Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Integrating Best Practices for Cloud-Based Document Storage in Law Firms

CAPSTONE REPORT

Brianne Hansen
Assistant Controller
Rissman, Barrett, Hurt, Donahue, McLain, & Mangan, P.A.

University of Oregon
Applied Information
Management
Program

Spring 2017

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Integrating Best Practices for Cloud-Based Document Storage in Law Firms

Brianne Hansen

Rissman, Barrett, Hurt, Donahue, McLain and Mangan, P.A.

Abstract

The efficiencies, cost savings, and sustainability offered by today's technological innovations are compelling law firms to migrate their document storage to cloud-based environments. For law firms to store their documents within the cloud, they must develop best practices to address legal, ethical, and security issues. This annotated bibliography provides managing partners, executive directors, information directors, chief information officers, and controllers of law firms with literature focusing on these issues and potential solutions.

Keywords: cloud computing, cloud-based document storage, best practices, legal, ethical, security, privacy, law firms, and contract negotiations

Table of Contents

Introduction to the Annotated Bibliography

Problem

Technological advances are providing cloud-based services for law firms, which allow documents to be housed in offsite datacenters (Ambrogi, 2013). "Interest in 'CLOUD computing' is picking up steam among lawyers for several good reasons. Proponents say its advantages center on economy, simplicity and accessibility" (Acello, 2010, p. 28). Cloud-based document storage promotes these benefits through "on-demand file access, enhanced support, and reduced IT costs" (Burney, 2011, p. 53).

Cloud-based document storage has become a relevant part of most organizations; especially those who want to encourage sustainability (Garg & Buyya, 2011). Law firms, however, have been slower in this process compared to most other information-driven organizations, since they house very private and/or confidential documents (Burney, 2011). Although there are advantages to these cloud-based document services, there are still questions arising from lawyers regarding legality issues, ethics, security concerns, and the safeguards that need to be in place to protect their organizations (Burney, 2011, p. 53).

One concern for law firms contemplating cloud-based storage is where the servers are located (Mitchell & Meggison, 2014, p. 3). If these servers are located in a country outside of the United States, law firms have to consider if that country's government policies are protecting their clients' privacy or if their documents are subject to the other country's laws (Sinjilawi, AL-Nabhan, & Abu-Shanab, 2014). Examples of laws that can complicate the storage of legal documents outside of the United States include allowing foreign governments access to law firms' stored data, other legal disputes from geopolitical and jurisdictional issues (laws within other countries where servers are stored), and any legal requirements when handling particular

types of sensitive data such as health or financial information (Mowbray, 2009, pp. 135-136, 140).

The effort for law firms in ensuring that legal issues with cloud-based document storage are addressed is not a one-time effort, but instead requires ongoing diligence (Allen, 2011). Law firms must address legal concerns while utilizing cloud-based document storage, and the concerns can change with evolving technological advances (Pearson, 2013). Technology and the laws surrounding cloud storage change frequently, which mean law firms must make a commitment to ensuring their cloud-based document storage processes are reviewed, followed, and modernized on a regular basis (Pearson, 2013).

Law firms must also address security problems when using cloud-based document storage because documents are stored offsite and, therefore, outside of the physical control of the document owner (Pearson, 2013). In addressing security requirements for documents stored in the cloud, Pearson (2013) notes that "…to ensure the security of the processing of such information, data controllers must implement appropriate technical and organizational measures to protect it against: unauthorized access or disclosure, destruction, modification or unauthorized use" (p. 12). Another enhanced security risk is sharing "components and resources between subscribers who are unknown to each other. This feature may facilitate unauthorized access to a client's data by other subscribers (or by attackers who pose as subscribers) to exploit vulnerabilities in the cloud environment" (King & Raya, 2012, p. 309).

Ethics are an important consideration for any law firm handling medical documents, personal financial details, or any other case-related evidence reports (Allen, 2011). "Because cloud computing places data—including client data—on remote servers outside of the lawyer's direct control, it has given rise to some concerns regarding its acceptability under applicable

ethics rules" (American Bar Association, 2017). There are strict Health Insurance Portability and Accountability Act (HIPPA) laws regarding medical documents, which are continuously integrated in case files (Klein, 2011). Determining if the technology used to house medical documents complies with HIPAA standards is the responsibility of the organization; "HIPAA does not certify software as compliant or noncompliant, and it is therefore up to the institution to ensure that the requirements are met" (Klein, 2011, p. 574). When these files are stored onsite, lawyers must only be concerned that their own actions and those of their employees meet the necessary ethical standards (Pearson, 2013). Documents stored onsite can be kept safe with strong internal controls; however, when these files are stored offsite, lawyers must become concerned with the controls of the host company and whether the behavior of the businesses they use to house the documents meets their ethical standards (Pearson, 2013).

Adherence to laws, security, and high ethical standards are of the utmost importance when dealing with case files, evidence, and legal correspondence; therefore, these same concerns have restrained law firms from jumping into cloud-based document storage (Acello, 2010). Addressing these challenges is becoming increasingly imperative, as it has become inevitable that law firms will have to migrate to cloud-based document storage options in order to obtain and retain a competitive advantage (Brink, 2017). "This is why it's important law firms embrace cloud computing securely to ensure their workforce is working as smartly as possible and their IT systems are highly available" (Brink, 2017, Cloud is Vital to Remain Competitive, para. 2). Law firms seeking to adopt cloud storage of case files need to establish best practices for ensuring that the storage is handled legally, securely, and ethically.

Purpose

Cloud-based document storage can be an asset for law firms, but the question still remains if legal issues, ethical concerns, and security problems can be overcome (Burney, 2011). The purpose of this annotated bibliography is to present literature that addresses the legal, ethical, and security issues of law firms that store or are contemplating storing their data and documents in the cloud. Some of the literature provided covers legal issues when utilizing the cloud and suggestions on how law firms can stay compliant and retain confidentiality for their clients. Other sources identify security and privacy concerns coupled with potential solutions. Finally, literature is provided regarding ethical standards for law firms that house documents in the cloud.

Research Question

How do law firms establish best practices for ensuring that storage of their documents in the cloud is achieved legally, ethically, and securely?

