MISSM RESEARCH

STUDY OF LEGAL RISKS ASSOCIATED WITH SAAS MIGRATION

LEOPOLDO DELA ROSA
123189, ldelaros@student.concordia.ab.ca
780-7096584

Research Advisors: Pavol Zavarsky, Ron Ruhl, Dale Lindskog
{dale.lindskog,pavol.zavarsky,ron.ruhl}@concordia.ab.ca

Master of Information Systems Security Management
Concordia University College of Alberta

10/31/2010

STUDY OF LEGAL RISKS ASSOCIATED TO SAAS MIGRATION

LEOPOLDO DELA ROSA
ldelaros@student.concordia.ab.ca
Concordia University College of Alberta

Research Advisors: Pavol Zavarsky, Ron Ruhl, Dale Lindskog
{dale.lindskog,pavol.zavarsky,ron.ruhl}@concordia.ab.ca

Abstract

This paper identifies, investigates, and explores the legal risks associated with migration to "Software-as-a-service". This paper shows how these risks might impact migration. Based on the legal risks identified, this paper suggests mitigating strategies using, but not limited to, contractual terms in the SLA.

1. Introduction

Enterprises are fast seeing the benefits of SaaS because of ease and speed of deployments, the virtual lack of a requirement to acquire and maintain hardware infrastructure, and ease of upgrades. However, chief among the concerns for migrating to SaaS is the security of data entrusted into the cloud provider. Enterprises are concerned over their loss of control over the data deployed. Nevertheless once these security concerns are addressed by SaaS providers through technical safeguards, most decision makers jump into the cloud bandwagon without considering other risks associated thereto. [1]

Such a boom in business has lead to the mushrooming type of growth in the Cloud computing sector particularly in the SaaS service deployment type. Service providers as well as businesses are looking at off-shore locations to place servers that will host applications to lower cost[2]. This trans-country expansion has created legal conundrums that most decision makers are either ignorant of or neglecting to pay attention to.

When an enterprise adopts SaaS, it entrusts a portion or all of its information to the service provider. The provider in turn stores this information in its data centers within its network and is accessed by the clients via the Internet. Depending on a number of factors, such as location of the provider, client, user of the information, data processing and transmission path this paper finds legal risks and jurisdictional issues may arise.

This paper shall refer to the following terms for the entire discussion:

- Enterprise Customer/Client/ – refers to the organization, corporation, or business migrating or entrusting information to the SaaS provider.
- SaaS/service provider – refers to the organization offering the "Software-as-a-service" to the enterprise for a fee.
- User – refers to the individual owner of the information
- Covered entities - refers to enterprises under the purview of a particular statute.

This document examines laws relating to privacy, compliance, storage, handling, transmission, and processing of personal, health, and corporate financial information held or entrusted by an enterprise to a SaaS provider. This research is not exhaustive and makes no attempt to consider all possible, potential, and pertinent laws that may apply. It serves merely as a guide and presents only a landscape of the legal risks. It is not intended to constitute as legal advice or opinion and is for general information purposes only.

The discussion is limited to federal and/or national laws in the United States of America, Canada, and European Union as well as other countries that may have similar statutes, relevant to SaaS migration.

This paper finds the following

1. when financial, technical, and operational gains associated with SaaS migration are established, it should not be the sole basis for adopting SaaS
2. information containing corporate finances, personal financial/cardholder payment, health records, when entrusted to a SaaS provider may have further restrictions, compliance requirements, changes in status, and loss of privacy protection based on applicable statutes
3. the SLA of the client and the SaaS provider is crucial in mitigating most of the legal risks identified

In section two, it shall begin by giving an overview of the general legal risks associated to SaaS migration, section three then examines and discusses pertinent laws based on the information entrusted to a SaaS provider. In section four, mitigating strategies are suggested through, but not limited to, contractual terms in the SLA. Finally in section five the conclusion is presented.

2. OVERVIEW OF SAAS GENERAL LEGAL RISKS

This section examines three general legal and regulatory risks associated with SaaS information migration. We begin by defining each legal risk followed by a common example. A more detailed discussion follows in section three.

2.1 TRANSBORDER DATA FLOW

Transborder data flow (TBDF) is defined by the United Nations Centre on Transnational Corporation as, "the movement across national boundaries of computerized, machine-readable data for processing, storage or retrieval." To simply put it, TBDF is the flow of electronic data across multiple jurisdictional and/or political boundaries, such as between states and/ or countries.[3]

Since enterprises are usually unaware of the actual physical storage location of their entrusted information [4], access to it may cause transmission of data across borders. Data at rest or passing through a different state/country will be subject to different laws and/or regulation. This applies despite being merely transmitted or is returning to its original source but has since emanated from another.

