liable, as they are not located in the EU and are utilizing servers located outside of the EU, the act of setting or recalling of cookies from within the EU essentially utilizes equipment located within the EU; The user's computer becomes the equipment that is being utilized for the purpose of placing a 'cookie' for the purposes of gathering and processing personal information. After all the cookie is placed on the user's hard drive, thereby utilizing a machine within the EU. As such, "the European legal framework for the use of cookies has a tremendous extra-territorial application" (Debussere, 2005).

Given the lack of knowledge as to the enforcement and possible penalties that could be imposed in entities that infringe on this Directive, it is still unclear what path will be taken by non-EU web sites that may try to elude having to comply with the newly implemented Directive. The other possibility is that even non-EU websites may modify their practices to comply with the legislation and rather than offering a two-tiered system for EU and non-EU, which could end up being more expensive for them; they may offer services that will meet the requirements of the directive for all of their users, regardless of their physical location. This is especially curious in light

of the fact that both Apple and Google have already been investigated for violating EU privacy laws and the new e-Privacy Directive, after it was alleged that iPhones and Google devices operating on the android operating system were collecting user location data (Rashid, 2011).

These legislative changes have the potential to arm consumers and the public in general with considerable control over the manner in which their personal and identifiable information is collected and analyzed, unlike ever before. The approach undertaken by the European Parliament and Council appears to be aimed at getting users to become more involved with and more accountable for their personal privacy. They will ultimately have the ability to accept or reject all or some of the cookies that host websites want to set on their machines. Rather than implementing draconian and top down legislation forbidding certain types of cookies from being utilized within the EU, the onus has been placed on the user to get informed and take an active role in deciding how much they are willing to share with companies that track their movements and collect information about them. Given the fact that currently, only 69% of internet users are aware of cookies and understand what they are, and of those individuals, only 73% regularly manage their cookie settings and the fact that, on average, a UK website sets 14 cookies per page (O'Malley, 2012); it looks like all parties have their work cut out for them.

Another piece of legislation currently being worked on by the European Commission is called "The Right to be Forgotten" Legislation, which is a part of a larger set of amendments to the European General Data Protection Directive. The proposed changes would give data subjects the ability to demand the erasure of their personal information by a data custodian if there was no longer a legitimate reason for keeping the information (Rosen, 2012).

The European Commission's Working Paper (2012) has identified several potential issues with the proposed legislative changes. As far as the "Right to be Forgotten" is concerned, the Commission has taken note of the fact that "in practice it is difficult for an individual to enforce this right vis-à-vis the data controller"[38]

38 European Commission. COMMISSION STAFF WORKING PAPER: Impact Assessment, *Accompanying the document:* Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, 25.1.2012. SEC(2012) 72 final. p30.

This comes as a result of several factors, most notable among them are: differing interpretations of the European Data Protection Directive by individual member states, difficulty for people to assess the data preservation policies of the data controller; this being a critical factor to the determination of whether the data is being maintained for a legitimate purpose in line with the original purpose of the collection; difficulties with the phenomenon of "data portability", which gives the data controller the ability to transfer all or parts of the personal data held to other entities; in the absence of a requirement of complete disclosure of all instances of data sharing or disclosure by the data controller, it would become next to impossible to effectively exercise the "Right to be Forgotten" if one is unable to determine all instances of the personal information that has been identified for deletion[39].

Critics of the changes to the European Commission's Directive have signaled that there would have to be certain limitation in place, as many individuals could potentially seek to erase all unflattering or negative references to themselves from the public domain. According to the European Commission's Vice-President Viviane Reding, the new law would propose that individuals be given the ability to request the deletion of personal information that they themselves have disseminated. While this narrower definition appears to be something that could actually be manageable and even logical, the actual text of the proposed legislation does not necessarily lend itself to as narrow a definition as proposed by Vice-President Reding.

As these proposals and amendments are only in their infancy, it remains to be seen the exact direction that will be adopted by the European Commission as to their enforcement and even the possibility of enforceability, two concepts which don't always go hand in hand.

39 European Commission. COMMISSION STAFF WORKING PAPER: Impact Assessment, *Accompanying the document:* Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Brussels, 25.1.2012. SEC(2012) 72 final. p30.

CHAPTER IV

THREATS TO PRIVACY IN THE CLOUD

Having laid the legal foundations for the privacy protection frameworks that exist in Europe and North America, it is probably worthwhile to ask a simple question: are threats to personal information and privacy a significant issue in today's society to debate the need for taking necessary steps to safeguard our privacy and data? After all, is the use of cloud computing significant enough to consider that such threats pose a significant risk to the security and integrity of personal information in the cloud? Given the rate of uptake by both private and public sector corporations, it seems that the issue is in fact very real and possibly a growing one.

A Pew Internet & American Life Project Memorandum poll conducted in 2008[40] found that 69% of American internet users have engaged in a form of cloud computing, using webmail services, storing data online or using cloud-based applications. Given the projected growth in the field of cloud computing, it would seem that the issues surrounding data security and migration of data into the cloud, especially for Government institutions is a real concern. With the cloud market value estimated to be heading towards record numbers as far as sales are concerned, it seems accurate that AMI Partners placed the estimate at "exceeding $95 billion by 2014, approx. 11 percent of total worldwide SMB ICT spending—indicative of a compound annual growth rate of 13 percent" (Hickey, 2010)[41]. Given the total value of worldwide investment in operating system software purchase pegged at $30.5 billion in 2010[42], the figures for cloud solutions show the magnitude of the issues on the horizon.

---

40 Pew Internet & American Life Project. http://www.pewinternet.org/reports/2008/use-of-cloud-computing-application s-and-services.aspx?r=1 *Accessed: 2012-04-28*

41 Hickey, Andrew, R. CRN. SMB Cloud Spending To Approach $100 Billion By 2014. http://www.crn.in/Software-019Aug010-SMB-Cloud-Spending-To-Approach-100-Billion-By-2014.aspx *Accessed: 2012-04-27*

42CIO Insight. Citing a Gartner Report. http://www.cioinsight.com/c/a/Latest-News/Gartner-Operating-System-Software-a-304-Billion-Market-in-2010 831284/ ?kc=rss&utm_source= feedburner &utm_medium=feed

With increasing numbers of decision makers in Government looking towards cloud computing adoption, it is inevitable that cloud security and privacy concerns will come to the forefront of the discussion. Given the increasing adoption of cloud computing by Government, we are precisely at a time when these issues need to be dealt with, as implementing remedies once data migration has been undertaken, while possible, are probably not nearly as effective at ensuring that the data is secure and that individual privacy is protected. Looking at statistics for current use and projected use by Government agencies of cloud-based solutions, we see that a significant increase has been observed year-to-year, with 8% more currently using web 2.0, 4% more currently at the implementation stage, 5% more at the investigation stage, contemplating adoption (1105 Government Information Group, 2012)[43].

The threats are very real, and the need to identify the nature of those threats as well as formulating strategies to mitigate against them is equally important. In order to fully appreciate the types of threats that are possible "in the cloud" we must remember exactly what cloud computing is. First and foremost, we must remember that a Cloud service provider in essence becomes a third party data manager (Dorey & Leite, 2011) for our organization or corporation, which is one of the primary underlying issues with this solution, when we apply it to personally identifiable information, it is no longer directly managed from within the client organization. Secondly, cloud infrastructure simultaneously supports different Service Delivery Models (SDMs) with each of the SDMs having their own and often unique security issues which are based upon their respective underlying technologies (Almorsy et al., 2011). These underlying issues are further complicated by two key characteristics of the cloud: multi-tenancy and elasticity which also yield additional worries for cloud clients (Almorsy et al., 2011). The security of various deployment models are further complicated by the fact that cloud computing takes a layered approach to provisioning of service. Each of the layers is intertwined with other layers, which means that the security of the whole is highly dependent upon the security measures

---

&utm_campaign =Feed% 3A+RSS%2Fcioinsight+%28CIO+Insight+Update+-+Ziff+Davis+Enterprise%29
Accessed: 20120-04-28

43 2012 statistics: 17% currently using, 21% at implementation stage, 52% investigating and 10% as interested.

deployed at each layer. This means that the whole can be negatively impacted by security weaknesses at any of the lower layers, which could be exploited to yield access to higher layers (Almorsy et al., 2011). The cloud ontology formulated by Yousseff et al. (2008) identified five distinct layers or characteristic of cloud infrastructure: the Cloud application layer – which provides users with access to the cloud, the cloud software environment layer – which gives cloud application developers access to an adaptive and scalable platform, the Cloud software infrastructure layer – which provides the computational resources like virtual machines, data storage and inter-layer communication enabling the development of cloud software environments and applications, the Software kernel layer – which provides software management in the form of an "OS kernel" or virtual machine and finally the Hardware and firmware layer – which consists of actual and physical hardware (Glott et al. 2010).

The realities of multi-tenancy are such that data storage and computing for several clients is happening on the same servers, using the same hardware and software, depending on need which is where elasticity comes in. The European Network and Information Security Agency (ENISA, 2009) has also identified "isolation failure" which refers to a breakdown of the mechanisms used to separate data during storage, memory and routing between tenants of the shared infrastructure. Multi-tenancy and the sharing of resources has been identified as a possible risk by the United States Government Accountability Office (2010), which stated that "one client could deliberately or inadvertent gain access to another customer's data, causing the release of sensitive information" (Karadsheh, 2012).

Potential threats can be divided into several categories, some of which are related to the human factor, mainly intentional attempts at breaching information, most notably through account hijacking or the activities of malicious insiders, as well as failures by service users to adequately safeguard their passwords and access credentials. A more important factor is the architecture and technology factor, which can result in more subtle yet potentially more dangerous breaches such as data leakage or seepage, failures in effective isolation of data as it resides on a server. Given the virtualization technology, which although impressive in its ability to resolve the issues of access to data is also at the heart of the problem, as client data can be moved about to various servers, even without their knowledge, therefore residing alongside data that has already been compromised or alongside data that has

been placed on the server for the sole reason of utilizing that servers computing power against itself to gain access to other data.

The final category of threat is something I have referred to as systemic threats, because they relate to the service providers and the system that they have created with regard to their product and the support for that product. Most notable limitation include: limitations of liability, service lock-in and the use of unique or proprietary software, which causes difficulties with data migration. More importantly however, the issue of data residency and jurisdictional matters has shown itself to me a big stumbling block. Service providers are reluctant to guarantee data residency, because this would have a detrimental effect on their ability to leverage resources and provide a high level of service. Guaranteeing data residency in accordance with the wishes of the client would also have a potential negative effect on the financial well being of Service Providers although very little exists in the way of statistics as to whether or not this would be a noticeable detriment.