Audience

The stakeholders who may benefit from this research include, but are not limited to, managing partners, executive directors, information technology (IT) directors, chief information officers, and controllers of law firms of any size. Managing partners are lawyers who manage the firm and sometimes participate on IT committees within their organizations that help to establish and approve all information technology tasks (Farkas, n.d.). As the top executives of the firm, the potential for legal, ethical, and security issues related to cloud storage of documents, and the solutions to address the concerns will be of key importance to these stakeholders.

Information technology directors manage the IT departments, create proposals and presentations on concerns about changes to software and hardware, and help implement changes

approved for the organization (Farkas, n.d.). Their interest in the information will be more direct, as these stakeholders are responsible for determining the IT policies and practices of the firm.

Executive directors typically oversee all employees who are not lawyers, manage a firm's day-to-day business, determine what information is worthy of managing partners' attention, and help manage activities so that the managing partners' valuable time is not wasted (Farkas, n.d.). A change from onsite to cloud storage of documents will have direct impact on the processes they and the employees of the firm use to access and store documents.

Finally, controllers oversee the accounting department, which utilizes important accounting software to scan and store invoices and other documents (Farkas, n.d.). A change in where these documents are housed and how they are accessed will impact their daily business practices.

All of these stakeholders will benefit from understanding the legal, ethical, and security concerns related to cloud-based document storage. Moreover, with knowledge from this study, these stakeholders can ensure their firms are adhering to best practices in maintaining ongoing procedures.

Search Report

Search strategy. This research paper focuses on cloud-based document storage for law firms. More specifically, the research identifies sources that describe best practices for ensuring that cloud-based document storage is handled legally, ethically, and securely. An initial search of literature was performed in the four following areas: (a) legal concerns, (b) ethical standards, (c) security, and (d) privacy.

Search engines. The search strategy involved using the UO Libraries' website and Google Scholar to discover relevant, peer-reviewed articles and other research papers for this topic.

Databases. The following databases proved useful in locating relevant articles: (a) Gale Databases, (b) Springer Link, (c) ProQuest Ebook Central, (d) ScienceDirect, (e) HeinOnline, and (f) De Gruyter.

Key terms. Key phrases used in the search for references were:

- cloud computing,
- cloud-based document storage,
- law firms migrating to the cloud,
- safeguard policies for the cloud,
- case studies in moving to cloud-based document storage,
- security issues with cloud-based document storage,
- law firms moving to the cloud,
- privacy and the cloud,
- ethical requirements for lawyers moving to cloud-based document storage,
- frequency of cloud-based document storage policies updated,
- HIPAA concerns in cloud computing, and
- contract negotiation for the cloud.

Documentation approach. All of the references for this research were documented in two ways. The first method of documentation was to detail the references in a Microsoft Excel spreadsheet, listing the author, title of source, year of publication, link to the source, and the database where the source is located. The references are grouped into categories that relate to the three topics of legal concerns with the utilization of cloud storage, ethical concerns with cloud computing, or security and privacy in the cloud. The second method for documenting the references is listing them in a Microsoft Word document. This list has all of the references in

order by author's last name and includes the abstract for each source. In addition, the sources are marked as being in the legal, ethics, or security category. This categorization allows for a quick reminder of which sources are potentially useful during different phases of research.

Reference evaluation criteria. The references for this research study were evaluated based on the Center for Public Issues Education (n,d.) document titled *Evaluating Information Sources*. This document details the importance of evaluating references on characteristics that include authority, timeliness, quality, relevancy, and bias. The document includes a list of red flags to consider when researching references online. These red flags, which included inflammatory language, typographical errors, broad generalizations, and persuasive point of views, were utilized in the research process of this study (Center for Public Issues Education, n.d.).

The authors of these references were considered to have good authority based on their credentials, places of employment, and the organizations that published their works. Authors with advanced degrees or other published books and articles and who were associated with reputable organizations were considered authorities. Timeliness was categorized by those references published within the last ten years, and the majority of sources selected were published within the last five years to ensure current information. Each reference was carefully reviewed to define the quality of the writing based on grammar, spelling, and punctuation (Center for Public Issues Education, n.d.). The relevancy for these references was established by researching scholarly sources instead of popular sources (Center for Public Issues Education, n.d.). Also, the sources were analyzed for relevancy in the three main topics of legal concerns, ethical considerations, and security related to the cloud storage of documents. Finally, each reference was reviewed to ensure there was no form of bias by making sure the author was

including differing perspectives and was not promoting a certain product or service (Center for Public Issues Education, n.d.).

Annotated Bibliography

The following references are annotated in order to demonstrate their applicability for this research. They are grouped alphabetically within the categories of legal, ethical or privacy/security concerns associated with the utilization of cloud storage. Each reference includes a citation, abstract, and summary to detail its relevance in the accompanying category, which address the research question.

Legal Concerns With the Utilization of Cloud Storage

Hon, W. K., Millard, C., & Walden, I. (2012, Fall). Negotiating cloud contracts: Looking at clouds from both sides now. *Stanford Technology Law Review 16*(1), 79-129. Retrieved from https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/cloudcontracts.pdf

Abstract. Contract terms for cloud computing services are evolving, driven by users' attempts to negotiate providers' standard terms to make them more suitable for their requirements, as well as market developments, particularly among cloud integrators. This Article, drawing on sources including interviews with cloud computing providers, users and other market actors, is the first in-depth research into how cloud contracts are negotiated. In particular, we have focused on instances where users have requested to changes to providers' standard terms, and the extent to which providers agreed to those changes. We have found that the terms that generated the most negotiation were provider liability, service level agreements, data protection and security, termination rights, unilateral amendments to service features, and intellectual property rights. Changes to providers' standard terms are likely to filter down from large deals where users have negotiated amendments, and filter up from regulatory action affecting the consumer market. This Article suggests a multiplicity of approaches are emerging,

rather than a de facto ‘cloud’ model, with market participants developing a range of cloud services with different contractual terms, priced at different levels, and embracing standards and certifications that aid legal certainty and compliance, particularly for small and medium-sized enterprise users.

Summary. This article provides qualitative research on negotiated cloud contracts. In their research, the authors found the six most popular types of terms negotiated. The six types of terms listed were exclusion or limitation of liability, service levels, security and privacy, lock-in and exit, providers’ ability to change service features, and intellectual property rights. These terms are all relevant to the legal implications of cloud computing.