A good example of this scenario is a typical webmail or e-commerce application, i.e. online shopping. A user provides information to access an email service or purchases a product on a website and sends it across multiple jurisdictions depending on locations of the provider or online merchant.

2.2 CONTRACTUAL AND REGULATORY COMPLIANCE

Presumably, every jurisdiction has its own local regulation that mandates the way information containing health and finances of an individual or business is handled, stored or transmitted.

Concomitant with compliance and regulatory requirements, SaaS providers and its clients are bound contractually through a service-level-agreement (SLA) that determines the level of service between the parties. It outlines the manner and delivery of the agreed upon service, including, but not limited to data security, government access, limitations, performance, and termination.

Often SaaS providers have contracts that limit their liability and have no warranties about their provided service. This means that should entrusted information be unavailable, through disruption or loss of service, not only is the SaaS provider limited in liability, but they also do not warrant when they can return the agreed upon service. Ultimately the liability falls on the enterprise because they are also bound by contractual agreements with the user or compliance requirements on the availability of the entrusted information.

These service disruptions may lead to investigations either for contractual liability purposes or for violations of laws or government regulations. The next section discusses the general implications to the service provider, enterprise and the end user of evidence gathering for purposes of investigations.

2.3 ELECTORNIC DISCOVERY

Electronic discovery or E-discovery is defined as the exchange of information in electronic format (electronically stored information or ESI), with or without the aid of digital forensics analysis for the purpose of recovering evidence for litigation.[5] Some E-discoveries may go as far as the production of the actual physical drive that contains the data as well as all other electronic copies thereto including the back-up.[6] Seizure by Governments of the actual physical drive from a SaaS provider may result in data unavailability for numerous clients.

SaaS providers are bound by law to comply with these E-discovery requests and the SLA cannot hinder nor hamper such investigation or evidence gathering. This again raises legal and contractual risks for the enterprise due to the multi-tenant nature of the SaaS model.[7]

Bearing in mind the above-mentioned legal risks, this paper shall now discuss key laws and regulations pertaining to information entrusted to a SaaS provider.

3. COMPLIANCE AND PRIVACY REQUIREMENTS IN SAAS

By entrusting information to a SaaS provider the enterprise maybe inadvertently exposing itself to various risks arising from contractual, legal and privacy compliance risks. This is due to the application of different laws on the information during transmission, processing or storage location and sometimes based on content. These risks and applicable laws must be known by the decision makers prior to migration or at least during the decision making process in order for mitigation strategies to be instituted early and to enable it to make a more informed decision.

The succeeding sub-sections examines a few key federal and national laws relevant to the storage, handling, processing and transmission of protected health information (PHI), electronic health records (EHR), corporate financial data, cardholder payment data, and non-public information (NPI) entrusted to a SaaS provider.

3.1 FINANCIAL REPORTING, SAAS, AND SOX COMPLIANCE

Section 404 of the Sarbanes-Oxley (SOX), mandates that management of publicly traded US corporations, shall be responsible for establishing and maintaining an adequate internal control structure and procedures for financial reporting including an assessment of its effectiveness.[8]

If certain operations requiring financial information processing is outsourced by covered entities to a SaaS provider, then the management requirement of assurance extends also to the service provider's internal controls and processes. Management should ensure, assess, and test that the controls and processes implemented by the service provider are adequate and effective to be compliant with SOX. [8]

This particular extended requirement is not limited to merely the US based companies. Other countries have similar legislation such as Japan's Financial Instruments and Exchange Law, J-SOX, Canada's Keeping the Promise for a Strong Economy Act (Budget Measures) 2002, C-SOX, and Australia's Corporate Law Economic Reform Program Act 2004, CLERP-9. All modeled after the US-SOX and imposing comparable requirements upon management.[1][9]

There are two ways for management to approach the assurance for this requirement, first, management may consider the controls and processes of the provider in the same way it addresses similar controls and processes within its organization. This approach would entail inclusion in the contract or SLA a right to audit and provision for documentation. Second, management may to a certain extent make a reliance on the provider's internal testing of controls based on their SAS 70 type II report.[10]