These threats among others are examined in greater detail, as they have been identified as being 'common' to cloud computing infrastructure and a significant proportion of them have a direct tie in to data integrity and the preservation of privacy (Tripathi & Mishra, 2011):

Virtual Machine (VM) level attacks

Cloud computing is based on VM technology which utilizes hypervisors such as: VMWare, Microsoft Virtual PC, Xen etc. The threat arises due to vulnerabilities found in the deployed hypervisor technology and coding deficiencies. A subsequent issue identified in relation to VMs is related to the elasticity/scalability aspect of cloud services. VMs that are "archived and powered off for long periods of time" can cause security patch installation to fail (Litty & Lie, 2011).

Abuse and Nefarious use of cloud computing

This threat generally arises as a result of "relatively weak" registration systems in the cloud computing environment. The ease of procuring cloud services and the elasticity identified earlier lead to relative anonymity enabling spammers, malicious code authors and criminals to attack the system from within.

Loss of governance

Client cedes control over their data to the provider which could result in loss of control, breach of confidentiality, data integrity or availability of the data.

Lock-in

The use of proprietary technologies and solutions means that clients are unable to migrate data from one provider to another. This can also become an issue when data is to be migrated back to the client for deployment on client servers. Will the data revert back in a useable format given the proprietary technology used to store and process the information in the cloud? Currently, there are no standardized or commonly accepted frameworks between CSPs for data transfer between providers (Harding, 2010). This practice has been identified as hindering the development of sustainable "cloud ecosystems" and has been referred to as the "Hazy Cloud" phenomenon by some scholars and IT practitioners (Kuyoro, Ibikunle & Awodele, 2011).

Insecure interfaces and Application Programming Interfaces (APIs)

Customers use software interfaces and APIs to access cloud services. Given the expectations surrounding availability of cloud services as being "on-demand" accessible from various locations and using different devices, including mobile devices, this presents certain challenges in ensuring that the interfaces are secure. The utilization of unsecured networks, public networks and/or public or shared computers; could lead to the "interception of data in transit, poor application of authentication, communication encryption weakness or the absence of encryption" (Karadsheh, 2012). This results in an "increase in the number of points of access which threatens to compromise data integrity because of the increase in the number of parties, devices and applications involved" (Zissis & Lekkas, 2010)

Isolation failure

The components used to build disk partitions, CPU cache and graphics processing units do not offer strong compartmentalization of data. This weakness can lead to a couple of different scenarios of data breach and privacy breach: directed hacking attempts that would take advantage of the inferior compartmentalization of data, as well as breach due to "data remanence" (Zississ & LeLekkas, 2010), which is the residual representation of the data that has been moved, erased, removed or otherwise accessed. Malicious users have been known to claim large amounts of disk space and computing resources to scavenge for sensitive data (Zississ & LeLekkas, 2010). The potential for accidental data sharing between "virtual neighbors" or revelation of "user's activity patters" as well as the creation of "side channels" to gain access into restricted data is also a concern (Karn, 2011).

Data Loss or Leakage

Can occur as a result of "insufficient authentication, authorization, audit controls, inconsistent use of encryption, data center reliability, disposal challenges and disaster recovery" (Tripathi & Mishra, 2011) This threat is also related to the cloud computing architecture concepts of multi-tenancy and isolation failure (Kuyoro, Ibikunle & Awodele, 2011), among other possible design and management flaws that can be utilized to gain access to data stored in the cloud (Wang et. al. 2009).

Account or service Hijacking

Theft of credentials to gain access to critical systems or data itself, can lead to the compromise of the stored data or availability of the services themselves. This aspect is actually a dual-threat because it can relate to the both the CSP and the client. The hijacking of CSP credentials is potentially much more dangerous, as gaining administrator level privileges to the system managing the stored data opens up the possibility to gain access to the data of multiple if not countless users (Bhattacharya et. al., 2005). This threat is also related to insecure interfaces, which also increases the risk to user credential hijacking.

Management Interface Compromise

The accessing of resources and large amounts of data using web browsers can pose certain challenges, as web browsers are not immune from vulnerabilities. This is especially problematic given the fact that cloud computing is essentially a combination of "web applications and data hosting" and can result in threats like: phishing, compromised hosts running botnets, downtime, data loss password weakness (Karn, 2011).

Compliance Risks

Customers of CSPs do not have access to view the "processes, procedures and practices of the provider as they relate to areas of access, identity management and segregation duties" (Tripathi & Mishra, 2011). There is also a need to ensure that the CSPs data handling is legally compliant with that of the client. This doesn't necessarily have to mean identical legislation, but there is generally a clause indicating that the data must be afforded substantially similar protection in the jurisdiction where it is to be computed and stored (Karn, 2011).

Malicious Insiders

A considerable threat; given the level of access that many CSPs have to customer data. If the CSP has inadequate policies and controls to prevent or at least detect malicious activity originating from within, client data cannot be adequately protected or secured (Bhattacharya et. al., 2005).

Denial of Service or DoS attack

These types of attacks could violate privacy principles of access to information, notification, rights to correction of incorrect data, as well as deletion or blockage of illegally obtained or stored data (Bhattacharya et. al., 2005). This aspect is also central to one of the most advantageous features of cloud computing, that being "accessibility and usability on demand" (Zississ & Lekkas, 2010).

Limitations of liability

The terms and conditions of service level agreements generally contain clauses limiting the CSPs liability for service disruptions, data loss or breach, unauthorized disclosure or access, or privacy breach (Wernick, 2010). This could result in potentially devastating financial repercussions for the client (Calloway, 2012)[44]. "Hidden in these agreements are limitations of liability clauses, veritable safe harbors for cloud providers and submerged icebergs for the unwary cloud customer…a provider could purposefully delete its customers' data or shut down its users' website, leaving the aggrieved customers with no cause of action or right to recover" (Calloway, 2012). Financial burdens on the client could come from several directions, but in the context of privacy, Canadian legislation contains clauses enabling financial penalties for privacy breaches up to $500,000[45]. While limitations of liability built into Service Level Agreements (SLAs) is important, it is important to keep in mind that not all risk can be transferred even if an CSP accepts liability in the SLA, because "if risk leads to failure of a business, serious damage to reputation

---

44 "Domino's Pizza is currently working with Microsoft to host online pizza orders in the cloud. To date, Domino's has received over $1 Billion in sales through its website. Losing Service for even a few hours could effectuate losses in the millions of dollars". p171.

45 Queen's Printer Alberta. The Freedom of Information and Protection of Privacy Act (*FOIP Act)*. http://www.qp.alberta.ca/574.cfm?page=F25.cfm&leg_type=Acts&isbncln=9780779762071 *Accessed: 2012-04-27*

Offences and penalties 92(1) A person must not wilfully:

(a) collect, use or disclose personal information in contravention of Part 2, (b) attempt to gain or gain access to personal information in contravention of this Act, (c) make a false statement to, or mislead or attempt to mislead,
the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or other person under this Act, (d) obstruct the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or other person under this Act, (e) alter, falsify or conceal any record, or direct another person to do so, with the intent to evade a request for access to the record, (f) fail to comply with an order made by the Commissioner under section 72 or by an adjudicator under section 81(2), or (g) destroy any records subject to this Act, or direct another person to do so, with the intent to evade a request for access to the records. **(2)** A person who contravenes subsection (1) is guilty of an offence and liable to a fine of not more than $10 000. **(3)** A person must not wilfully disclose personal information to which this Act applies pursuant to a subpoena, warrant or order issued or made by a court, person or body having no jurisdiction in Alberta to compel the production of information or pursuant to a rule of court that is not binding in Alberta. **(4)** A person who contravenes subsection (3) is guilty of an offence and liable (a) in the case of an individual, to a fine of not less than $2000 and not more than $10 000, and (b) in the case of any other person, to a fine of not less than $200 000 and not more than $500 000. **(5)** A prosecution under this Act may be commenced within 2 years after the commission of the alleged offence, but not afterwards.

or legal implications, it's hard if not impossible for the other party to compensate for that" (Catteddu & Hogben, 2009).

Jurisdictional issues

Because of the composition of *SaaS* and cloud computing, clients must ultimately be aware of the architecture involved and the manner in which cloud services are provisioned in order to make informed choices about the suitability of the cloud for the storage of particular types of data. "in cloud computing, data can be stored anywhere" and the traditional thinking has suggested that users do not have a need to know exactly which location their data is being accessed from (Loganayagi & Sujatha, 2011) which I consider to be a gross oversimplification and a situation whereby cloud computing consumers are not treated seriously by CSPs. Many service providers take the position that the customer shouldn't care how it is delivered as long as the contracted service is available (Karn, 2011).

There are profound security and privacy concerns associated with data residency and jurisdictional issues in the cloud, because of the regulatory subjection of data to legal requirements in each jurisdiction. "Unlike local data centers residing in one country, cloud infrastructures often extend over multiple legislation and countries" (Glott et al., 2011). The applicability of law and safeguarding of the personally identifiable data is of critical importance. There are several scenarios for the manner in which a multitude of players enter the equation in this regard. Firstly, the cloud service provider may be sub-contracting their services to another provider, who could potentially also be sub-contracting their services further (Estevez & Rong, 2010). If the sub-contractors are not directly contracted by the "data custodian", their duties to maintain confidentiality of the data, becomes questionable at best. An example of such a scenario is the Amazon cloud, which allows other corporations to use their servers to run web applications and store their customer's data, "but claim the right to disclose this data under certain circumstances"[46] (Ozer & Conley, 2010).

In the absence of specific and detailed knowledge of the chain of providers and locations where the data may be stored or recalled from, the client risks failing to

46 The Amazon Web Services agreement states that "Amazon may disclose data to comply with …the request of a government or regulatory body, subpoenas or court orders".

meet their due diligence in ensuring security of the data. Cloud providers also rely upon “data redundancy” to ensure availability of data and computing ability. That means that the information uploaded gets copied several times on multiple servers to prevent down-time and lack of availability.

The server-chain that emerges can affect the personal information being stored, as the back-up servers are often located in much dispersed geographic locations and jurisdictions. According to the IT Law Group, (2011), “Cloud service providers want the freedom to move data to different servers for load balancing or to take advantage of the lower cost of utilities or personnel in different geographies. However, by doing so, they may inadvertently expose their customers’ data to the laws of countries other than those where the customer opted to operate”.