Liability negotiations cover whether an organization wants unlimited liability or limited liability within its contracts. Service levels must be considered due to concerns over availability, reliability, and performance, since cloud computing consists of a combined network of various organizations sharing the same databases. Contract security and privacy terms should be negotiated because confidential information must be kept confidential or the law firms could face legal complications. Lock-in and exit are of high concern because of proprietary standards prevent data portability and the ability to export metadata. Providers’ ability to change service features is an important negotiation because organizations need to make sure there are strict stipulations on how, if, and when changes can be made to handle problems that arise from excess load on providers’ infrastructure due to numerous users or peak spikes in usage. Intellectual property rights are important in cloud computing because contract terms need to specify who owns the data so that an organization retains ownership of their own confidential documents.

All of these contract terms are relevant and important for law firms who want to adhere to legal, ethical, and secure standards when storing documents in the cloud. The authors conclude

that legislators and regulators need to be educated on cloud-based technologies in order to help reduce the legal concerns associated with using such technologies. The authors also explain that there needs to be more transparency by cloud service providers, specifically by providing more detail on the relationship between data location and data security.

Klein, C. A. (2011, December). Cloudy confidentiality: Clinical and legal implications of cloud computing in health care. *The Journal of the American Academy of Psychiatry and Law, 39*(4), 571-578. Retrieved from http://jaapl.org/content/39/4/571

Abstract. The Internet has grown into a world of its own, and its ethereal space now offers capabilities that could aid physicians in their duties in numerous ways. In recent years software functions have moved from the individual's local hardware to a central server that operates from a remote location. This centralization is called cloud computing. Privacy laws that speak to the protection of patient confidentiality are complex and often difficult to understand in the context of an ever-growing cloud-based technology. This article is a review of the legal background of protected health records, as well as cloud technology and physician applications. An attempt is made to integrate both concepts and examine Health Insurance Portability and Accountability Act (HIPAA) compliance for each of the examples discussed. The legal regulations that may inform care and standards of practice are reviewed, and the difficulties that arise in assessment and monitoring of the current situation are analyzed. For forensic psychiatrists who may be asked to provide expert opinions regarding malpractice situations pertaining to confidentiality standards, it is important to become acquainted with the new digital language from which these questions may arise.

Summary. This article covers topics of legal implications with cloud computing in health care. This information is relevant to this research study because law firms must comply with

federal HIPAA laws when handling evidence involving medical records. The author discusses the conflict with using the cloud for document management, storage, collaboration tools, databases, patient management, billing, webhosting, communication, teleconferencing, outsourcing of medical services, and cell phone applications. The conflict for each of these cloud-based services that promotes legal concerns is ensuring the rights of privacy. These services increase access to confidential information, increasing the potential for noncompliance in HIPAA regulations.

Klein also provides suggestions of how to address these legal implications, including using existing government tools, mitigation, de-identification, informed consent, and IT counsel. Government tools will help ensure administrative, physical, and technical safeguards are in place regarding HIPAA. Mitigation covers any security breaches or loss of data; HIPAA regulations specify the required steps that must be taken and the actions that must be documented. De-identification is a method of reassigning HIPAA compliant identifiers to prevent individual identities from being connected with the individuals' information stored in the cloud. Informed consent refers to providing patients the information on how these confidential documents will be kept and gaining their permission in advance. Finally, IT counsel can help organizations remain compliant with HIPPA regulations.

Mitchell, R. B., & Meggison, P. F. (2014). Strategies for integrating cloud computing concepts. *Journal of Applied Research for Business Instruction, 12*(2), 1-6. Retrieved from http://libproxy.uoregon.edu/login?url=http://search.proquest.com.libproxy.uoregon.edu/docview/1537962889?accountid=14698

Abstract. In an attempt to control IT costs and to increase technology agility, organizations are moving toward the utilization of cloud computing services at an astonishing

rate. The projection of cumulative jobs generated by cloud computing worldwide by 2015 is 13.8 million. Many of these will be in small-and medium- sized businesses. This shift requires that student have a more comprehensive knowledge base of this crucial aspect of today's IT environment, rather than just simple cloud applications such as virtual software.

Summary. This article details classifications of cloud systems, economic impacts of cloud computing, and legal risks of cloud computing. Classifications are listed as Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Business Process as a Service (BPaaS). The authors describe key legal risks of cloud computing, including confidentiality, privacy, data protection, regulatory compliance, and intellectual property concerns. As part of a solution to address these key risks, the authors include a section on available educational services and resources to promote understanding of the cloud by employees of cloud-based organizations to help reduce an organization's risk level, including services offered by Amazon (Amazon Web Services in Education), IBM (IBM Academic Initiative Program), and Microsoft (Microsoft Faculty Connection).

Mowbray, M. (2009). The fog over the Grimpen Mire: Cloud computing and the law. *Scripted, 6*(1), 132-146. Retrieved from https://script-ed.org/wp-content/uploads/2016/07/6-1-Mowbray.pdf

Abstract. This paper is about legal questions connected with cloud computing, the business trend in which computation is carried out on behalf of a user on remote machines, using software accessed through the Internet. The user may not know where these machines are: they are "somewhere in the cloud." Some of these legal issues will be resolved by standard agreements between buyers and vendors. I will give some examples from current agreements

from prominent cloud service providers. Other issues will probably end up in court. It makes sense to consider these questions now, before they become urgent.

Summary. This article focuses on legal questions regarding cloud computing. The legal concerns mentioned in this article include the location of servers housed by the cloud computing vendors, the reliability of these cloud computing vendors, and the contracts/agreements for cloud computing vendors. The location of these servers can be a legal complication if laws within the country of the customer that owns the document are not carried over into the country housing the servers. Reliability concerns include whether there are adequate safeguards in place to back up the data. Contracts/agreements should address those reliability concerns, location issues, and any other liability issues.

The author's solutions are a combination of technical solutions, business practices, and contracts between vendors and clients. Key suggestions include researching potential software vendors to identify and evaluate their business practices and hiring outside legal experts to review contracts with these vendors.