3.2 PERSONAL FINANCIAL INFORMATION, SAAS, AND GLBA COMPLIACNE

The Gramm-Leach-Bliley Act, (GLBA) also known as the Financial Services Modernization Act raises issues for financial institutions and non-financial institutions collecting, receiving, and storing data pertaining to consumer personal financial information (PFI). The succeeding sections discusses two provisions affecting PFI in SaaS, namely the financial privacy rule, (FPR) and safeguards rule (SR).[11]

3.2.1 FINANCIAL PRIVACY AND SAFEGUARDS RULE

Under the financial privacy rule of the GLBA, when financial and non-financial institutions are collecting, receiving, and storing personal financial information it is required to give their customers privacy notices. These notices contain the following[12];

- the institution's policy on handling personal financial information
- a written agreement with the SaaS provider concerning the intended purpose of its disclosure
- prohibition from sharing PFI to non-affiliates third parties
- and an "opt-out" choice

Under the safeguards rule, personal consumer information held by financial institutions requires protection under a written protection plan, a due diligence selection of a provider and a contract mandating the institution to implement and maintain appropriate technical safeguards in protecting the

1 THE SEED FOR THIS IDEA CAME FROM -Hariharan M, "A Quantitative Model for Information security assessment", March 2010 Birla Institute of Technology and Science

information, assignment of liability, and the capability to honour "opt out". [13]

A common requirement under the two rules is a written contract between the provider and the institution mandating the latter to ensure that the former is in compliance with GLBA with regard to the information entrusted. This means that to comply, institutions migrating personal financial information must also contractually bind their SaaS provider to the provisions of the GLBA.

3.2.2 ENCRYPTION REQUIREMENT FOR FINANCIAL INSTITUTIONS

A further requirement, however, is encryption. Several US agencies have released guidelines addressing pertinent provisions of the safeguards rule.[14] One agency in particular, the Federal Financial Institutions Examination Council (FFIEC), has formally required that financial institutions "should employ encryption strength sufficient to protect information from disclosure until such time as the information's disclosure poses no material threat", and that "Encryption can be used as a preventive control, a detective control, or both." [15]

3.3 HEALTH INFORMATION, SAAS, AND HIPAA COMPLIANCE

The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law for the protection, security, and privacy of health information. It covers Protected Health Information (PHI) and Electronic Protected Health Information (EPHI). The next section examines the privacy and security rule pertinent and its implications to enterprises and service providers holding E/PHI. [16]

3.3.1 BUSINESS ASSOCIATE, SAAS, PRIVACY AND SECURITY RULE

The privacy rule prohibits use and disclosure of PHI by covered entities, unless allowed or mandated by HIPAA or permitted in writing by the individual concerned. [17] The security rule pertains specifically to EPHI and sets down three safeguards namely: administrative, physical, and technical to ensure, among others, that transmission of EPHI are only to those who have authorized access. [17]

HIPAA refers to SaaS providers as "business associates". [17] Prior to disclosure of E/PHI to a SaaS provider, a covered entity is required to enter into a "business associate contract" stating, that the service provider agrees to be contractually bound by the same privacy and security rule.

A further requirement in the contract is a special reporting duty by the SaaS provider in cases of subpoena of E/PHI it is holding for a covered entity's behalf. This duty stems from an HIPAA requirement wherein the covered enterprise must notify and give the individual, whose E/PHI is subpoenaed, an opportunity to dispute the mandated disclosure. [17]

This reporting requirement has been expanded by the HITECH act to include among other things notifications for security breaches concerning E/PHI. [17] [18] The next sub-section discusses this expansion.

3.4 HITECH ACT: BREACH NOTIFICATIONS, PHI, AND SAAS

The Health Information Technology for Economic and Clinical Health (HITECH) Act was established in the US to encourage adoption of and to address privacy and security concerns associated with the electronic transmission of electronic health records (EHR). [18]

Subtitle D of the HITECH Act effectively extended the enforcement of the privacy and security rule of the HIPAA to business associates of covered health care providers. Thus, any non-affiliated third party SaaS provider, whether an aggregator or re-bundler of SaaS services, that has access to unsecured PHI of covered health providers should also be under a business associate contract. [19][20]

The HITECH Act also expands the notification obligations to include discovery of breach of unsecured PHI. The requirement now obliges business associates to notify covered entities and covered entities to notify affected persons upon discovery of breach of unsecured PHI if the breach causes significant risk of financial, reputational, or other harm to the concerned individual. [21]