As a result of concerns over jurisdictional matters, many CSPs have established localized storage facilities to provide clients with greater control over the data residency issue. Amazon allows users to determine the location of their data, through facilities in both the USA and Europe (Armbrust et al. 2009), giving users the illusion of “greater freedom to place their storage” in an effort to neutralize fears of potentially invasive legislation like The US PATRIOT Act. Based on US case law, this would seem to be a false sense of security, as recent interpretations of data residency and jurisdiction have determined that even if the data is held outside the US, it is still subject to US laws if held by a US subsidiary subject to US laws (Bodle, 2012). In fact, it has now been realized that “the only way European companies can absolutely guarantee that their data doesn’t end up in the hands of US authorities is by choosing a provider that not only has a data centre within their jurisdiction, but is also owned by an organisation based in that jurisdiction” (Curtis, 2012).

Another cause for concern with regard to judicial interpretations and doctrines is the so called “business record doctrine” also referred to as the “third party doctrine”, which pre-dates decisions relating to the internet. The doctrine holds that when personal information is turned over to a third party business, in “relinquishing exclusive control” over the data, the data subject waives their reasonable expectation of privacy and Fourth Amendment protection and accepts full risk and responsibility for the potential voluntary disclosure of that information by the third party (Ozer & Conley, 2010).

What if the data storage is being handled in jurisdictions not known for high standards in terms of privacy protection, human rights, corruption or even provisioning of security? Many back-up service centres are located in South East Asia for instance and Transparency International (2007) has cited high corruption levels throughout the region as a crucial barrier towards adoption of e-Government and ICT (Nandan, 2008). While one issue is the integrity of CSPs and their subsidiaries, another important factor to consider is the fact that data is subject to Government scrutiny in many jurisdictions around the world. Another possible problem that can arise from the provisioning of the services of CSPs in exotic locations is the stability and security of the indigenous networks and infrastructure. Cybercrime statistics for the Asia-Pacific region have remained high with internet based criminal activities rising by 60% year-to-year and "virus incidents (82 percent) and insider abuse of network access (80 percent)...the most cited forms of attack or abuse" (Sembok, 2003).

LAWFUL ACCESS

One of the central threats to the integrity and security of information stored in the cloud is the ability of Government and Law Enforcement agencies to compel data to be turned over. There are varying degrees of the formalities that have to be met to compel CSPs to disclose information, depending on which legislation is invoked to compel disclosure. This thesis has already established that there are serious issues and questions surrounding data residency, jurisdiction and migration of data to other foreign storage facilities, thereby subjecting the data to the laws of the land. The Terms of service of all CSPs clearly state that they data can be disclosed to comply with law enforcement and have also admitted to having had to comply with such requests (Ozer & Conley, 2010) (Whittaker, 2011).

The provisions of the PATRIOT Act which enable access to 3rd party information behind the mire of secrecy and inability of CSPs to disclose that such disclosure has taken place, results in further distrust of the legal framework. In the absence of even the vaguest statistics, it's hard to say whether clients, both potential and existing should be assuming the worst case scenario, that the frequency with

which the PATRIOT Act is being invoked is high or low? It should be noted, that the PATRIOT Act is but one piece of legislation that can be utilized for gaining access to personally identifiable information. "In the United States, the legal statutes defining the range of entities that can be compelled to assist in electronic surveillance by law enforcement and foreign intelligence investigators are remarkably broad" (Soghoian & Stamm, 2010). Furthermore, The US Government and Law Enforcement agencies have few limitations to prevent them from spying on foreigners, both in the US and abroad (Soghoian & Stamm, 2010).

> "An order authorizing the interception of a wire, oral or electronic communication…shall…direct that the provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with the minimum of interference with the services that such service provider…is according the person whose communications are to be intercepted" (18 U.S.C. §2518(4))

It was revealed in 2006, that the United States Department of the Treasury had been accessing thousands of financial records of the Society for Worldwide Interbank Financial Telecommunications (SWIFT) relating to worldwide transactions (Solomon, 2010). In 2009, FBI raids on a datacenters in Texas resulted in the seizure of equipment at various facilities, belonging to both suspects and what has been called "innocent virtual bystanders" severely and in several cases completely limiting their ability to carry on operations (Karn, 2011).

Google's 2011 Transparency Report[47] indicates that a total of 15,744 requests had been received from Governments requesting access to user's personal information. These requests are not related to The PATRIOT Act, because that piece

47 Google Transparency Report 2011.
http://www.google.com/transparencyreport/governmentrequests/userdata/ *Accessed 2012-05-07*

of legislation prevents the disclosure of such statistics, but rather to requests that do not preclude the ability to inform data subjects that such a request has been received. A more accurate depiction of the scale of access requests to personal information may be the "Lawful Access" legislation in effect in the U.K. since 2007, which requires statistics to be kept and communicated to the Interception of Communications Commissioner. The statistics for the number of requests in the first two years are quite alarming, in 2007, 519,260 requests were received and approved, while in 2008 the number was down slightly to 504,073 requests (Whitehead & Kirkup, 2009)[48]. This translates into 1 in 78 adults in Britain having been under surveillance, with 1400 requests coming each day, that's one request every 60 seconds!

In late 2009, it was revealed that a large amount of information had been disclosed to US authorities, which had been excluded from the surveillance statistics that are reported to Congress. "Sprint Nextel provided law enforcement with over 8,000,000 hits from its customers' Global Positioning System (GPS) information between September 2008 and October 2009, and Cricket Communications received 200 requests for data each day (Parsons, 2012).

The far reaching effects of The PATRIOT Act can also be seen in Section 508 of that legislation, which specifically refers to records of the National Centre for Educational Statistics (NCES). The NCES primarily houses records related to primary and secondary schooling, which includes nursery and pre-school programs and related policy issues (Seltzer & Anderson, 2002). These statistics lead to the conclusion that requests compelling the production of personal information are much more common than suspected and have the potential to affect tens of thousands of individuals throughout the world, regardless of the nature of their activities or lack of "criminal" activity.

48 Whitehead, Tom & Kirkup, James. A request to snoop on public every 60 seconds. The Telegraph. http://www.telegraph.co.uk/news/uknews/law-and-order/6001357/A-reques t-to-snoop-on-public-every-60-seconds.html *Accessed 2012-04-25*

ELECTRONIC FOOTPRINTS

Additional information is also generated by cloud-based activities of users which can further compromise their personal information and privacy. The information and trails that are generated raise concerns when done independently, let alone when that information becomes correlated with other cloud computing activities. This linking of information could yield a great deal of information about the user, far more than was ever imagined or intended. Google Docs for example "records information such as account activity (e.g. storage usage...log-ins, actions taken) data displayed or clicked on (e.g. UI elements, links), and other log information (e.g. browser type, IP address, date and time of access, cookie ID, referrer URL)" (Ozer & Conley, 2010). When this aspect is combined with the provisioning of e-Government services, it becomes especially intrusive, given the wide array of activities that Governments engage in. The potential for data mining, phishing and electronic footprints to yield massive amounts of useful and personally identifiable data are quite extensive.

Present day realities of large amounts of data being compiled about internet user activities and identities, utilizing spyware and cookies while online has led to greater concerns for privacy than ever before partly due to the creation of "data shadows" (Gunnarsson & Ekberg, 2003). The use of these massive databases makes it easier than ever to establish individual's identities.

> "As databases play an increasingly important role in our lives, there is a danger that we will lose the ability to define ourselves, having surrendered the definition of ourselves to the data gathering entities, often unregulated and beyond our control" (Langenderfer & Miyazaki, 2009)

PROPONENTS OF THE "SECURITY OF THE CLOUD"

There has been some suggestion that the architecture of cloud computing actually aids in the provisioning of more sound security practices and mechanisms, thanks to the centralization of resources, making it a very secure solution that can even rival in-house server solutions that many corporations can afford. The cloud architecture itself; it has been argued: lends itself to "imposes a number of security benefits, which include centralization of security, data and process segmentation, redundancy and high availability" (Zississ & Lekkas, 2010). It would seem that the very same arguments being used to criticize cloud architecture as being inherently insecure are also touted as some of its best features. In fact, it is the architecture that results in a duality of roles, acting as both a strength and weakness when adopting cloud computing. According to Andrei, (2009) there are several architectural "cloud computing challenges"; some of which have already been identified earlier in this thesis; that have an effect on weakening privacy controls over PI information:

1. **Self-healing** – in case of application/network/data storage failure, there will always be a backup running without major delays, making the resource switch appear seamless to the user.
2. **SLA-driven** – service level agreements allow several instances of one application to be replicated on multiple servers
3. **Multi-tenancy** – multiple clients using the same hardware simultaneously
4. **Service-oriented** – cloud allows one client to use multiple applications to create its own
5. **Virtualized** – applications are not hardware specific, various programs may run one machine or many machines may run one program.
6. **Linearly scalable**: increases in data processing resources is handled linearly, if "n" times more users need a resource than the complete request time will be roughly the same
7. **Data management** – distribution, partitioning, security and synchronization of data

Ultimately, it must be realized that the centralization of these resources coupled with the centralization and pooling of data with a select group of CSPs makes the entire industry a prime target for hackers who can take advantage of the centralization of data from multiple corporations or Government agencies, therefore allowing hackers to make better use of their resources in pursuing the data (Esteves & Rong, 2010). Furthermore, given the ability to utilize the CSPs own infrastructure to perpetrate an attack, it seems all the more likely and plausible to occur. Several high profile attacks have been known to have occurred in this manner, most notably: Red and Blue Pill, Cloud Burst, Zeus botnet, Spam Attack and new targeted attacks such as the economic DDoS (carried out using the Amazon cloud). Attacks targeting the lower layers of the hypervisor servers are expected to become more frequent in the years to come (Delettre, Boudaoud & Riveill, 2011). Given high profile outages and successful hacks of large CSPs infrastructure, it would seem that no provider, or customer for that matter, is immune from these types of attacks (Esteves & Rong, 2010).

The threat from hacking is but one of the possibilities that could result in the compromise of sensitive personally identifiable data. It has already been discussed earlier, that there is also a distinct threat towards data integrity from the data mining and phishing activities of some service providers, a situation which would not be combated by CSPs that engage in such practices. Even transferred or deleted data continues to be of value to a third party, as a result of data redundancy, backups and data shadows (Delettre, Boudaoud & Riveill, 2011).

