Title:		**NA14: Trust in Cloud Service Contracts – Final Report**
Status:		Final
Version:		5.1
Date submitted:		February 29, 2016
Last reviewed:		May 29, 2018
Author:		InterPARES Trust Project
Writer(s):		Jessica Bushey, Marie Demoulin, Elissa How, Robert McLelland
Research domain:		Legal
URL:		
Project lead:		Marie Demoulin

Document Control

Version history			
Version	Date	By	Version notes
1	August 24, 2015	RM, EH	
2	September 19, 2015	JB	
3	February 11, 2016	RM, MD, JB, EH	
4	February 28, 2016	MD, EH	Changes made following InterPARES Trust Plenary in Vancouver, BC.
5	March 10, 2016	JB	Final Edit
5.1	May 29, 2018	Corinne Rogers	Copy edit

This study does not constitute legal advice. The authors do not recommend for or against any particular cloud service provider (or the use of cloud services in general). Individuals and organizations should consult legal counsel if they want legal advice on a particular contract.

Trust in Cloud Service Contracts

An InterPARES Trust Project

1. Introduction

The 'cloud', a term used to describe a wide array of scalable services for the storage, access, and use of information, is increasingly being used in the everyday business activities of organizations worldwide. The apparent ease and cost-effectiveness with which these services can be adopted to store large amounts of information has made them an attractive option for many organizations and has increased the likelihood that such services will be used to store organizational records.

Despite the benefits that can be found in the utilization of cloud services, the risks associated with the storage of vital business records in such a service are not well understood, and can result in records that are not kept in accordance with legal requirements and best practices in the field of archives and records management. In order to utilize the benefits of these services, organizations of all kinds need the support of their records managers and archivists to ensure that records kept in such services will remain authentic. To achieve this, there is a need for a tool which can be utilized to help guide recorded information professionals and their organizations in choosing services that will fulfill their recordkeeping needs. This tool is the "Checklist for Cloud Service Contracts" developed within the scope of the present research (see also Appendix A).

2. Purpose and Scope of Study

Legal contracts reflect the fundamental basis for the services provided by cloud companies to their customers. These agreements are often written solely by the service provider, presented in 'boilerplate' format, and as a result largely reflect the needs of the company over the customer. Such agreements can lead to an imbalance of power in business relationships and can establish uncertainty in what is required by each party. As such, customers may agree to such agreements without significantly understanding how their use of the service will affect their recordkeeping and the legal, professional, and ethical obligations therein. The researchers acknowledge that it is likely that larger organizations have the ability to negotiate their own contracts with service providers. However, many smaller organizations do not have this capacity and are using boilerplate contracts. In addition, some of them cannot afford corporate cloud services and rather use individual public cloud services.

Given these realities, this project was conceived to establish what needs exist for recordkeeping and long-term records preservation in a cloud environment based on professional standards and legal requirements. Considering these needs, the project was initially slated to develop a model cloud-computing contract that could be used as the basis for the development of more equitable agreements between cloud service providers and their customers. As this study progressed, however, it became clear that developing a model contract for use by various organizations and their service providers would be problematic as individual cases, capabilities, provider capacities and legal tradition may change how the services are enacted. In light of this, the original intent to develop a model contract was shifted to the production of a tool that would enable organizations to determine whether potential service contracts meet the standards for recordkeeping systems promulgated by the records

management and archival community. This tool would be based on recordkeeping standards for the purposes of ensuring the trustworthiness (i.e., accuracy, reliability and authenticity) of digital records held within the system.

In this respect, the researchers settled on the creation of a checklist of requirements that could be easily applied to terms by a recordkeeping professional to assess whether a potential contact meets the needs of her organization in employing cloud services in their records program. This checklist was designed to be as simple to use as possible, as the researchers felt that the less complex the tool was, the greater the likelihood that it would be used and the easier it would be to communicate the results of its use to other stakeholders within the organization. This research builds upon the results of another InterPARES Trust study, Project 10 - Contract Terms with Cloud Service Providers, to cover the gaps that it discovered in boilerplate contracts. It also expands the work conducted by Project 10 by raising additional legal and archival issues.

The target audience of this Checklist for Cloud Service Contracts is records managers, archivists, chief information officers, and others who are assessing cloud services for their organization. The aim of this document is to provide a tool to:

- gain an understanding of boilerplate cloud service contracts;
- verify if potential cloud service contracts meet their needs;
- clarify recordkeeping and archival needs to legal and IT departments;
- communicate recordkeeping and archival needs to cloud service providers.