3.5 PERSONAL INFORMATION PROCESSING, EUROPEAN UNION DATA PROTECTION ACT, AND SAFE HABOR PROGRAM

The EU data Protection Act (Directive 95/46/EC), EUDPA is a directive adopted by member European Union states that controls the process, use, exchange as well as protects the privacy and security of personal data collected for or about citizens of the EU. The directive prohibits transfers of personal data about EU citizens to third-party countries that do not provide an "adequate" level of privacy protection. [22] This impacts enterprises and SaaS providers holding personal data of EU citizens. They are now barred from transferring this information

outside EU member states or to those not on the EU Data Protection Act's list of countries with an adequacy finding.

Interestingly though, the U.S. is not on this EU list of countries with adequate privacy standards. [23] EU members as well as covered entities cannot transfer personal EU citizen data to the US and other countries not on the list for failure to meet the adequacy standard.

However, a US based service provider may only be able to legally receive EU personal data provided it adheres to the ''Safe Habor Program'' developed by the US together with EU members. [24]

3.6 PERSONAL INFORMATION, CANADA PIPEDA, AND SAAS

Personal Information Protection and Electronic Documents Act or PIPEDA is a Canadian data privacy law that pertains to the collection, use and disclosure of personal information for business or commercial purposes by the private sector.[25]

When PIPEDA covered entities migrates information to SaaS providers, it is considered as a "transfer of data to third-parties for processing". [26] Despite the transfer, the covered entity is mandated to be ultimately responsible and is required to ensure a comparable level of protection is accorded to personal information. This is achieved by the use contractual agreements, similar to HIPAA, to bind the SaaS providers to the provisions of the PIPEDA directive. [27]

3.6.1 PEROSNAL DATA, TBDF, CANADA PRIVACY COMMISSIONER, AND SAAS

The Privacy Commissioner of Canada oversees compliance under PIPEDA [28] and as such has released guidelines relating to trans-border data flow or transfers of personal information to third-parties for processing outside Canadian jurisdiction.

Under the guidelines, the enterprise remains responsible for personal information collected regardless of data processing location, whether within Canada or in a foreign jurisdiction. It further obligates enterprises to take reasonable steps in protecting personal information from unauthorized use and disclosure while in the hands third-party processors. It must be satisfied with the third-party data processor's procedures, policies, staff training, security measures, and must have a right to audit and inspect the provider.[29]

3.7 CARDHOLDER DATA, PAYMENT INFORMATION AND SAAS

3.9.1 PCI-DSS COVERAGE

Payment card industry- Data security standard or PCI-DSS is an international information security standard that defines a minimum set of control objectives for organizations that process card payments. It is designed to safeguard cardholder data wherever stored, processed, and transmitted. [30]

This standard applies and is incumbent upon the covered enterprise despite migration payment processing to SaaS or as PCI defines it ``service providers``. PCI requires a written contract that indicates an acknowledgement by the service provider of its responsibility to secure card holder data.[31] The succeeding sub-sections section discusses PCI standards relevant to organizations with cardholder and payment card data and the implications of its SaaS deployment. [27]

3.9.2 PCI-DSS CARDHOLDER DATA ENVIRONMENT

Much of the standards and requirements of PCI-DSS covered entities pertain to cardholder data environment or CDE and its protection. A CDE is defined by PCI-DSS "as an environment in a network that either possesses, stores, or transmits cardholder data". [32] The covered entity is mandated to protect cardholder and payment data in the CDE from unauthorized access as well as from authorized access even if it outsourced to a shared hosting provider.[33]

PCI further requires upon the covered entity a written contract similar to HIPAA and GLBA that includes an acknowledgement by the SaaS provider that it is responsible for the security of the cardholder data it possess for its client's behalf. [34] The contract should contain PCI standards in protecting cardholder data within the CDE such as data segregation, access control, encryption, monitoring of wireless implementations and review of logs and audit. The succeeding sub-sections discuss these standards.

3.9.3 PCI-DSS STANDARDS DATA SEGREGATION, ACCESS CONTROL, ENCRYPTON, WIRELESS IMPLEMENTATION

Data segregation under PCI-DSS requires the restriction of access of a cardholders' data to only its own data environment or CDE. [32] If the CDE is with a shared hosting provider or SaaS provider, the covered entity is required to ensure that each client of the provider should only have access and can only

run processes within their respective data environments. [35]

Corollary to data segregation is the requirement of an access control on the data held by the shared hosting or SaaS provider. These controls should restrict each of the covered entities' user's access to their own data in the CDE as well as protect the data from unauthorized access by other users in the same environment. [36]

A good strategy for this requirement is to have the access control list (ACL) managed by the covered entity and have the SaaS provider interface directly to it. This way the covered entity maintains direct control over access through their preferred directory service.