The relative lack of maturity of the cloud services market, which generally translates into high volumes of startups and an equal number of mergers and takeovers, which can drastically change Service Level Agreements (SLAs) and data residency, storage and backup realities (Strukhoff, 2010)[49]. Given the frequent intricacies of Service Agreements, sub-contracting, sub-storage contracts etc. "The bankruptcy any one member of that network could reverberate throughout this environment and impact remote participants in many indirect ways" (Caplan, 2010). In the event that such a situation arises, and there is a threat of a CSP ceasing operations, what will happen to the data that it was storing? Will it be protected in

49 Strukhoff, Roger. Gartner Analyst Says Cloud Computing "Immature" Yet Inevitable. Virtualization Journal. 2010. http://virtualization.sys-con.com/node/1292249 *Accessed: 2012-05-05*

any way? Will the CSP honor their agreements if they are going under? Will they sell their databases to the highest bidder?

According to the Bankruptcy Code 2005, several high profile cases that arose showed that the databases of sensitive and personally identifiable information were very valuable assets that other players in their respective industries were willing to pay top dollar for to acquire. Furthermore, some CSPs opted to sell their databases, despite earlier contractual obligations and privacy policies, having successfully claimed before the courts that they in fact owned the data once it came into their possession, giving them the ability to re-sell it (Caplan, 2010). This would be in keeping with interpretations from other jurisdictions (Australia) which have interpreted the transfer of personal information to be the equivalent of a “disclosure” of information to a separate entity (Solomon, 2010). Even if we accept the relative security of data stored and computed in the cloud from external hacking attacks; which has been shown to be a significant risk; we are still left with the risk arising from so called “lawful access”.

CHAPTER V

MITIGATING AGAINST THE RISKS TO PRIVACY

Cloud Computing risks have been identified by many scholars and practitioners in the field of privacy protection (Tancock, Pearson & Charlesworth, 2010), which has resulted in risk mitigation schemes and best practices having been put forward to assist both corporations and public bodies with the decision to "cloud or not to cloud". The most widely used tool for risk assessments in the field of privacy are Privacy Impact Assessments (PIA), which are a way for organizations to systematically address and identify privacy issues within information systems, while at the same time taking into account future consequences of a current or proposed action (Wright, 2011).

> "Risk management is a process that manages inherent risk, including fraud, non-compliance with laws, regulations, costs, competition and change by identifying: potential risk, potential impact of that risk on organization, controls that reduce the risk, quality of the controls, and possible impact of any residual risk" (Duff, Smieliauskas & Yoos, 2001)

One question that often arises is: when should a PIA be undertaken? Meaning, in what circumstances at what stage and does an organization need to complete a PIA? Ten criteria have been identified as warranting the completion of a PIA (Karol, 2001):

1. Major changes to existing programs
2. New programs
3. New delivery structures and partnerships
4. Changes in the technology
5. Additional systems linkages

6. Enhanced accessibility
7. Service monitoring
8. Delivery channel management
9. Data warehousing
10. Reengineering business processes

The underlying assumption being of course, that the project or system must be dealing with the collection, use or disclosure of personal information. There are several stages to the PIA process, including (Wright, Wadhwa, De Hert & Kloza, 2011), (Wright, 2011):

1. project initiation is to determine if a PIA is required. Is personal information being collected?
2. data flow analysis: examine how personal information will be collected, used, disclosed and retained.
3. privacy analysis: identification of the possible risks to privacy
4. privacy impact analysis: a discussion of the possible risks, associated implications and possible remedies.

Privacy protecting PIAs should be proactive, rather than reacting to issues that arise post-implementation. If privacy enhancing or privacy preserving characteristics are built into a system during the initial design and development stages, the risks to causing a privacy breach or incurring costs associated with retrofitting or having to redesign the system are minimized (Tancock, Pearson, Charlesworth, 2010). PIAs are currently utilised or mandated in several jurisdictions, most notably: Canada, the UK, the US, Australia, and New Zealand, with Canada being the only jurisdiction to make PIAs mandatory for all government institutions as of 2002 (Wright, 2011).

While these are the main steps in the implementation, this should not constitute the end of the process, as follow-up and compliance audits are necessary to ensure that the designed system is operating according to specs and that the privacy protection provisions contained within are effective. Accountability reports need to

be utilised to ensure that the implemented privacy protection provisions are constantly monitored and documented. These reports need to be completed through a joint effort of IT and records management professionals. The evaluation of controls and effectiveness can only succeed if subject matter experts are utilised (Duff, Smieliauskas & Yoos, 2001).

Three assessment methods have been identified: abstract, requiring an expert to drive the method, mid-level which requires a collaborative effort, whereby an expert is paired with "data owner" and concrete, which focuses only on the "data owner". The assessment methods follow several approaches like: temporal, which entails stress testing a system in real-time, functional, which performs threat analysis without actual systems testing taking place, and comparative, which compares the built system "against an explicit standard" (Abu-Nimeh & Mead, 2010). In order for these schemes to be effective, it's important to determine which of the methods and approaches are best suited to deal with assessments of the security risks and which focus on privacy risks.

Another important factor to consider is the need for PIAs to be completed especially when organizations and public bodies are dealing with cross-jurisdictional projects not only individual projects that are localized in the same geographic and jurisdictional area (Wright, 2011). This is of utmost importance, given the increasing number of projects that seek to take advantage of cloud computing, which often results in data migration to alternate jurisdictions. This is especially the case given that a Canadian audit of PIAs found that "little consideration had been given to projects involving the intra-institutional, inter-institutional and cross-jurisdictional flow of personal information" (Wright, 2011). There is a series of questions and issues that must be addressed when conducting a PIA for a cross-jurisdictional cloud computing solution, which will result in personal information being migrated, shared or otherwise computed in the cloud environment. Eight critical principles have been put forward to effectively deal with cross-border privacy impact assessments (Karol, 2001) (*See Appendix 1*):

1. Organizational responsibility for the ownership of personal information (PI); 2. Identifying the purpose for which the PI is kept;

3. Limiting data collection to business objectives; 4. Required consent; 5. Limitations on the retention of PI information; 6. Accuracy of data; 7. Data security; and, 8. Training and communication.

For each of the principles, a series of questions, which delve progressively deeper into each of the aspects needs to be asked and answered in order to arrive at a fully informed decision as to whether or not the intended cross-border migration of data is fully compliant with jurisdictional and data security requirements. It is imperative that the questions are answered in a comprehensive and truthful manner

As a result of the lack of international standardization for the PIA process, with "critical variations in implementation of PIAs" (Tancock, Pearson & Charlesworth, 2010) across various jurisdictions, the principles listed above are of critical importance, to ensure that all issues in the myriad of legislative and jurisdictional differences have been addressed. Tancock Pearson and Chalesworth (2010) have proposed the creation of a PIA tool as a kind of "decision support system", which would rely on the input from subject matter experts. What's more, the PIA tool would itself be a cloud-based (*SaaS*) application relying on a knowledge base (KB) that would be populated, on an on-going basis by subject matter experts from across all of the jurisdictions that utilize PIAs. The tool would be accessed by "end users" via a Web User Interface, where the PIA tool would prompt the user to answer a series of contextually generated questions. Based on the initial questions, the tool would then prepare a project profile with more detailed questions that would form the final PIA.

The idea of an omnibus PIA tool is interesting, but implementation remains very unclear. Who would be tasked with providing the expert content for the KB? Who would be maintaining it and ensuring that it is up-to-date? What if legislative changes are not captured by the tool, leading to faulty assessments and questions being asked? Is it even feasible that a single application could capture all of the different legislative intricacies involved across multiple jurisdictions? In the US, there are 50 States with differing privacy legislation, as well as other pieces of legislation that contain sections that deal with privacy as well, as was shown by the

example of California State Law. In Canada, there are 10 Provinces that have differing, although similar, privacy legislation, including Federal legislation. Only the EU can truly boast a fully uniform Privacy Legislative system, because the Directives undertaken by the European Parliament and Commission apply to all member states, yet discrepancies in the implementation and interpretation of the directives have been observed in the past. The authors state that to their knowledge, no such solution currently exists, their proposal being a pioneer in the field of PIAs. That may be as a result of the impossibility of the undertaking, given the differences and intricacies of the legislative frameworks.

A different approach that has been characterized as being complimentary to traditional PIAs is the concept of Privacy by Design (PbD), "strongly advocated by the Canadian privacy commissioner (Ontario) Ann Cavoukian. The origins of PbD can be traced back to a 1995 report by the Dutch data protection authority and the Canadian privacy commissioner" (Lieshout, Kool, van Schoonhoven & de Jonge, 2012). The PbD framework establishes a set of best practices for the implementation of privacy enhancing characteristics into Cloud computing architecture (Cavoukian, 2010).

1. Proactive not Reactive; Preventative not Remedial – the framework seeks to anticipate and prevent privacy invasive events before they occur. It is not about providing remedies for privacy infractions after the fact.
2. Privacy as a Default – the delivery of a maximum degree of privacy by ensuring that the data is automatically protected in any given IT system or practice. User decisions should not focus on whether or not to protect certain information but rather how much protected information they wish to allow more access to.
3. Privacy Embedded into Design – privacy protection features should be embedded into the design of the system rather than being retrofitted post implementation.
4. Full Functionality; Positive-sum not Zero-sum – accommodation of all legitimate interests and objectives rather than trade-offs and false dichotomies of privacy vs. security.

5. End-to-End Lifecycle Protection – by including the privacy mechanisms in the design, complete lifecycle management of information is guaranteed, from the moment PI is first collected to the time the system is decommissioned and data is securely destroyed.
6. Visibility and Transparency – components need to remain visible to enable verification of their proper operation, subject to independent verification.
7. Respect for User Privacy – the systems need to remain user-centric, offering strong privacy, appropriate notice and user-friendly options.