Wang, F. F. (2013). Jurisdiction and cloud computing: Further challenges to Internet jurisdiction. *European Business Law Review, 24*(5), 589-616. Retrieved from http://bura.brunel.ac.uk/bitstream/2438/8330/5/FullText.pdf

Abstract. As a result of technologic innovation and optimization, the advent of cloud computing may change the way we work, communicate with each other, and share information. In the cloud-based environment, access to computing resources (such as storage, processing, and software) has shifted from an internal network to a public network in particular in the public cloud environment. It may challenge the allocation of responsibility among cloud providers, cloud customers, and cloud users. Subsequently, it may affect the attribution of title to data

controllers and data processors. This paper undertakes primary research and provides insights into the significant yet complicated determination of the validity of jurisdiction clauses for cloud service contracts and the intertwined issues regarding the balance between the cloud interoperability and the protection of data privacy and intellectual property rights. It addresses key legal challenges faced by cloud computing providers and users today and proposes possible solutions to establish greater legal certainty in cloud computing service contracts with reference to the current practice in the EU and US. In general, this paper argues that although the development of cloud computing may complicate the determination of jurisdiction when disputes arise, a well-negotiated and sophisticated service contract of cloud computing may minimize such risk.

Summary. The main emphasis of this article is jurisdiction regarding cloud computing and the legal concerns that come with it. The author provides a list of general legal complications in cloud computing related to different models, the definition of parties, and balance. Legal complications posed by different models increase when combinations are used for layered services, such as Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS). The definition of parties raises legal concerns for cloud computing because some providers might carry more than one role. The legal complications of balancing in terms of cloud computing are spread across contract, torts, criminal law, jurisdiction, data protection, and other relevant matters causing risks between providers and clients.

Wang (2013) discusses the validity of jurisdictional clauses and their benefits, including the choice of court agreements for international jurisdiction. Wang recommends harmonization of international jurisdiction as a way forward to balancing potential conflicting interests. Finally,

the author explains special jurisdiction for rights infringement in data privacy protection and intellectual property protection for cloud service providers. Specific concerns in these areas are piracy and the security of confidential information. The conclusion suggests a sophisticated contract with the service provider as a potential solution to minimize the risks posed by the identified legal concerns and suggests that the contract cover the location and function of data centers. The author asserts that sophisticated contracts that include jurisdictional clauses to reduce the legal concerns posed by the location and function of data centers are key to balancing the potential conflicting interests of the parties.

Ethical Concerns With Cloud Computing

Acello, R. (2010, April). Get your head in the cloud: Despite ethics questions, law firms are storing client data on the net. *American Bar Association Journal*, *96*(4), 28-29. Retrieved from http://www.jstor.org/stable/41332805

Abstract. Interest in "Cloud computing" is picking up steam among lawyers for several good reasons. Proponents say its advantages center on economy, simplicity and accessibility. Cloud computing –also known as software as a service, or SaaS – is, in essence, a sophisticated form of remote electronic data storage on the Internet. Unlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored "in the cloud" is kept on large servers located elsewhere and maintained by a vendor.

Summary. This article concentrates on ethical questions for law firms who are storing client data in the cloud. Although the author mentions that it is an acceptable means of storing data, lawyers who choose to store client data in the cloud are still required to do their due diligence in maintaining ethical standards within their firms. The author includes safeguards that are deemed appropriate in establishing these ethical requirements as described by the American

Bar Association, including conducting due diligence and taking appropriate safeguards. Acello (2010) recommends that lawyers consult specialists on computer security in order to guarantee they are taking reasonable precautions.

Allen, J. (2011). Techno-ethics and the practice of law. *American Journal of Family Law, 24*(4), 211-217. Retrieved from http://go.galegroup.com/ps/i.do?p=AONE&sw=w&u=s8492775&v=2.1&it=r&id=GALE%7CA246098210&asid=2c5c26887b69816f5727f1de4d322258

Abstract. The technologies that can make us better, faster, and more efficient as lawyers and make our practice easier, more effective, and more efficient can, at the same time, place us at risk for ethical violations and expose us to malpractice liability. Most attorneys want to use technology to assist them in their practice. While some attorneys fear technology because they do not understand it, most fail to appreciate the dangers that improperly employed technology can pose to their practice and their pocketbook. Many attorneys have blissfully embarked on the use of technology, without a second thought to the risks associated with the employed technologies. In this article, we will explore the manner in which technology can turn on you, creating legal and ethical dilemmas.

Summary. The author of this article focuses on the evolution of technology and its ethical impacts on law firms. One specific section of this article addresses Software as a Service (SaaS), which is described as software that is housed on a vendor's server and is accessed by the client via a website. This means that the clients' information is stored in an offsite facility, which poses ethical dilemmas in the legal field. The article includes tips for helping protect ethical standards in law firms, which include checking the vendor's stability, verifying the vendor has a software escrow, determining if data can be stored on an in-house computer rather than on the

vendor's servers, confirming that the vendor's program converts data to a proprietary format, making sure the vendor has a secure connection, considering server security, and reviewing the server backup structure.

Burney, B. (2011, March-April). Flying safely in the cloud. *Law Practice Magazine*, *37*(2), 53. Retrieved from http://www.americanbar.org/publications/law_practice_magazine/2011/march_april/flying_safely_in_the_cloud.html

Abstract. Many lawyers have realized the advantages that cloud computing offers in terms of on-demand file access, enhanced support, and reduced IT costs. But owing to the skeptical soul of the legal profession, others have been hesitant to embrace the cloud owing to ethical responsibilities concerning client confidentiality. Technology, however, tromps forward without heed for the meticulous analysis of ethics committees, and it appears cloud computing solutions have become inevitable. The fundamental question, then, is how a lawyer's time-honored duty of confidentiality can be applied to the cloud.

Summary. This article provides information from a lawyer's perspective on cloud computing and the ethical concerns for law firms utilizing the cloud for storage. The author offers details on the rules regarding transmitting confidential information, including the need to take reasonable precautions in the cloud. The author notes that some states have differing laws regarding third-party storage and unauthorized access of data stored in the cloud. Finally, the author recommends numerous ideas on how a law firm could follow through with reasonable precautions in the cloud. These suggestions include verifying that the provider has technology to guard against security and privacy breaches and reviewing the geographical locations of the provider's datacenters to ensure the laws within other countries will cover all

agreements/contracts for the organization's main country and that all data can be protected from security breaches.

Dysart, J. (2011, April). The trouble with terabytes: As bulging client data heads for the cloud, law firms ready for a storm. *ABA Journal, 97*(4), 32-37, 62. Retrieved from http://www.jstor.org/stable/23034073

Abstract. Perhaps no case could be a more monumental example of the reality of modern e-discovery than the ongoing Viacom copyright infringement lawsuit against YouTube filed back in 2008. In that dispute, the judge ordered that 12 terabytes of data be turned over, according to Matthew Knouff. Experiences like these have left law firms and in-house attorneys scrambling to make sense of the new risks associated with the seemingly endless data produced by emerging technologies like cloud computing and social media – first as a way to get their own house in order and second as a sorely needed service for the vulnerable corporations employing them.