Although it is not directly targeted at lawyers and cloud service providers, it might also help them to understand the needs of their customers in terms of recordkeeping in the cloud.

It must be noted that this checklist is a tool for consideration only and does not constitute legal advice. Individuals and organizations should consult legal counsel if they want legal advice on a particular contract.

3. Methodology

This study undertook an interdisciplinary approach to conduct its research, reviewing literature on cloud services from the fields of archival science, records management and law. This review included professional standards and guidelines; governance documents, reports, and recommendations regarding the adoption of cloud technologies and their agreements; academic papers discussing the issues involved with cloud technologies and the law, as well as legal cases and their decisions. This literature review provided the basis of the authors understanding of what should be included in a cloud-based recordkeeping program. This literature is discussed in greater detail in section 5. An annotated bibliography is available on the public area of the InterPARES Trust website (see also Appendix B).

This enabled the authors produce a collection of baseline needs for a recordkeeping system employing cloud technology by incorporating the viewpoints of multiple common stakeholders within a record producing body. These baseline needs spanned data ownership; availability, retrieval and use of the data; data storage and data preservation; data retention and disposition; security, confidentiality and privacy; data location and cross-border data flow; end

of service and termination of the contract. These areas closely matched those used in Project 10's preliminary research, but were re-organized and expanded as needed. These categories are discussed in greater detail in section 7. With the establishment of these categories, the authors drafted questions for each that were meant to guide a records professional through determining whether a cloud service contract meets their needs (as identified by this project).

The authors then sought an array of contracts with which to test the usefulness of the questions. Considering the purpose of the study, the analysis focused on cloud services that were relevant for recordkeeping purposes. As many small organizations cannot afford corporate services, individual cloud services were examined as well. In the interest of expediency, only publicly available boilerplate contracts from cloud service providers were selected. Moreover, only contractually binding documents such as terms and conditions, service level agreements, privacy policies, acceptable use policies, etc. were taken into consideration. Marketing material or other information (such as white papers, guides, etc.) on the providers' websites were not analyzed, as they are not part of the contract. Ultimately, contracts from 15 companies were selected. These contracts spanned multiple jurisdictions, especially Canada, the United States and a few European countries. They were most often broken up into several smaller agreements based on which services a customer was purchasing.

The selected contracts were analyzed in order to test how comprehensive they were in meeting recordkeeping needs and to determine the relevance of the questions in assessing the compatibility of a service with the recordkeeping obligations of an organization within the terms being offered. Based on this analysis, recommendations were developed for bridging existing gaps between terms and agreements that serve the provider as well as the recordkeeping needs of the customer. The analysis and the recommendations are discussed in greater detail in section 6 and 7.

These recommendations and the collection of questions were then used to create a checklist to guide the assessment of contracts for recordkeeping and legal needs. A draft of this checklist was disseminated to the InterPARES Trust project at large for the purposes of receiving feedback during fall 2015. The feedback period lasted approximately a month, during which over 45 responses were received. These responses were reviewed, discussed, and accepted or rejected based on whether they were within the scope of the project's intention. The result was the deletion, addition, and rewording of a number of checklist questions and the addition of footnotes to contextualize, explain or provide examples when necessary. The final checklist is available on the public area of the InterPARES Trust website (see also Appendix A).

4. Terminology

As this study and the InterPARES Trust Project are interdisciplinary research pursuits, the terminology used within this report may be interpreted differently depending on the perspective of the reader. For this reason, every effort has been made within the report to utilize the InterPARES Trust Terminology Database for key language. When necessary, reference is made to specific definitions provided by governance documents such as recordkeeping standards and legal acts.

Another issue with terminology associated with this research is the general lack of standardization that exists within cloud service contracts themselves. Therefore, it should be assumed that terminology used by the researchers themselves adheres to the InterPARES Trust Terminology Database. For example, the term "record" means "a document made or received in the course of a practical activity as an instrument or a by-product of such activity that is set aside for action or reference"; the term "information" refers to "an assemblage of data intended for communication either through space or across time"; and the term "data" refers to "the smallest meaningful units of information".