The original concept of PbD relied heavily on the promotion of the implementation of Privacy Enhancing Technologies (PETs) (van Blarkom and Borking, 2001, Borking 2010). PETs have been broken down into four separate functionalities, each with a distinct focus; the aim of all of being protecting personal privacy (Burkert, 1997):

1. Subject oriented PET: aim to anonymize a data-subject or to offer a pseudo-identity
2. Object-oriented PET: aim to conceal what is exchanged
3. Transaction-oriented PET: aim to conceal occurrence of a transaction
4. System-oriented PET: any combination of the previous three orientations

Cvrcek and Matyas (2007) have gone further in characterizing the aims of the functionalities as providing:

1. Anonymity
2. Pseudonimity
3. Unlinkability: meaning the items do not appear to be related
4. Unobservability: items of interest are indistinguishable from other items

All of the characteristics and functionalities combined form a more decisive privacy protecting and privacy enhancing mechanism. They are also key players in the strategies and techniques for mitigating privacy risks in cloud computing environments, which have been characterized as being "disruptive innovation which challenges norms and forces out-of-the-box thinking…as individual or enterprise-level consumers shy away due to data security and/or privacy concerns" (Cavoukian, 2010). It is undoubtedly the case that the implementation of data security and privacy mechanisms, cloud providers can alleviate many of the fears and concerns communicated by both industry and government as the main barriers towards the adoption of the technology.

A recent IBM survey found that 77% of respondents believed that the adoption of cloud computing makes protecting privacy more difficult and 50% expressed concern about data breaches and loss (Coleman, 2011). These perceptions should be clear indicators for the direction that the CSP industry needs to take, in order to ensure greater uptake of the technology and provide "assurance that providers are following sound security practices in mitigating the risk facing both customer and the provider" (Catteddu & Hogben, 2009). Yet that has not been the case, as we see the identification of issues surrounding the adoption of schemes like PbD, which pose serious barriers towards its adoption by CSPs (Lieshout, Kool, van Schoonhoven & de Jonge, 2012):

> "However, the implementation of such a holistic approach is not easily realized. A potential lack of economic incentives, legacy systems and a lack of clear view of the benefits are considerable barriers for the adoption of PbD solutions by organizations"

Privacy by Design has been identified by industry leaders as a very probable direction in the future, as it is realized that offering embedded privacy in systems can become a "market differentiator for companies; respecting privacy by default and empowering customers to control their personal data can be a strong business

proposition" (Knutson, 2007). But in order for this process to be legitimate and trustworthy, CSPs must ensure that there is greater transparency and accountability from the industry and that documented processes and practices are in place. In a recent study of the security assurances of the cloud provided by CSPs, Chakraborty et al. (2010) discovered that most of the security and privacy claims have been based "purely on the size of the organization" (Dorey & Leite, 2010) rather than actual security policies, protocols and technological solutions.

TECHNOLOGICAL AND SYSTEMIC SOLUTIONS

A variety of tools and mechanisms have been proposed to ensure that personal information remains secure and protected. None of the solutions alone can stand up to the multitude of risks that have been presented as emerging from the very fabric of cloud computing architecture. Assuming that encryption alone is the answer to a secure solution that will prevent personal information from being breached or otherwise subjected to unauthorized access would be a mistake.

Ten security criteria have been identified to ensure the optimal database security (Delettre, Boudaoud & Riveill, 2011):

1. User identification and authentication – In a safe and unambiguous manner.
2. Identification of robustness and authentication – Making it difficult to usurp or hijack identities.
3. Rights separation – Distinguish types of users and their predefined actions and privileges.
4. Data Access Control – Allowing for various types of access only to authorized users.
5. Integrity and Confidentiality of the stored data – Ensure only authorized users can read or modify the stored data.
6. Communication ciphering – Ensure the integrity and confidentiality of requests and data exchanges between various equipments implementing or using the database.

7. Data concealment- Concealing real data in false data to conceal the actual volume of data.
8. Data masking- Use irreversible processes to replace sensitive data and ensure that the original data cannot be restored.
9. Audit services- Log all events concerning access to the DBMS and ensure integrity of the logs.
10. Certification- Evaluation Assurance Level (EAL) certification that allows for evaluation of IT applications.

There is currently a multitude of technological and some systemic tools that could be leveraged to address the issues raised, to ensure an adequate and optimal level of database security and as a result security of the personal information within those databases. These tools include, but are not limited to:

Multi-factor Authentication

The implementation of strict registration and multi-factor authentication processes, including encryption, will minimize account hijacking and credential usurpation (Zissis & Lekkasm, 2012). The implementation of strong compartmentalization needs to be employed to reduce likelihood of unauthorized access, both accidental and targeted to the data of one customer by another. This is closely tied to the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) and the use of strong firewalls on virtualized machines (Tripathi & Mishra, 2011).

Privacy Violation Detection and Monitoring

One proposed system that accomplishes IDFS/IPS tasks and has been successfully tested is called Privacy Violation Detection and Monitoring (PRIVDAM). The system utilizes data mining techniques to search for anomalies. In order to do this, the system relies upon the creation of positive and negative access patterns as the basis for comparison to expose anomalies which will be identified as privacy violations (Bhattacharya, 2005). The system therefore requires two inputs to accomplish its task: 1) an audit log of events in the host, application, database or network, and 2) the privacy policy and agreements with user profiles and/or signatures (Krekke, 2004).

Data Encryption

Encryption of data, both in transit and at rest, needs to be utilized to ensure greater security. However, this is something that is not common in the industry today because encryption would prevent the ability to index and search the data (Mowbray, Pearson & Shen, 2010). Recently developed schemes like Predicate Encryption and Private Information Retrieval (PIR) have addressed the issue of indexing and search ability of cipher-text, enabling the performance of computations on encrypted data without decrypting (Chow et al., 2009). Another example of this technology is the Public encryption with keyword search (PEKS), which enables the searching of encrypted data for certain keywords by the gateway, without having the gateway learn anything more about the content of the data itself (Boneh, Ostrovsky, Crescenzo & Persiano, 2004). It is also possible to use a combination of asymmetric and symmetric cryptography, which would result in a "best-of-both-worlds" scenario whereby full advantage is taken of the efficiency of symmetric cryptography and the security of asymmetric cryptography (Zississ & Lekkas, 2012)

Privacy Manager

A relatively new approach to ensuring privacy in cloud computing is the use of a "Privacy Manager", which utilizes a process called "obfuscation" to carry out a type of "encryption" of data to be uploaded using a key that is chosen by the user and known to the Privacy Manager. The key is never known to the CSP, therefore preventing the de-obfuscation of the data while in storage, theoretically eliminating the risk of theft or unauthorized access. A very interesting and promising aspect of obfuscation is that the data is not personally identifiable, which could enable greater flexibility with the selection of providers and storage location (Mowbray, Pearson & Shen, 2010).

Trusted Third Party (TTP)

This is sometimes referred to as a "Trusted Third Party" (TTP), who acts as an intermediary and assists in watching over the secure handling of customer information. Furthermore, a TTP "supplies the technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction" (Zissis & Lekkas, 2012). TTPs can assist with: Low and High level confidentiality, Server and Client Authentication, Creation and Security of Domains, Cryptographic Separation of Data and Certificate-Based Authorization (Zissis & Lekkas, 2012). The TTP scenario has given rise to a new offering in the area of Identity and Access Management (IAM) called Identity as a Service (IDaaS), which utilizes the third party facilitator as a go-between Service Providers, Identity Providers and Users as an additional layer that is able to process and interpret "multiple forms of Identity and Authorization management" (Dorey & Leite, 2011). Given the relative infancy of the concept of IDaaS, it remains to be seen whether an entire industry actually emerges from this idea.

Data Concealment

Another technique which enhances data security and privacy protection while at the same time making the data less valuable to potential hackers or miners is data concealment. This is accomplished through the insertion of artificial data into the real data, thereby making the process of data mining more difficult with potentially flawed and useless results being generated. The artificial data generated must be of a similar type to the original data so that it does not stand out, and it must be inserted in real time. The data custodian must be able to quickly differentiate between the real and artificial data (Delettre, Boudaoud & Riveill, 2011).

Data Ambiguity and PriView

The data ambiguity technique enables the protection of both "presence privacy" and "association privacy" by hiding and breaking down the quasi-identifier (QI) values associated to the data. This technique may not be well suited to all types of data however, as it can result in some "negligible" data loss, something that may not be a reasonable risk as far as the data integrity is concerned (Wang, 2010).

Anonymity based method

This method proposes to run all personally identifiable data through an anonimization algorithm, stripping the data of personal QI, which would result in there no longer being a need to protect the anonymized data. It goes further to say that CSPs could freely mine such anonymized data, as there would no longer be a risk to personal privacy (Wang, Zhao, Jiang & Le, 2009). Given the level of information sharing and flow as well as cross referencing of multiple databases, possibly in several jurisdictions, this approach may not prove to be as effective as envisioned. The stripped QI could foreseeable be reintroduced into the data set from other sources, once again making the data identifiable. Location-based tracking systems (LTSs) could render this method insufficient as "the centralization of aggregated information and the combination of location information with other personal information" can lead to de-anonymization. At the present time, there are no laws limiting the use of LTS technology, which has increased the risks to privacy and security of individuals (Wang & Loui, 2009). Nonetheless, depending on the nature and sensitivity of the data, it may be a concept worth exploring for implementation of e-Government initiatives.

Perimeter Protection, Trusted Zones and Federated Clouds

As a result of the difficulties of perimeter security in enterprise applications, CSPs need to establish zones of trust, making the virtual machines (VM) "self-defending" thereby moving the location of the perimeter to the VM itself (Trend Micro: Cloud Computing Security, 2009). By organizing Cloud infrastructure into distinctive security domains, it is possible to create a "collection of single clouds that can interoperate i.e. exchange data and computing resources through defined interfaces…each single Cloud remains independent but can also interoperate with other clouds" (Zississ & Lekkas, 2012) also referred to as Federated Clouds. Trusted Zones on the other hand can be used to achieve better isolation of data and applications at the network, device or application level (Durbin, 2011).

Certificate based authorization and SSL Certificates

Due to the non-traditional relationships between resources and users in a Cloud environment, the management of identities and permissions is more difficult. A scheme that has been developed to make identity and permissions management more attainable is the issuance of certificates by a third party Public Key Infrastructure (PKI) facility that would act as an intermediary in enforcing access control through web portals. The certificates carry with them a combination of attribute-value pairings and information about the principals to whom they apply (Zississ & Lekkas, 2012).