Summary. This article explores the risk involved with cloud computing related to the storage of data off-site under the control of a third-party vendor. The author details how these third-party vendors might not be as devoted to privacy or confidentiality as lawyers have to be, which can lead to ethical concerns for law firms. The author recommends approaches for law firms to overcome these new rising ethical concerns, such as creating an online resource for emerging practices and safeguards by the American Bar Association (ABA). The ABA's Commission on Ethics 20/20 Working Group released a paper, "Implications of New Technologies," seeking guidance from lawyers with questions to help provide the best possible answers for overcoming ethical concerns for law firms. The article notes that the questions

include topics from creating safeguard policies to whether law firms should purchase cyber insurance.

Security and Privacy in the Cloud

Buckman, J., & Gold, S. (2012, Fall). Privacy and data security under cloud computing. *College and University, 88*(2), 10-22. Retrieved from http://libproxy.uoregon.edu/login?url=http://search.proquest.com.libproxy.uoregon.edu/docview/1372330564?accountid=14698

Abstract. This article outlines privacy and data security compliance issues facing postsecondary education institutions when they utilize cloud computing and concludes with a practical list of do's and don'ts. Cloud computing does not change an institution's privacy and data security obligations. It does involve reliance on a third party, which requires an institution to implement practical and legal protections to facilitate compliance with such obligations.

Summary. The authors of this article provide background on cloud computing basics, U.S. privacy and data security law, and cloud computing do's and don'ts. The authors recommend that postsecondary institutions who are considering the use of cloud computing identify applicable security requirements, conduct due diligence, and negotiate effective contractual provisions. Specific suggestions include developing policies that establish the organization's ongoing best practices, managing cloud compliance by developing an ad hoc or permanent cross-functional team to establish requirements and research vendors, continuously evaluating cloud compliance policies to ensure they fulfill those requirements, conducting ongoing evaluations of security requirements to ensure confidential information is protected, and making sure the contracts cover all areas of concerns associated with privacy and security.

King, N. J., & Raja, V. T. (2012, June). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review, 28*(3), 308-319. https://doi.org/10.1016/j.clsr.2012.03.003

Abstract. The global ubiquity of cloud computing may expose consumers' sensitive personal data to significant privacy and security threats. A critical challenge for the cloud computing industry is to earn consumers' trust by ensuring adequate privacy and security for sensitive consumer data. Regulating consumer privacy and security also challenges government enforcement of data protection laws that were designed with national borders in mind. From an information privacy perspective, this article analyses how well the regulatory frameworks in place in Europe and the United States help protect the privacy and security of sensitive consumer data in the cloud. It makes suggestions for regulatory reform to protect sensitive information in cloud computing environments and to remove regulatory constraints that limit the growth of this vibrant new industry.

Summary. This article explains privacy and security risks that can be exacerbated with the use of cloud computing. These risks include having shared components between subscribers who are unknown to each other, increased system complexity that exposes more security vulnerabilities for hackers, exposing clients' applications over the internet, and inadequate external controls by the service providers. The authors also note the lack of federal laws to protect against such cloud vulnerabilities. Their suggestions on helping reduce these risks include expanding legal definitions of sensitive data that deserve heightened data protection and reducing regulatory constraints that limit both the European Union (EU) and the U.S. from taking full advantage of cloud computing.

Pearson, S. (2013). Privacy, security and trust in cloud computing. In S. Pearson & G. Yee (Eds.), *Privacy and security for cloud computing* (pp. 3-42). doi:10.1007/978-1-4471-4189-1_1

Abstract. Cloud computing refers to the underlying infrastructure for an emerging model of service provision that has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on information technology (IT) budgeting but also affect traditional security, trust and privacy mechanisms. The advantages of cloud computing—its ability to scale rapidly, store data remotely and share services in a dynamic environment—can become disadvantages in maintaining a level of assurance sufficient to sustain confidence in potential customers. Some core traditional mechanisms for addressing privacy (such as model contracts) are no longer flexible or dynamic enough, so new approaches need to be developed to fit this new paradigm. In this chapter, we assess how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed.

Summary. This article discusses privacy and security issues in relation to cloud computing. It states that the major privacy issues are trust, uncertainty, and compliance. Trust relates to unauthorized usage of confidential information. Uncertainty concerns ensuring that data is controlled; destroyed when appropriate; and is not breached, and if breached, knowing who is at fault. Compliance should ensure data locations globally are complying with trans-border data flow. The authors also identify security threats posed by the use of cloud computing; including unwanted access; gaps in security; and lock-ins, or easily transferring an organization's data from one provider to the next if a switch is needed. Solutions to these concerns are grouped

into three main dimensions: innovative regulatory frameworks, responsible company governance, and supporting technologies. Innovative regulatory frameworks cover areas of accountability in global business and provision of redress within the cloud. Responsible company governance requires cloud service providers to be responsible with the data by ensuring responsible behavior and accountability mechanisms, which balance innovation with individuals' expectations. Supporting technologies cover privacy-enhancing technologies that include security mechanisms, encryption, and anonymization.

Sinjilawi, Y. K., AL-Nabhan, M. Q., & Abu-Shanab, E. A. (2014, May). Addressing security and privacy issues in cloud computing. *Journal of Emerging Technologies in Web Intelligence*, *6*(2), 192-199. Retrieved from http://www.jetwi.us/uploadfile/2014/1210/20141210031010501.pdf

Abstract. Cloud computing is a new development of grid, parallel, and distributed computing with visualization techniques. It is changing the IT industry in a prominent way. Cloud computing has grown due to its advantages like storage capacity, resources pooling and multi-tenancy. On the other hand, the cloud is an open environment and since all the services are offered over the Internet, there is a great deal of uncertainty about security and privacy at various levels. This paper aims to address security and privacy issues threatening the cloud computing adoption by end users. Cloud providers are mindful of cloud security and privacy issues and are working hardly to address them. Few of these threats have been addressed, but many more threats still unsolved. This paper focused on cloud computing security and privacy threats, challenges, and issues. Furthermore, some of the countermeasures to these threats will be discussed and synthesized. Finally, possible solutions for each type of threats will be introduced before we end with conclusions and future work.