Logs and audit trails of the covered entity on the SaaS provider's network should be enabled for each data environment and access should be provided for monitoring and forensic purposes but limited only to each covered entity. [37]

Covered entities must ensure the following on the shared or SaaS providers' network, testing for wireless access points on a quarterly basis, vendor defaults are not used, and strong encryption and security protocols are used during transmission of cardholder data. Incidentally, the use of WEP as a security control was prohibited as of 30 June 2010. [38]

3.9.4 SAAS PROVIDER AND ENTERPRISE PCI-DSS COMPLIANCE

Even if its SaaS provider is compliant with under PCI with one covered entity, compliance with the others is not guaranteed. PCI requires each entity which has access to cardholder data is responsible for its own compliance at all times and should validate compliance as applicable.[39][40]

3.10 GLOBAL CRYTOGRAPHY REGULATIONS

The International community has recognized both the value and risk associated with encryption technology. It offers security and privacy of communications but at the same time it can also be used to conceal illegal activities. Thus many countries have passed laws regulating import, export and use of cryptography. [41]

Enterprises considering off-shore SaaS providers should be aware of these laws at least those applicable to the data transmission path of the provider. Complying with International encryption requirements is complex and entails significant risks because of widely diverse regulations from country to country. Violations or non-compliance can be costly and sometimes punishable by either seizure of technology or criminal penalties. [42]

In some cases governments have threatened to block or have barred encrypted communications of certain service providers. For example the recent threat of U.A.E. and Saudi Arabia to ban RIM Ltd. Blackberry services on grounds of national security because of its refusal to open certain encrypted data to the Governments. [43] This highlights the gravity and necessity to comply with per country encryption laws. A helpful guide and list of global encryption laws are available at the Wassenaar arrangement and the Cryto Law Survey.[44] [45]

3.11 INFORMATION SEIZURE, US PATRIOT ACT SECTION 215, 505 AND SAAS

The US Patriot Act, born out of the events of Sept 11'01, gives the American Government considerable disclosure powers while dispensing the need for transparency. Under Section 215 and 505 of the Act, the FBI, upon application to a Judge, or through the use of National Security letters NSL, can compel the disclosure of virtually any electronic data, or the production of any ``tangible things`` which may include physical hard drives of the service provider within the jurisdiction of the US. Furthermore, those who receive an NSL or a section 215 court order are strictly prohibited from informing the entities affected. [46]

Because of these powers, potentially any type of data situated or possessed by a US based company may be subject of a seizure under the Patriot Act. An obvious solution for enterprises and SaaS providers would be to simply store or transmit data elsewhere. However, steering away from US jurisdiction may not always result in absolute security. [47] It seems that the US government have other cross-border enforcement options as examined in the next sections.

3.11.1 LETTERS ROGATORY, MUTUAL LEGAL ASSISTANCE TREATY AND SAAS

The US Government, in the past, has used the Mutual Legal Assistance Treaty or MLAT and Letters of Rogatory in connection with national security to enforce records attainment despite violation of another jurisdiction's law. [48][49][50] MLATs are bilateral treaties that requests assistance directly from justice departments of foreign countries, to obtain evidence and Letters Rogatory are formal assistance requests from law for evidence from a foreign law court.[51]

According to US court rulings both foreign companies with US based offices or subsidiaries and foreign subsidiaries of US based companies can be compelled to produce records on grounds of national security for the former and on the extent of control powers of the latter.[52][53] Apparently data storage location of SaaS providers may not matter when it comes to the application of the Patriot Act. It seems that, if a SaaS provider has sufficient connections to the US then it may still be subject to US laws on disclosure.