SSL Certificates on the other hand are used to provide certification status to portals and services online, thereby communicating to users that their information is being handled by a secure partner, certified by one of the Certificate Authorities (CAs) (Connolly, 2008). The CA is responsible for verifying the identities of partners to whom they grant certification. The SSL encrypted connections help to secure millions of internet transactions daily. While this scheme has provided a certain degree of security as far as trust is concerned in the processing of data, especially financial data over the Web, it is not without weakness. Depending on the level of certificate purchased, the identity verification may be severely limited, and require nothing more than a reply to an email to establish administrative privileges (Connolly, 2008)[50]. In addition to failing to meet the OECD Guidelines, there have also been examples of "compelled assistance", where Governments have successfully compelled companies to "violate their customer's privacy-providing the Government with email communications, telephone calls, search engine records, financial transactions and geo-location information" (Soghoian & Stamm, 2010)[51]

50 The office of the Information and Privacy Commissioner of Ontario and Australia's federal Data Protection Commissioner conducted a joint study comparing privacy criteria of the three most popular seals – TRUSTe, BBBOnLine and WebTrust – against the OECD Guidelines. In our opinion, none of these seal programs…fully met the standards of the OECD Guidelines. The common deficits were no requirements to: 1) limit collection, 2) ensure data was relevant to the purposes; 3) provide information to the data subject in reasonable time and manner, without excessive charge, and in an intelligible manner; and 4) provide reasons for the denial of access".

51 Examples of compelled assistance include "a secure email provider that was required to place a covert back door in its product in order to steal users' encryption keys, and a consumer electronics company that was forced to remotely enable microphones in a suspect's automobile dashboard GPS navigation unit in order to covertly record their conversations. The Chinese Government, for example, has repeatedly compelled the assistance of telecommunications and technology companies in assisting with its surveillance efforts".

Information Security Management

In order for any of the potential solutions to data integrity and privacy protection listed above to be effective, it's important that organizations identify and implement Information Security Management Systems (ISMS), which are systems that provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets (Almorsy, Grundy & Ibrahim, 2011). There are three main phases to the implementation of such systems:

1) Defining security requirements – including identifying security goals/objectives, conducting risk analyses and detailing those risks in the security policies.
2) Enforcing security requirements – identifying security controls to be used and implementing and configuring those controls based on the identified requirements.
3) Monitoring and improving security – including current status, existing issues and improvements to current security controls.

There are consequently four requirements of successful ISMS systems for Cloud Computing scenarios: customers must be allowed to specify their security requirements, customers must be able to monitor their assets security status as well as the status of the underlying platform, multi-tenancy based on strong isolation of customer data and finally, they must be based on already existing security management standards of both the customer and the CSP (Almorsy, Grundy & Ibrahim, 2011).

In order for a successful ISMS to be implemented and in order for it to function properly, both the client and CSP must strive for a common understanding and the building of a "quality" relationship and system. Some definite indicators of the lack of quality in such a system have been identified, with the first three having a direct connection to security and privacy concerns (Menkus, 2001):

1) Lack of realism in administering the application of computing.
2) Lack of reliability in the operation of the continuing specific aspects of the organization's investment in computing.
3) Lack of trustworthiness in the performance of the actual application. In the computing environment there is no such thing as acceptable error or relative accuracy. If the data being considered is not absolutely correct then it is absolutely wrong.
4) Lack of well defined profitability in computing activities.

Realism in the administration of the application of computing is critical, otherwise the potential exists for the client and CSP to be agreeing to very different levels of service and protection without taking into account the realities of what is possible and what is merely a wish. The realities and expectations of the security requirements of the client must be presented to the CSP, and adequate "assurance that providers are following sound security practices in mitigating the risk facing both customer and the provider" (Catteddu & Hogben, 2009). CSPs have been urged to adopt newly emerging approaches to the security of information systems, which are quite different than traditional security systems.

These include: Security-as-a-Service (SECaaS) and Data protection and privacy-as-a-Service (Ristov, Gusev & Kostoska, 2012). SECaaS utilizes the provisioning of security resources through the cloud to the infrastructure or software itself or to the customers' own systems (Cloud Security Alliance, 2011). The interest in and uptake of SECaaS appears to be on the rise, with predictions that cloud-based security service will triple in many segments by 2013.

These security management expectations need to be communicated to the CSPs during the negotiation of the Service Level Agreement (SLA) to enable organizations to maximize the security and management of their records in the Cloud (Katharine & David, 2010). Once these assurances have been secured and documented, CSPs must allow for independent 3rd party audits of their systems to take place, to provide for an unbiased assessment of the security procedures and mechanisms as well as their effectiveness or real life performance (Wright, 2011).

Only this way can we achieve the trustworthiness in the functionality of the application as well as the CSP operating it.

When conducting audits and assessments, it's important to take into account the assessment of the quality of the system that has been designed or implemented, which can be realized using one of the following approaches (Menkus, 2001):

1. Identifying and abandoning any product or service that fails to conform to the applicable measure of its condition or performance
2. Constructing a product or service development and operation setting in which the lack of quality is not tolerated.

Once an audit or assessment has been completed and if it has identified deficiencies in either the operation or the design of the system, appropriate steps must be undertaken to ensure that personally identifiable information is not being compromised or is not at risk of being compromised. If such a situation is discovered however, the system must be repaired or abandoned to prevent a privacy breach from occurring or continuing, if discovered after the fact. This scenario could prove to be very challenging if the assessment is being done on a Cloud-based system, as abandonment of the application may result in abandonment of some or all data migrated into the cloud as well (Caplan, 2010).

CONCLUSION

After examining the security of personal information in a cloud computing environment, I focused on the potential risks to the security and privacy of personally identifiable data in a *SaaS* architecture platform. First, I defined the concepts of Privacy, e-Government, EAS and applicable Legal Frameworks, setting the stage for the exploration of ***the threats to the security of personal information in SaaS "cloud-based" applications for Enterprise Application Systems (EAS) e-Government initiatives.*** I identified potential risks to privacy and security of personal information in the Cloud, both from a legal standpoint (pp35-39) and the technical/architectural (pp48-53) and I propose strategies for mitigating against those threats (pp70-74).

I pointed out significant threats to data security and privacy and addressed some ***shortcomings of the methods currently proposed for identifying and mitigating against the risks to privacy in applications (pp62-68).*** I recommend the use of a comprehensive PIA tool (Appendix 1), which will assist organizations to minimize the risks to personal information and to enable them to demonstrate their due diligence. This tool will guide organizations through the myriad of questions that must be asked and answered before a final decision is made as to whether or not the Cloud is suitable for the information at hand.

In conclusion, I believe that ***the deployment of EAS on the cloud using the SaaS platform does not offer adequate safeguards and does not substantially minimize the risks that are associated with the SaaS platform.*** In fact, such a deployment can actually result in a false sense of security. A sense of security, which cannot be guaranteed or reconciled because of the architecture and inherent weaknesses of that deployment model as it relates to data security and privacy protection.

As Governments all over the world move an increasing number of services and communications platforms to the cloud in search of easier access, greater reach and cost savings, it is of utmost importance that privacy is adequately addressed. As a result of the very personal and potentially sensitive personal information being collected and handled by Governments; and in meeting the regulatory and legal limitations placed on public bodies in many parts of the world; adequate attention

must be paid to ensure that Governments are not willingly and intentionally breaching or compromising individual privacy by migrating services to the Cloud.

The most common choice for deployment has traditionally been *SaaS*, which at the same time offers the least amount of control over the application or data being collected and stored. As such, I have discovered that the nature of cloud architecture is of central importance, given its multi-layered composition which could introduce threats and weaknesses at any of the layers.

I propose a safer path down Cloud adoption, especially for Government agencies, which is founded upon thorough and exhaustive risk assessments. These assessments are of critical importance and must be undertaken especially in light of the risks and relative deficiencies of currently existing methods and strategies for ensuring data security. This project is important because it has drawn together research from several fields and sources, analyzing them to arrive at this conclusion. Furthermore, I also conclude that a complete elimination of the risks to personal information is highly unlikely; especially given the complexity of the multi-layered infrastructure, technological limitations, and the human factor. Only through the utilisation of the identified risk mitigation tools and strategies, “due diligence” on the part of the organisation will have been met.

Responsibility for the protection of individual privacy ultimately rests with the records custodian that has collected and is using or storing the information. The driving factors for the adoption of e-Government: efficiency, democracy and effectiveness must not become a trap that leads to the compromise of individual privacy, as it will most likely result in the exact opposite effects, mainly the failure to achieve greater efficiency and effectiveness as people will lose trust in the system and will be reluctant to take advantage of e-Government services out of fear. Governments must therefore examine the types of data that are appropriate for the Cloud environment, given the lack of transparency and many unknowns in the industry as outlined in this thesis. They must be able and willing to discard the Cloud as a computing solution if: the nature of the data is sensitive, CSPs are unwilling or unable to provide satisfactory guarantees as to the security and audit-ability of their operations, the PIA and risk assessments have identified potential risks that cannot be mitigated against, and data residency and jurisdictional issues cannot be resolved.

“Whether data owners purchase $150 worth of processing capacity for the day or spend millions of dollars on a five-year IT outsourcing contract, they still have ultimate responsibility for their corporate information. And it is they that will be held to account if things go wrong and they find themselves in breach of the current morass of legislation and regulations in this area” (Everett, 2009)

GLOSSARY

(BPR) Business process reengineering -	Business process re-engineering is the analysis and design of workflows and processes within an organization, performed to achieve a defined business outcome.
(EAL) Evaluation Assurance Level -	The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation. The EAL level states at what level the system was tested.
ENISA - European Network and Information Security Agency -	The objective of ENISA is to improve network and information security in the European Union. The agency contributes to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the European Union, and consequently will contribute to the smooth functioning of the EU Internal Market.
(ESA) Enterprise System Applications -	Enterprise software describes a collection of computer programs with common business applications, tools for modeling how the entire organization works, and development tools for building applications unique to the organization.
(FOIPPA) Freedom of Information and Protection of Privacy Act	referred to as FOIPP in BC and FOIP Act in Alberta
(GPS) Global Positioning System -	is a space-based satellite navigation system that provides location and time

	information in all weather, anywhere on or near the Earth, where there is an unobstructed line of sight to four or more GPS satellites.
(HEW)	Department of **Health, Education and Welfare (U.S.)**
HIA - Health Information Act (Alberta)	
(IAM) Identity and Access Management -	Identity management (IdM) is a term related to how users are authenticated (identified) and authorized across computer networks.
(ICT) Information and Communication Technology -	refers to the merging of audio-visual and telephone networks with computer networks through a single cabling or link system.
(IDFS) Intrusion Detection Systems -	is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station
(IPS) Intrusion Prevention Systems -	The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity
(ISMS) Information Security Management Systems -	An information security management system (ISMS) is a set of policies concerned with information security management or IT related risks.
(KB) Knowledge Base –	A reference library for privacy legislation in various jurisdictions. Proposed by Tancock et al. For the cloud-based PIA Tool.
NCES -	National Centre for Educational Statistics (U.S.)
(OECD) Organization for Economic Co-operation and Development -	It is a forum for member states to compare policy experiences, seek

	answers to common problems, identify good practices, and co-ordinate domestic and international policies of its members.
(PAR) Performance/ Availability/Reliability –	refers to the assessment criteria for applications.
(PATRIOT Act)	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (U.S.)
(PEKS) Public encryption with keyword search –	technology that enables the searching of encrypted data for key words.
(PET) Privacy Enhancing Technologies –	refers to computer tools, applications and mechanisms which - when integrated or used in conjunction with online services or applications, allow users to protect their privacy and integrity of their personally identifiable information.
(PIA) Privacy Impact Assessment -	is a process used to determine how a program or service could affect the privacy of individuals, by identifying data flows, access permissions, security features and possible threats to privacy as well as providing mechanisms to mitigate against those threats.
PIPEDA -	***Personal Information Protection and Electronic Documents Act*** (Canada)
(PIR) Private Information Retrieval –	is protocol that allows users to retrieve an item from a server in possession of a database without revealing which item is being retrieved.
(PKI) Public Key Infrastructure -	is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. PKI associates keys with user identities.