Summary. This article defines cloud security challenges as data segregation, authentication, privacy, policy integration, console security, recovery, and access to sensitive data. It also explains solutions for these challenges as Application Program Interface (API) standardization, legal support improvement, virtual machine improvement, and cryptography. All of these features are security measures to help aid in reaching acceptable levels of security for cloud computing. API standardization is needed to easily move from one provider to another because if one provider has their own API, the transfer to another provider who has a different API will cause problems. Improvement of legal support is needed to address contract negotiations and aid in guaranteeing sensitive data is secured. Improving virtual machines will ensure console security. Finally, cryptography, or converting data into unreadable text, addresses security concerns by preventing hackers or unauthorized individuals from having access to confidential information.

The privacy challenges mentioned in this article include shared resources, transferring data between countries, and the process of data collection. The authors recommend solutions include privacy-preserving methods to address the security concerns, including an anonymity-based method, a privacy-preserving authorization system, privacy-preserving architecture, and the Oruta (One Ring to Rule Them All) approach. The anonymity-based method is an algorithm that processes data and anonymizes either all or some of the information before releasing it to the cloud. The privacy-preserving authorization system works by allowing users to define their access policies and how to access their own data, which allows control in the cloud. A privacy-preserving architecture prevents both internal and external attacks with encryption and user access rights. Finally, the Oruta method is an approach coined by Boyang Wang and Baochun Li that achieves privacy-preserving auditing with three major entities: cloud server, third party

auditing (TPA), and users. These methods help to ensure the privacy of data is addressed according to an organization's needs.

Smallwood, R. F. (2012). *Safeguarding critical e-documents*. Hoboken, NJ: Wiley. Retrieved from http://ebookcentral.proquest.com.libproxy.uoregon.edu/lib/uoregon/detail.action?docID=821999

Abstract. Practical, step-by-step guidance for corporations, universities and government agencies to protect and secure confidential documents and business records. Managers and public officials are looking for technology and information governance solutions to "information leakage" in an understandable, concise format. Safeguarding Critical E-Documents provides a road map for corporations, governments, financial services firms, hospitals, law firms, universities and other organizations to safeguard their internal electronic documents and private communications. Provides practical, step-by-step guidance on protecting sensitive and confidential documents-even if they leave the organization electronically or on portable devices Presents a blueprint for corporations, governments, financial services firms, hospitals, law firms, universities and other organizations to safeguard internal electronic documents and private communications Offers a concise format for securing your organizations from information leakage In light of the recent WikiLeaks revelations, governments and businesses have heightened awareness of the vulnerability of confidential internal documents and communications. Timely and relevant, Safeguarding Critical E-Documents shows how to keep internal documents from getting into the wrong hands and weakening your competitive position, or possible damaging your organization's reputation and leading to costly investigations.

Summary. This book describes aspects of safeguarding confidential e-documents from security breaches. According to the author, intellectual property, crossing borders, and leaks or misuse of confidential information can be security concerns. The author states that the first major step in dealing with these concerns is implementing information governance, which is defined as how an organization maintains its security, complies with regulations, and keeps up with ethical standards when managing documents in the cloud. The author recommends approaching information governance by first implementing better policies and then implementing better technology. These two steps should encompass policies and technologies that manage what information is stored, where it is stored, the duration of the storage, and how the information is retained.

Waleed, A.-M., Chunlin, L., & Naji, H. A. H. (2014, December). The faults of data security and privacy in the cloud computing. *Journal of Networks, 9*(12), 3313-3320. Retrieved from https://pdfs.semanticscholar.org/e567/1c56fc297f24701331698c400816eb568b33.pdf

Abstract. According to Winkler [1], public cloud is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

The main benefits of using public cloud services include:

- Easy and inexpensive set-up.
- Scalability to meet needs.
- No resource wastage.

The term "public cloud" was invented to differentiate between the standard model and the private cloud, which is a proprietary network or data center that uses cloud-computing

technologies, such as virtualization. Examples of public clouds include Amazon Elastic Compute Cloud [2], IBM's Blue Cloud, and Sun Cloud. Despite of the advantages it also has some faults in its infrastructure. With the customer being unaware of their data storage over the internet, the problem is mainly the security and storage of client's data. In the paper the faults on security of their data storage and its privacy is reviewed. It also includes in it conducted experiment and statistical analysis using ubuntu simulation. The paper identifies the faults and proposes solutions to combat the identified problems.

Summary. This research paper focuses on cloud computing security challenges and provides a proposed solution. The authors stated that cloud computing security challenges include ensuring business continuity, disaster recovery, incident response, encryption, vulnerability assessment, identity access management, and virtualization. The authors assert that organizations must consider items like computer downtime and Internet connections associated with public cloud service providers as possible disadvantages for cloud computing because downtimes and lost Internet connections can result in outages. The proposed solution to help mitigate these problems is encryption of data with digital signatures, which provides clients with superset signatures and the encryption of metadata query results. The simulation tool recommended by the authors utilized several cryptographic methods. The authors stated that this simulation tool is helpful in ensuring security in the cloud and one of the most important ways to localize possible threats is through simulation and modeling.

Conclusion

Document storage has migrated from onsite filing cabinets to offsite electronic datacenters for many organizations because of advancements in technology (Allen, 2011). For law firms, particular challenges arise because of the confidentiality of the documents (Burney, 2011). This annotated bibliography documented 15 references that will help law firms integrate best practices to address legal and ethical concerns and security and privacy in storing their organizations' data in the cloud. These references were categorized into three groups: legal concerns with the utilization of cloud storage, ethical concerns with cloud computing, and security/privacy in the cloud. The literature suggests that law firms should create safeguard policies to integrate their established best practices (Acello, 2010; Burney, 2011; Dysart, 2011). Safeguard policies are defined as the practices where "the lawyer took appropriate steps to safeguard the information from inadvertent or unauthorized disclosure" (Acello, 2010, p. 28).

Legal Concerns With the Utilization of Cloud Storage

Multiple researchers identified contract negotiations, location of servers, and HIPAA violations for storing documents in the cloud as legal concerns related to cloud storage (Hon, Millard, & Walden, 2012; Klein, 2011; Mitchell & Meggison, 2014; Mowbray, 2009; Wang, 2013). Hon et al. (2012) note that cloud service providers' contracts typically contain standard terms that emerge after large deals where users have negotiated amendments and from related regulatory actions; these standard terms sometimes pose problems for customers. Hon et al. identified the contract terms that generated the most requests for amendment as provider liability, service level agreements, data protection and security, termination rights, unilateral amendments to service features, and intellectual property rights.