Furthermore, in Canada, federal and provincial Governments have outsourced information technology and data management services to US companies.[54][55] Despite this, however, the Privacy Commissioner released an opinion declaring, among other things, that contractual terms may not preclude or override the provisions of Section 215 and 505 of the Act. According to the Commissioner's findings, US based third-party service providers may be ordered to disclose Canadian controlled outsourced information and contracts cannot prevent its applicability. [56]

Though there are no officially known extra-territorial applications of the Patriot Act to date, an inference can be made on its applicability based on the opinion of the Privacy Commissioner of Canada, US case law, and recent actions of the FBI concerning data centers. [2]

A recent raid in data center in Texas highlights compliance risk and the collateral damage an enterprise may encounter. The FBI seized several physical servers containing hundreds of other business' data in an effort to investigate crimes of fraud. [57]

4. MITIGATING STRATEGIES

Based on the examination of laws, regulations, and compliance requirements this paper finds that due diligence on the part of the enterprise in information analysis, SaaS provider selection, reviewing/drafting the SLA, and research of applicable laws are the most critical mitigation steps it can take to reduce impact of legal risk.

The next sections discusses the specific due diligence in more detail.

4.1 DUE DILIGENCE IN ANALYSIS OF INFORMATION AND PROCESSING REQUIREMENTS

Enterprises should determine precisely what type of information it collecting storing, handling, and processing. Content should be given considerable weight and is an important factor in determining which laws apply as well as the level of protection and type of SaaS service required when it is migrated.

The enterprise should then decide on the location of information processing. Should it outsource the process of information or should it remain in-house and migrate only the application? Keeping information processing onsite, however, significantly reduces compliance requirements because information may no longer be transmitted across borders.

4.2 DUE DILIGENCE IN SELECTING SAAS PROVIDER

Enterprises in its exercise of due diligence should to inquire about the provider's security processes controls, policies, backup, availability, location, jurisdiction, data path transmission, training and certifications. A SAS 70 type II audit report is a good basis for evaluation. It can permit the enterprise to asses if the provider can meet its compliance needs. However, enterprises should not stop there; if possible, conduct an ocular inspection to actually verify implementation of controls.

Location of data storage is essential and should be central to the evaluation of the provider because it affects the obligations of both parties based on applicable laws and regulations.

Ensure a direct relationship with your SaaS provider and refrain from having or selecting secondary providers.

4.3 DUE DILIGENCE IN REVIEWING SLA

A service-level-agreement is the most crucial factor in evaluating and mitigating legal risk associated SaaS migration. It should be thoroughly reviewed and carefully drafted before entering into a contractual relationship with the SaaS provider.

Comparing different SLA's of multiple providers is prudent and recommended. It will enable the enterprise to determine what other providers are offering in order to base negotiations for inclusions and exclusions of stipulations or terms in the contract that can maximize protection and minimize risks.

Enterprises should remove disclaimers or waivers of liability, unilateral change in terms, and include penalties for service disruption or loss of data, right to make onsite inspection and audit.

[2] Idea comes from reference [57]

An important provision is the notification obligations or incident response. Enterprise should expand their notification requirements upon the provider to include every possible instance of unauthorized access of the information held.

4.4 DUE DILIGENCE IN APPLICABLE LAWS

Based on the enterprises' analysis of information requirements and selection of SaaS providers, it should then be able to determine applicable laws, regulations, and compliance requirements.

An understanding of pertinent laws can substantially reduce incidence of violations, non-compliance, and can significantly minimize litigation costs.

5. CONCLUSION

An enterprise's service level agreement with a SaaS or service provider is seemingly the most critical factor in its evaluation of legal risks relating to migration. It should be thoroughly and carefully examined before adhering thereto or entering into a cloud relationship. A carefully crafted SLA that addresses applicable laws and can significantly minimize legal risks to the enterprise while maximize the information protection.

This research can be used as a guide for further studies on more stringent state and provincial laws and compliance requirements. It can also be used to compare legal risk with other types of information such as copyrights, trademarks, patents, trade secrets, and data mining.

REFERENCES

[1] C.G. Lynch, "Enterprises Adopt SaaS Aggressively, on Wed, May 07, 2008, available: http://www.cio.com/article/351563/Report_Enterprises_Adopt_SaaS_Aggressivelwww.cio.com/article/351563/Report_Enterprises_Adopt_SaaS_Aggressively

[2]Gary Kim, "Cloud Communications Industry to Grow, IT Retail Prices to Drop, Says Gartner", Cloud Communications Feature,September 14, 2010, http://it.tmcnet.com/channels/cloud-communications/articles/101550-cloud-communications-industry-grow-it-retail-prices-drop.htm

[3] "Transnational Corporations and Transborder Data Flows: A Technical Paper", page 8 United National Center on Transnational Corporations (UNCTC) Published: 1982 available: http://unctc.unctad.org/data/e82iia4a.pdf.