(QI) quasi-identifier –	Information that is not personally identifiable on its own, but contains enough information to yield identity when combined with other identifying information. Examples of common quasi-identifiers in the context of health information are: dates (such as, birth, death), locations (such as, postal codes, and regions), race, ethnicity, languages spoken, profession, and gender.
(SWIFT) Society for Worldwide Interbank Financial Telecommunications -	provides the network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment.
(TTP) Trusted Third Party -	is an entity which facilitates interactions between two parties who both trust the third party; The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content.
URL -	In computing, a uniform resource locator (URL) is a specific characteristic string that constitutes a reference to an Internet resource.
OS kernel -	A kernel is a central component of an operating system interface between the user applications and the hardware. The sole aim of the kernel is to manage the communication between the software (user level applications) and the hardware (CPU, disk memory etc).
Cookie -	A cookie, also known as an HTTP cookie, web cookie, or browser cookie, is a piece of data stored by a website within a browser, and then subsequently sent back to the same website by the browser. The cookie is placed on the visitor's hard drive and reports back to the host website certain information that the cookie has been programmed to collect and communicate.
CPU cache -	is used by the central processing unit of a computer to reduce the average time

	to access memory. The cache is a smaller, faster memory which stores copies of the data from the most frequently used main memory locations
CSP –	Cloud Service Provider
DBMS Database Management System -	is a software package with computer programs that control the creation, maintenance, and use of a database.
DoS and DDoS -	a denial-of-service attack or distributed denial-of-service attack is an attempt to make a computer or network resource unavailable to its intended users.
FBI –	Federal Bureau of Investigations
IP address –	Internet Protocol Address - is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network. It has two principal functions: host or network interface identification and location addressing
IPX/SPX -	stands for Internetwork Packet Exchange/Sequenced Packet Exchange. The SPX layer sits on top of the IPX layer and provides connection-oriented services between two nodes on the network.
LTS technology –	location-based tracking systems - allows for quick and accurate location of assets or individuals.
PbD - Privacy by Design -	framework for systems design where privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal
PI – Personal Information –	information that contains identifiers associating it with an identifiable individual.
SaaS – Software-as-a-Service -	is a software delivery model in which software and associated data are centrally hosted on the cloud. *SaaS* is

	typically accessed through a web browser.
SLA – Service Level Agreement -	records a common understanding about services, priorities, responsibilities, guarantees, and warranties.
SMB ICT –	small-medium business information and communications technology.
SNA or SSL Certificates -	the Secure Socket Layer protocol was created to ensure secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one or both ends of the transaction.
TCP/IP -	The Internet protocol suite is the set of communications protocols used for the Internet and similar networks.
UI -	The user interface refers to the field of human-machine interaction where interaction between humans and machines occurs.
VM technology -	A virtual machine (VM) is a software implementation of a machine that executes programs like a physical machine.

BIBLIOGRAPHY/REFERENCES

1105 Government Information Group. Mainstreaming Cloud Computing. January 2012.

Abu-Nimeh, Saeed & Mead, Nancy. Privacy Risk Assessment in Privacy Requirements Engineering. Second International Workshop on Requirements Engineering and Law. 2010.

Almorsy, Mohamed, Grundy, John & Ibrahim, Amani. Collaboration-Based Cloud Computing Security Management Framework. 2011 IEEE 4th International Conference on Cloud Computing. 2011.

Amazon Web Services. Overview of Security Processes. September, 2008.

An Oracle White Paper. Cloud Candidate Selection Tool: Guiding Cloud Adoption. December, 2011.

Andrei, Traian. Cloud Computing Challenges and Realted Security Issues.WUSTL. 2009.

Armburst, Michael, et al. Above the Clouds: A Berkley View of Cloud Computing. Technical Report No. UCB/EECS-2009-28. 2009.

Ausloos, Jef. The 'Right to be Forgotten' – Worth remembering? Computer Law and Security Review 28. 2012.

Axelrod, Warren, Bayuk, Jennifer & Schutzer, Daniel. Ed. Enterprise Information Security and Privacy. Artech House. 2009.

Beresford, Alastair & Stajano, Frank. Location Privacy in Pervasive Computing. Security and Privacy. IEEE CS and IEEE Communications Society. 2003.

Bhattacharya, Jaijit, et al. PRIVDAM: Privacy Violation Detection and Monitoring Using Data Mining. Ahmedabad: Indian Institute of Management. 2005.

Barnatt, Christopher. A Brief Guide to Cloud Computing: An Essential Guide to the Next Computing Revolution. Constable & Robinson. 2011.

Blandford, Richard. Information Security in the Cloud. Network Security. April, 2011.

Blauer, Fred. Cloud Computing: Are open source business systems and software as a service the next generation of ERP? CA Magazine. March 2009.

Boneh, Dan, et al. Public Key Encryption with keyword search. In proceedings of Eurocrypt. 2004.

Burns, Michael. Work in process: Using Technology to improve the way you do Business. CA Magazine. September, 2010.

Calloway, Timothy. Cloud Computin, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm? Duke Law and Technology Review. Vol. 11. No. 1. 2011.

Caplan, David. Bankruptcy in the Cloud: Effects of bankruptcy by a Cloud Services Provider. American Bar Association Annual Meeting. August, 2010.

Catteddu, Daniele & Hogben, Giles. Ed. Cloud Computing: Benefits, risks and recommendations for information security. ENISA. 2009.

Cavoukian, Ann. Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach. NEC Company Ltd. & Information and Privacy Commissioner of Ontario. May, 2010.

Chow, Richard et al. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. Proceedings of the 2009 ACM Workshop on Cloud Computing Security. CCSW. 2009.

Cloud Security Alliance. SecaaS: Defined Categories of Service 2011.

Cloud Security Alliance. Top Threats to Cloud Computing V1.0. March, 2010.

Coleman, Nick. Cloud Control. The Lawyer. October 2011.

Connolly, Chris. The US Safe Harbor – Fact or Fiction? Galexia Pty Ltd. 2008.

Connolly, Chris. Trustmark Schemes Struggle to Protect Privacy. Galexia Pty Ltd. 2008.

Curtis, Sophie. New Privacy Laws Could Boost EU Cloud Industry. CSO Security and Risk. January 27, 2012.

Debussere, Frederic. The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? International Journal of Law and Information Technology. Vol. 13. No. 1. Oxford University Press. 2005.

Delettre, Christian, Boudaoud, Karima & Riveill, Michel. Cloud Computing, Security and Data Concealment. IEEE. 2011.

Dorey, Paul & Leite, Armando. Commentary: Cloud computing – A security problem or solution? Information Security Technical Report 16. 2011.

Duff, Wendy, Smieliauskas, Wally & Yoos, Holly. Protecting Privacy. The Information Management Journal. April, 2001.

Durbin, Steve. Information Security without boundaries. Network Security. 2011.

Ebrahim, Zakareya & Irani, Zahir. E-government adoption: architecture and barriers. Business Process Management Journal. Vol. 11. No. 5. 2005

E-Government Survey 2010: Leveraging e-government at a time of financial and economic crisis. United Nations. Department of Economic and Social Affairs. 2010.

Esteves, Rui & Rong, Chunming. Social Impact of Privacy in Cloud Computing. 2nd IEEE International Conference on Cloud Computing Technology and Science. 2010.

European Commission. Commission Staff Working Paper. Impact Assessment. *Accompanying the document:* Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Brussels, 25.1.2012. SEC (2012) 72 final.

Everett, Catherine. Cloud Computing – A question of trust. Computer Fraud & Security. June 2009.

Fayyad, Usama, Piatetsky-Shapiro, Gregory & Smyth, Padhraic. From Data Mining to Knowledge Discovery in Databases. American Association of Artificial Intelligence. 1996.

Fowler, Martin. Patterns of Enterprise Application Architecture. Addison-Wesley Professional. 2002.

Glott, Rüdiger. et al. TClouds. D1.1.1 Draft Scenario and Requirements Report. Seventh Framework Programme. 2011.

Grant, Colin. Municipalities in a Cloud? Cloud Computing Implications for Municipalities. 2012.

Guerrini-Waksberg, Ana & Aibar, Eduard. Towards a Network Government? A Critical Analysis of Current Assessment Methods for e-Government. 2007.

Gunnarsson, Annicka & Ekberg, Siri. Invasion of Privacy: Spam – one result of bad privacy protection. 2003.

Gupta, Ajay, Klavinsky, Thomas & Laliberte, Scott. Security Through Penetration Testing: Internet Penetration. InformIT. 2002.

Hickey, Andrew. Channel Web. Computer Reseller News. 2010

Hof, Robert. Jeff Bezos' Risky Bet. Business Week. November, 13, 2006.

Hurlburt, George et al. Privacy and/or Security: Take Your Pick. IEE Computer Society. 2009.

IBM Samrt Business. Dispelling the vapor around cloud computing: Drivers, barriers and considerations for public and private cloud adoption. 2010.

Jacobs, Dean. Enterprise Software as Service: Online services are changing the nature of software. QUEUE. July/August. 2005.

Jeselson, Pat et al. A Foundational Framework for a PbD – PIA. 2011.