Mowbray (2009) describes the location of cloud servers as a potential legal complication if laws within the country of the customer that owns the document are not carried over into the country housing the servers. Klein (2011) identifies the potential for noncompliance with HIPAA regulations as a key concern for organizations who store patient-related documents in the cloud due to increased access to confidential patient information.

Hon et al. (2012) established six types of terms within contract negotiations that will help aid in reducing legal concerns: exclusion or limitation of liability, service levels, security and privacy, lock-in and exit, providers' ability to change service features, and intellectual property rights. Liability negotiations cover whether an organization wants unlimited liability or limited liability within its contracts. Service levels must be considered due to concerns over availability, reliability, and performance, since cloud computing consists of a combined network of various organizations sharing the same databases. Contract security and privacy terms should be negotiated because confidential information must be kept confidential or the law firms could face legal complications. Lock-in and exit are of high concern because proprietary standards prevent data portability and the ability to export metadata. Providers' ability to change service features is an important negotiation because organizations need to make sure there are strict stipulations on how, if, and when changes can occur to handle problems regarding how the load on providers' infrastructure will handle numerous users or peak spikes in usage. Intellectual property rights are important in cloud computing because contract terms need to specify who owns the data so that an organization retains ownership of their own confidential documents (Hon et al., 2012).

Wang (2013) stated, "It is suggested that the insertion of jurisdictional clauses in Terms of Service in cloud computing will reduce the legal uncertainty in ascertaining connecting factors in particular the location and function of data centers" (p. 616). Klein (2011) asserts that HIPAA

legal risks can be reduced by using government tools, mitigation, de-identification, informed consent, and IT counsel. Klein notes that government tools will help ensure administrative, physical, and technical safeguards are in place regarding HIPAA. Mitigation covers any security breaches or loss of data; HIPAA regulations specify the required steps that must be taken and the actions that must be documented. De-identification is a method of reassigning HIPAA compliant identifiers to prevent individual identities from being connected with the individuals' information stored in the cloud. Informed consent refers to providing patients with information on how these confidential documents will be kept and gaining their permission in advance. Finally, IT counsel can help organizations remain compliant with HIPPA regulations (Klein, 2011).

Ethical Concerns With Cloud Computing

Ethical concerns were determined to be a crucial consideration for law firms utilizing the cloud for document storage (Acello, 2010; Allen, 2011). Jeffrey Allen, a lawyer since 1973, addresses the ethical concerns posed by the use of Software as a Service (SaaS), which is described as software that is housed on a vendor's server and is accessed by the client via a website. Allen (2011) noted that ethical dilemmas in the legal field are posed because clients' information is stored in offsite facilities, and provided recommendations to help protect law firms' ethical standards when utilizing SaaS. The key advice includes checking the vendor's stability, verifying the vendor has a software escrow, determining if data can be stored on an in-house computer rather than on the vendor's servers, confirming that the vendor's program converts data to a proprietary format, making sure the vendor has a secure connection, considering server security, and reviewing the server backup structure (Allen, 2011, pp. 216-217).

Law firms can adhere to ethical standards when utilizing the cloud by taking reasonable precautions (Acello, 2011; Burney, 2011). These precautions include verifying that the provider has technology to guard against security and privacy breaches and reviewing the geographical locations of the provider's datacenters to ensure the laws within other countries will cover all agreements/contracts for the organization's main country, and that all data can be protected from security breaches (Burney, 2011). Acello (2010) recommends that lawyers consult specialists on computer security in order to guarantee the law firm is taking reasonable precautions.

Because the topic of ethical standards in cloud computing is still evolving today, the American Bar Association's Commission on Ethics 20/20 Working Group released a paper on Implications of New Technologies, requesting guidance from attorneys on confidentiality issues related to the use of cloud services so that the committee members could develop a more thorough understanding of how to make sure law firms are held to the right ethical standards when using these services. The questions covered topics of creating online policies, amending ABA policies, and whether law firms should purchase cyber insurance (Dysart, 2011).

Security and Privacy in the Cloud

Security and privacy in the cloud are vital and necessary components when using cloud-based document storage for sensitive data (King & Raja, 2012). Buckman and Gold (2012) note that an institution's data security and privacy obligations do not change with the use of a cloud service provider and present specific suggestions to meet these obligations. Their suggestions include: (a) developing policies that establish the organization's ongoing best practices, (b) managing cloud compliance by developing an ad hoc or permanent cross-functional team to establish requirements and research vendors, (c) continuously evaluating cloud compliance policies to ensure they fulfill those requirements, (d) conducting ongoing evaluations of security

requirements to ensure confidential information is protected, and (e) making sure the contracts cover all areas of concerns associated with privacy and security (Buckman & Gold, 2012).

Smallwood (2012) notes the importance of implementing information governance to safeguard confidential e-documents and recommends as an approach first implementing better policies and then implementing better technology. Smallwood asserts that these two steps should encompass policies and technologies that manage what information is stored, where it is stored, the duration of the storage, and how the information is retained.

When dealing with trust, uncertainty, and compliance, Pearson (2013) provided three categories of recommendations: innovative regulatory frameworks, responsible company governance, and supporting technologies. Innovative regulatory frameworks cover areas of accountability in global business and provision of redress within the cloud. Pearson's approach to responsible company governance requires cloud service providers to be responsible with the data by ensuring responsible behavior and accountability mechanisms, which balance innovation with individuals' expectations. Supporting technologies cover privacy-enhancing technologies that include security mechanisms, encryption, and anonymization (Pearson, 2013).

Sinjilawi, AL-Nabhan, and Abu-Shanab (2014) suggest API standardization, legal support improvement, virtual machine improvement, and cryptography as necessary steps to achieve security in the cloud. API standardization among cloud service providers is needed to enable customers to easily move from one provider to another because if one provider has a proprietary API, the transfer to another provider who has a different API will pose challenges. Improvement of legal support is needed to address contract negotiations and aid cloud customers in obtaining guarantees from their service providers that their sensitive data is secured. Improving virtual machines helps to ensure console security. Finally, cryptography, or

converting data into unreadable text, addresses security concerns by preventing hackers or unauthorized individuals from having access to confidential information (Sinjilawi et al., 2014). These supporting technologies help to keep information confidential and easily transferrable between providers if contracts are terminated for whatever reason (Sinjilawi et al., 2014).