[4] Laura Smith, "Cloud location: Why it's important to know where your data resides", JUN 25 2010 CIO, Cloud computing, http://itknowledgeexchange.techtarget.com/total-cio/cloud-location-why-it%E2%80%99s-important-to-know-where-your-data-resides/

[5] Eoghan Casey. ed. "Handbook of Digital Forensics and Investigation" Academic Press. pp. 567. ISBN 0123742676.

[6] Bell ExpressVu Limited Partnership v. Heeren, 2010, 665, Court file no: 07-CL-6981, date: 20100127, available: http://www.canlii.org/en/on/onsc/doc/2010/2010onsc665/2010onsc665.html

[7]Frederick Chong, Gianpaolo Carraro, and Roger Wolter, "Multi-Tenant Data Architecture", June 2006, Microsoft Corporation, http://msdn.microsoft.com/en-us/library/aa479086.aspx

[8] ''Sarbanes-Oxley Act of 2002'', USA available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

[9] Gib Trub, Laurie Olski, October, 2008, version 2.0 "Global report on the status of IT compliance Processes" http://www.ca.com/files/industryresearch/gmg-globalcompliancereport.pdf

[10] Institute of Internal Auditors, "SARBANES-OXLEY SECTION 404:A Guide for Management by Internal Controls Practitioners", 2nd edition January 2008, available: http://www.theiia.org/download.cfm?file=31866

[11] *Federal Financial Institution Examination Council,* Gramm-Leach-Bliley Bill Section 501(b) available: http://www.ffiec.gov/exam/infobase/documents/02-con-501b_gramm_leach_bliley_act-991112.pdf

[12] "The Gramm-Leach-Bliley Act: The Financial Privacy Rule", Privacy Initiatives, *Federal Trade Commission,* available: http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html

[13] "The Gramm-Leach-Bliley Act: The Safeguards Rule", Privacy Initiatives, Federal Trade Commission, available: http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html

[14] "Interagency Guidelines Establishing Standards for Safeguarding Customer Information", Coauthored by the U.S. Department of the Treasury: Office of the Comptroller of the Currency and Office of Thrift Supervision; Federal Reserve System; and Federal Deposit Insurance Corporation; February 1, 2001, www.ffiec.gov/exam/InfoBase/documents/02-joisafeguard_ customer_info_final_rule-010201.pdf

[15] *Federal Financial Institution Examination Council,* Booklet: Information Security

Section: Security Controls Implementation
Subsection: Encryption
http://www.ffiec.gov/ffiecinfobase/booklets/information_security/04_03_encryption.htm

[16] *US. Department of Health and Human services*, "Health Information Privacy'', http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[17] *US. Department of Health and Human services "*HIPAA Administrative Simplification", *Regulation Text*45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through February 16, 2006), http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf page 71

[18] "American Recovery and Reinvestment Act of 2009/Division A/Title XIII/Subtitle D", http://en.wikisource.org/wiki/American_Recovery_and_Reinvestment_Act_of_2009/Division_A/Title_XIII/Subtitle_D

[19] 42 USC §17938. Subtitle D Privacy HITECH ACT, http://www.aishealth.com/Compliance/Privacy_HITECH%20Act.pdf

[20] "HHS Strengthens HIPAA Enforcement", Friday, October 30, 2009, News Release, http://www.hhs.gov/news/press/2009pres/10/20091030a.html

[21]HITECH Act Breach Notification Guidance and Request for Public Comment, April 17, 2009, Health Information Privacy, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

[22]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 , Official Journal L 281 , 23/11/1995 P. 0031 - 0050 , EurLex http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[23]FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES, European Council, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[24] Safe Harbor Overview, January 14, 2010, http://www.export.gov/safeharbor/eg_main_018236.asp

[25] "Personal Information Protection and Electronic Documents Act", 2000, c. 5, Assented to April 13th, 2000, http://laws.justice.gc.ca/en/ShowDoc/cs/P-8.6//20090818/en?page=1

[26] Personal Information Protection and Electronic Documents Act (2000, c. 5)
Schedule 1 Section 5, 4.1.3, http://laws.justice.gc.ca/eng/P-8.6/page-4.html.

[27] Personal Information Protection and Electronic Documents Act (2000, c. 5)
Schedule 1 Section 5, 4.1.3, http://laws.justice.gc.ca/eng/P-8.6/page-4.html.