Karadsheh, Louay. Applying security policies and service level agreement to IaaS service model to enhance security transition. Computers & Security 31. 2012.

Karn, Bernice. Data Security- The Case Against Cloud Computing. Cassels Brock Lawyers. 2011.

Karol, Thomas. Understanding Cross-Border Privacy Impact Assessments. EDPACS: The EDP Audit, Control, and Security Newsletter Vol. 29. No. 4. October, 2001.

Kepes, Ben. Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS. Diversity Limited. 2011.

Knutson, Tina. Building Privacy into Software Products and Services. IEEE Computer Society. 2007.

Krekke-Hermandson, Tina. Privacy Violation Detection. 2004.

Kuyoro, Shade, Ibikunle, Frank & Awodele, Oludele. Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN). Vol. 3. Issue. 5. 2011.

Langenderfer, Jeff & Miyazaki, Anthony. Privacy in the Information Economy. The Journal of Consumer Affairs. Vol. 43. No. 3. 2009.

Lee, Sang, Tan, Xin & Trimi, Silvana. Current Practices of Leading E-Government Countries. Communications of the ACM. Vol. 48. No. 10. 2005.

Loganayagi, Balusamy. & Sujatha, Sundaram. Enhanced Cloud Security by Combining Virtualization and Policy Monitoring Techniques. The International

Conference on Communication Technology and System Design 2011. Procedia Engineering 30. 2012.

Maximilien, Michael. Enabling Privacy As a Fundamental Construct for Social Networks. 2009 International Conference on Computational Science and Engineering. IEEE. 2009.

Mell, Peter & Grance, Timothy. The NIST definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. 2011.

Menkus, Belden. Understanding Cross-Border Privacy Impact Assessments. EDPACS: The EDP Audit, Control, and Security Newsletter. Vol. 29. No. 5. November, 2001.

Mowbray, Miranda, Pearson, Siani & Shen, Yun. Enhancing privacy in cloud computing via policy-based obfuscation. 2010.

O'Malley, Colin. The EU e-Privacy Directive: don't call it a cookie law. Econsultancy. 2012-05-16.

Ozer, Nicole & Conley, Chris. Cloud Computing: A Storm Warning for Privacy? ACLU Northern California. January, 2010.

Papanikolaou, Nick et al. Encore: Towards a Holistic Approach to Privacy. 2010.

Parsons, Christopher. Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies. Version 2.2. February 7, 2012.

PEW Internet & American Life Project. Use of Cloud Computing Applications and Services. 2008.

Pounder, C.N.M. Why privacy is at risk. Computer Law and Security Review 25. 2009.

Preece, Jenny. Online Communities: designing usability supporting sociability. Wiley and Sons. 2000.

Prakash, Niraj & Gulla, Umesh. Adoption of Enterprise Applications RTowards E-Government – A Select Case Study of Municipal Corporation of Greater Mumbai. 2008.

Rashid, Fahmida. EU e-Privacy Cookie Rules Will Impact Non-European Web Companies. www.securityweek.com. 2011.

Ristov, Sasko, Gusev, Marjan & Kostoska, Magdalena. Cloud Computing Security in Business Information Systems. International Journal of Network Security and Its Applications (IJNSA). Vol. 4. No. 2. 2012

Rosen, Jeffrey. The Right to be Forgotten. Stanford Law Review Online. 88. February 2012.

Ryan, Matthew. Cloud Computing – Legal Considerations for Data Controllers. Dillon Eustace. 2011.

Seltzer, William & Anderson, Margo. NCES and the Patriot Act: An Early Appraisal of Facts and Issues. 2002.

Sembok, Tengku. Ethics of Information Communications Technology (ICT). UNESCO Regional Unit for Social & Human Sciences in Asia and the Pacific (RUSHSAP). 2003.

Soghoian, Christopher & Stamm, Sid. Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL. 2010.

Solomon, Andrew. Privacy and the Cloud. Speech to Cloud Computing Conference and Expo, 9 September, 2010.

Sotto, Lisa, Treacy, Bridget & McLellan, Melinda. Privacy and Data Security Risks in Cloud Computing. Electronic Commerce & Law Report. 2010.

Steven, John. Adopting an Enterprise Software Security Framework. IEEE Security & Privacy. 2006.

Strukhoff, Roger. Gartner Analyst Says Cloud Computing "Immature" Yet Inevitable. Virtualization Journal. 2010.

Tancock, David, Pearson, Siani & Charlesworth, Andrew. A Privacy Impact Assessment Tool for Cloud Computing. 2nd IEEE International Conference on Cloud Computing Technology and Science. 2010.

Tillman, Bob. More Information Could Mean Less Privacy. The Information Management Journal. March/April 2003.

Trend Micro. Cloud Computing Security: Making Virtual Machines Cloud-Ready. A Trend Micro White Paper. August, 2009.

Tripathi, Alok & Mishra, Abhinav. Cloud Computing Security Considerations. Interface IEEE. 2011.

Van Ecke, Patrick & Truyens, Maarten. Privacy and social networks. Computer Law and Security Review 26. 2010.

Van Lieshout, Marc et al. Privacy by Design: an alternative to existing practice in safeguarding privacy. Emerald. 2011.

Von Tigerstrom, Barbara, Nugent, Patrick & Cosco, Venessa. Alberta's Health Information Act and the Charter: A Discussion Paper. May, 2000.

Wang – Liying, Jessa & Loui, Michael. Privacy and Ethical Issues in Location-Based Tracking Systems. IEEE. 2009.

Wang, Hui. Privacy-Preserving Data Sharing in Cloud Computing. Jouranl of Computer Science and Technology. 25(3). 2010.

Wang, Jian et al. Providing Privacy Preserving in cloud computing. 2009 International Conference on Test and Measurement. IEEE. 2009.

Wernick, Alan. Warning Cloud. 2010.

Whitehead, Tom & Kirkup, James. A request to snoop on public every 60 secs. The Telegraph. August 9, 2009.

Whittaker, Zack. Google Admits Patriot Act requests; Handed over European data to U.S. authorities. ZDNet. August 11, 2011.

Wright, David et al. Ed. PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights. Seventh Framework Programme. 2011.

Wright, David. Should Privacy Impact Assessments be Mandatory? Communications of the ACM. Vol. 54. No. 8. August, 2011.

Wright, David. The state of the art in privacy impact assessment. Computer Law & Security Review 28. 2012.

Yang, Lvquing & Liu, Zhenyu. The risk assessment of Enterprise application software based on gray relational analysis and FMEA. IEEE 2010.

Yang, Lvquing & Jiang, Chuan. Research on Enterprise Application Software Project Implementation Model.IEEE 2011.

Zississ, Dimitrios & Lekkas, Dimitrios. Addressing cloud computing security issues. Future Generation Computer Systems. January 2012.

Appendix #1

Cross-border Privacy Impact Assessments[52]

1. **Organizational responsibility for the ownership of personal information (PI)**

    a.i. Has the custody and control of the PI been determined and documented for each jurisdiction?

    a.ii. Have the privacy requirements been documented for each jurisdiction?

    a.iii. Does the organization have specific audit and enforcement mechanisms that oversee the collection, use and disclosure of PI information that is collected on its behalf?

    a.iv. Does the enterprise collect, transmit, maintain or disclose personally identifiable information in more than one jurisdiction (that is nation, state, province, or territory)?

2. **Identifying the purpose for which the PI is kept,**

    a.i. Are all parts of the PI information necessary to the business purpose?

    a.ii. Can the purpose be performed adequately with less information?

    a.iii. Is notification being provided when the information is being collected?

52 Karol, Thomas. Understanding Cross-Border Privacy Impact Assessments. EDPCAS: The Audit, Control and Security Newsletter. 29:4. 2001.

3. Limiting data collection to business objectives,

a.i. Is PI collected directly from the individual to whom it pertains, is the collection indirect, has the data subject consented to such collection?

a.ii. Are the purposes for the collection of the information clearly disclosed?

a.iii. Is there a process for the disclosure of the PI and documentation to support such disclosure?

4. Required consent,

a.i. Implicit in the concept of consent is the requirement that the person giving consent knows that the information is being collected and the manner in which it may be used and disclosed.

a.ii. Are the proposed consent provisions consistent with the existing laws and standards for each jurisdiction?

5. Limitations on the retention of PI information,

a.i. Retention only until business purpose has been fulfilled

a.ii. PI used to make decisions about individuals must be maintained long enough to allow the individual access to the data

6. Accuracy of data,

a.i. Does the record include the date of the original collection and all of the updates?

a.ii. Are all of the custodians of personally identifiable information aware of the cross-jurisdictional procedures regarding the individual's right to access?

7. Data security,

a.i. Have IT security procedures for the collection, transmission, storage and disposal of PI information and access to the PI been documented?

a.ii. Has staff been trained in the requirements for the protection of PI information, are they aware of the policies and penalties regarding violations of security or confidentiality?

a.iii. Are access rights restricted to individuals that have a business need to the data?

a.iv. Are the security measures adequate to the sensitivity of the PI?

a.v. Is sensitive PI encrypted?

a.vi. How is the data stored – records management procedures, are types of databases to be utilized documented (e.g. Oracle, Microsoft, SQL, DB2, Sybase or Informix)?

a.vii. How are audit records generated, protected, stored?

a.viii. Is there documentation of the PI that may be stored in the system's cache, memory or RAM?

a.ix. Is it possible that the PI could be transferred to other media?

a.x. How and why are cookies used on the site?

a.x.1. Are cookies transmitted and received in an SSL session

a.x.2. What type of cookie is used: session identifier cookies – typically contain no user specific data, user id cookies: used to id the user to the server following authentication, flag cookies: persistent cookies used to determine if the user has already seen certain warnings,

a.xi. What type of protocol is used to transmit data: TCP/IP, AppleTalk, SNA or IPX/SPX?

a.xii. Is access to the PI granted to any 3rd parties?

a.xii.1. Are there legal contracts and confidentiality agreements that detail the privacy and security requirements that are in place for IT consultants and contractors

a.xii.2. Are there any 3rd party applications or banners operating the CSPs site?

a.xii.2.a.i. Are the applications executable files downloaded by the client

a.xii.2.b. What personally identifiable information is logged by the server

a.xii.2.c. Does this information get correlated with other information

a.xii.2.d. Can cached information be accessed by the host server of the website being visited

8. Training and communication,

a.i. Does documentation of training provided exist?

a.ii. Have independent privacy oversight and review mechanisms been established by the organization?