Summary

While advancements in technology have pushed the use of cloud storage into the mainstream, it is still an ever-evolving environment (Allen, 2011). Law firms that wish to store documents in the cloud must first address legal, ethical, and security concerns (Acello, 2010; Allen, 2011). A lawyer's fundamental duty to protect the confidentiality of a client's information remains the same regardless of whether that information is in a stack of papers on a desk or stored in an offsite data center 3,000 miles away (Burney, 2011). Integrating best practices when storing documents in cloud-based storage environments while continuously updating safeguard policies will keep help these law firms to remain compliant and avoid legal, ethical, and security issues (Acello, 2010; Allen, 2011; Buckman & Gold, 2012; Burney, 2011; Hon, Millard, & Walden, 2012; Klein, 2011; Pearson, 2013; Sinjilawi, AL-Nabhan, & Abu-Shanab, 2014; Smallwood, 2012; Waleed, Chunlin, & Naji, 2014; Wang, 2013).

References

Acello, R. (2010, April). Get your head in the cloud: Despite ethics questions, law firms are storing client data on the net. *American Bar Association Journal*, *96*(4), 28-29. Retrieved from http://www.jstor.org/stable/41332805

Allen, J. (2011). Techno-ethics and the practice of law. *American Journal of Family Law, 24*(4), 211-217. Retrieved from http://go.galegroup.com/ps/i.do?p=AONE&sw=w&u=s8492775&v=2.1&it=r&id=GALE%7CA246098210&asid=2c5c26887b69816f5727f1de4d322258

Ambrogi, R. (2013). High in the cloud. *ABA Journal*, *99*(11), 30. Retrieved from http://go.galegroup.com/ps/i.do?p=AONE&sw=w&u=s8492775&v=2.1&it=r&id=GALE%7CA350976639&asid=cf4f774bc30aa046d3d163c4a06f24f9

American Bar Association. (2017). Cloud ethics opinions around the U.S. Retrieved from https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html

Brink, M. (2017, February 17). The ruling on cloud computing: Analysing the legal perspective. CloudTech. Retrieved from https://www.cloudcomputing-news.net/news/2017/feb/17/ruling-cloud-computing-analysing-legal-perspective/

Buckman, J., & Gold, S. (2012, Fall). Privacy and data security under cloud computing. *College and University*, *88*(2), 10-22. Retrieved from http://libproxy.uoregon.edu/login?url=http://search.proquest.com.libproxy.uoregon.edu/docview/1372330564?accountid=14698

Burney, B. (2011, March-April). Flying safely in the cloud. *Law Practice Magazine*, *37*(2), 53. Retrieved from

http://www.americanbar.org/publications/law_practice_magazine/2011/march_april/flying_safely_in_the_cloud.html

Center for Public Issues Education. University of Florida. (n,d.). *Evaluating information sources*. Retrieved from http://ae-coursematerials.uoregon.edu/aim/Capstone1Perm/evaluateinfo.pdf

Dysart, J. (2011, April). The trouble with terabytes: As bulging client data heads for the cloud, law firms ready for a storm. *ABA Journal, 97*(4), 32-37, 62. Retrieved from http://www.jstor.org/stable/23034073

Farkas, B. (n.d.). *Who works at a law office (lawyers and others)*. Retrieved from Lawyers.com website: http://research.lawyers.com/identifying-the-people-who-work-at-a-law-office.html

Garg, S. K., & Buyya, R. (2011). *Green cloud computing and environmental sustainability*. Retrieved from http://www.cloudbus.org/papers/Cloud-EnvSustainability2011.pdf

Hon, W. K., Millard, C., & Walden, I. (2012, Fall). Negotiating cloud contracts: Looking at clouds from both sides now. *Stanford Technology Law Review, 16*(1), 79-129. Retrieved from https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/cloudcontracts.pdf

King, N., & Raja, V. T. (2012, June). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review, 28*(3), 308-319. https://doi.org/10.1016/j.clsr.2012.03.003

Klein, C. A. (2011, December). Cloudy confidentiality: Clinical and legal implications of cloud computing in health care. *The Journal of the American Academy of Psychiatry and Law, 39*(4), 571-578. Retrieved from http://jaapl.org/content/39/4/571

Mitchell, R. B., & Meggison, P. F. (2014). Strategies for integrating cloud computing concepts. *Journal of Applied Research for Business Instruction, 12*(2), 1-6. Retrieved from http://libproxy.uoregon.edu/login?url=http://search.proquest.com.libproxy.uoregon.edu/docview/1537962889?accountid=14698

Mowbray, M. (2009). The fog over the Grimpen Mire: Cloud computing and the law. *Scripted, 6*(1), 132-146. Retrieved from https://script-ed.org/wp-content/uploads/2016/07/6-1-Mowbray.pdf

Pearson, S. (2013). Privacy, security and trust in cloud computing. In S. Pearson & G. Yee (Eds.), *Privacy and security for cloud computing* (pp. 3-42). doi:10.1007/978-1-4471-4189-1_1

Sinjilawi, Y. K., AL-Nabhan, M. Q., & Abu-Shanab, E. A. (2014, May). Addressing security and privacy issues in cloud computing. *Journal of Emerging Technologies in Web Intelligence, 6*(2), 192-199. Retrieved from http://www.jetwi.us/uploadfile/2014/1210/20141210031010501.pdf

Smallwood, R. F. (2012). *Safeguarding critical e-documents*. Hoboken, NJ: Wiley. Retrieved from http://ebookcentral.proquest.com.libproxy.uoregon.edu/lib/uoregon/detail.action?docID=821999

Waleed, A.-M., Chunlin, L., & Naji, H. A. H. (2014, December). The faults of data security and privacy in the cloud computing. *Journal of Networks, 9*(12), 3313-3320. Retrieved from https://pdfs.semanticscholar.org/e567/1c56fc297f24701331698c400816eb568b33.pdf

Wang, F. F. (2013). Jurisdiction and cloud computing: Further challenges to Internet jurisdiction. *European Business Law Review, 24*(5), 589-616. Retrieved from http://bura.brunel.ac.uk/bitstream/2438/8330/5/FullText.pdf