[28] "Role of the Privacy Commissioner of Canada", Office of the Privacy Commissioner, http://www.priv.gc.ca/information/guide_e.cfm

[29] "Guidelines for Processing Personal Data Across Borders", Privacy Commissioner of Canada, http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm

[30] "PCI SSC Data Security Standards Overview', https://www.pcisecuritystandards.org/security_standards/index.php

[31] "Requirements and Security Assessment Procedures Version 2.0, October 2010" Payment Card Industry (PCI) Data Security Standard, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[32] Glossary, Abbreviations and Acronyms', Payment Card Industry (PCI) Data Security Standard, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[33] Section A.1.1 to A1.1.4"Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers", Requirement https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[34] "Maintain an Information Security Policy" Requirement 12.8.2, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[35] "Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers", Requirement A.1https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[36] "Section A.1.2, Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers", https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[37] "Section A.1.3 and A.1.4, Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers", https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[38] Requirement 4: Encrypt transmission of cardholder data across open, public networks, Payment Card Industry (PCI) Data Security Standard,

https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[39] "Security Audit Procedures", Payment Card Industry (PCI) Data Security Standard https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf

[41] Crypto Law Survey Version 26.0, July 2010, http://rechten.uvt.nl/koops/cryptolaw/

[42]"A Guide to Software Encryption Export Compliance", BlackDuck Software http://www.blackducksoftware.com/media/_wp/SEEC-Guide.pdf

[43] Al Sacco, "BlackBerry maker to UAE, Saudis: No 3rd party can access encrypted data, not even us", Computer World, August 4, 2010 http://www.computerworld.com/s/article/9180145/BlackBerry_maker_to_UAE_Saudis_No_3rd_party_can_access_encrypted_data_not_even_us

[44] Crypto Law Survey Version 26.0, July 2010, http://rechten.uvt.nl/koops/cryptolaw/

[45] 'Warssenaar Arrangement on export controls for conventional arms, dual-use of goods and technologies", http://www.wassenaar.org/controllists/index.html

[46] "UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001", PUBLIC LAW 107–56—OCT. 26, 2001 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf

[47]Martha Peden, "Privacy is not absolute: An Update on the USA Patriot Act", Center for Constitutional Studies http://www.law.ualberta.ca/centres/ccs/issues/privacyisnotabsoluteanupdateontheusapatriotact.php

[48] "CRIMINAL MATTERS, REQUESTS FROM FOREIGN TRIBUNALS, AND OTHER SPECIAL ISSUES" (CT:CON-259; 06-23-2008) (OFFICE OF ORIGIN: CA/OCS/PRI,), http://www.state.gov/documents/organization/86744.pdf

[49] BCGEU v. British Columbia (Minister of Health Services), 2005 BCSC 446.

[50] Simon Hayes, "U.S. law raises privacy worries", News.com.au (2 November 2004) online: News.com, http://www.news.com.au/common/story_page/0,4057,11256981%255E15319,00.html

[51] MICHAEL GEIST AND MILANA HOMSI "OUTSOURCING OUR PRIVACY?: PRIVACY AND SECURITY IN A BORDERLESS COMMERICAL WORLD", AVAILABLE, WWW.MICHAELGEIST.CA/RESC/FINAL_UNB.DOC

[52] *In Re Investigation of World Arrangements* 13 F.R.D. 280, 285 (D.D.C. 1952). Quoted *In re Uranium Antitrust Litigation*, 480 F. Supp. 1138 at 1145.

[53] *Re Grand Jury Proceedings the Bank of Nova Scotia*, 740 F.2d 817 (11th Cir.1984) ("*Bank of Nova Scotia*")

[54] British Columbia Government and Services Employees' Union v. British Columbia (Minister of Health Services) *[*B.C. G.S.E.U*] [32]*

[55] CGI, News Release, "The Canada Revenue Agency Selects CGI for Key IT Initiatives" (9 December 2004) online:http://www.cgiusa.com/web/en/news_events/press_releases/2004/332.htm

[56] "Report of Findings", Elizabeth Denham Assistant Privacy Commissioner, August 2008 http://www.cippic.ca/uploads/OPC_Findings-canada.com.pdf

[57] Kim Zetter, FBI Defends Disruptive Raids on Texas Data Centers, April 7, 2009 http://www.wired.com/threatlevel/2009/04/data-centers-ra/