Other terms employed by cloud service contracts that also bear clarification from the InterPARES Terminology Database are security, confidentiality, and privacy. Drawing from the terminology database, the researchers use the terms thusly: "security" means "the state of being protected from attack, risk, threat, or vulnerability"; "confidentiality" means "the expectation that private facts entrusted to another will be kept secret and will not be shared without consent"; and "privacy" means "control over access and use of one's personal information". The term "availability" is also regularly referenced in cloud service contracts, typically regarding how often the service will be available. When the term is used by the researchers, it is used in the InterPARES Trust definition of "capability of being accessed or used". (Definition is a draft from 2015-03-19 accessed on 2016-02-27.)

Finally, this report refers to several terms from archives and records management: retention, disposition, and auditing. As of the writing of this report, the database did not have a definition drafted for "retention", but did have an entry for "retention schedule" which is defined as "a document providing description of records series and/or classes and specifying their authorized dispositions". Retention can therefore be considered the keeping of a record for the period of time mandated before its disposition. "Disposition" is defined by the terminology database as "records' final destruction or transfer to an archives as determined by their appraisal". "Audit" is used in this paper in relation to records and a recordkeeping system. InterPARES Trust defines an audit as "the systematic assessment of compliance with established policies, procedures, laws, and standards". In this case, the policies, procedures, laws, and standards that govern the keeping of authentic records in a particular organization.

5. Literature Review

In order to establish a foundation for considering the requirements of a recordkeeping system regardless of medium, the authors undertook a literature review. This literature review focused on current research on cloud service agreements, cloud case law and scholarly discussion regarding the legal ramifications of cloud computing, as well as an examination of the current records management standards that exist which might offer guidance for those considering contracting in the cloud. The findings of the literature review influenced our creation of a checklist and are summarized in brief below.

5.1 Recent Studies on Cloud Computing

When examining recent literature on cloud computing contracts, the authors concentrated on those studies that stemmed from the perspective of archival science, records

management, and legal studies. This examination revealed that while different cloud service providers differed in approach, in general the Terms and Service Agreements tended to be broken down into several legal documents such as Terms of Service; a document for more specific services such as the Service Level Agreement, and documents covering other general areas such as the Privacy Policy, and the Acceptable Use Policy (Bradshaw, Millard and Walden, 2011, 44). The relevant literature suggests that not only is there very little standardization of terms across providers' agreements (Baset, 2012) but it also suggests that the manner in which such contracts are written can support the view that they are "…incomprehensible to the vast majority of users." (Bradshaw, 2013, 32)

Indeed, the literature further suggests that such contracts typically offer wide-ranging exclusions of liability that favor the provider (Bradshaw, 2013, 30) to the extent that small organizations possess such little bargaining power (Walden, 129) and face scant option beyond risking signing this type of standard contract or avoid cloud services in general (Oppenheim, 454). The authors also noted that studies have been conducted that examine the legal framework for the use of cloud based services by the federal and provincial authorities (Vermeys et al., 2014). Finally, of particular note, the literature review underscores that it is in the best interests of organizations to conduct adequate due diligence before signing any such contract, and, additionally, to conduct adequate ongoing monitoring to ensure the needs of each individual organization are met (Stiven, 423-424).

5.2 Cloud Case Law and Related Articles

During the literature review cloud case law and related articles, two key points quickly became apparent. First, while, there have yet been relatively few cases decided that deal specifically with cloud contracts, numerous well-established legal tenets come into play that will likely impact any future cases in this area. Second, this subject is complex not only by different legal approaches in different jurisdiction but also by different legal requirements in different industries. As a result, current cloud case law and related articles reveal a complexity that makes sweeping generalizations challenging. In order to address this, the authors focused on the following key areas of the law (themselves often interrelated and overlapping) and how these areas relate to cloud contracts: traditional contract law; privacy, access, confidentiality and security with respect to data; and data jurisdiction/conflict of laws.

Traditional contract law, especially within the field of Information Technology (IT) can be seen as having a solid connection to cloud contract law; however, the literature reveals that cloud contract law is not merely an extension of IT law (Pasquale, 600). Indeed, new technologies and new perils alike, such as the issue of coverage and contract applicability with outsourcing (Pasquale, 600) often come into play. Indeed, when dealing with contracts on the internet, those considering contracting in the cloud must consider the validity of contract law when dealing with such phenomena as clickwrap contracts (where the contract is indicated by clicking online on button) and browserwrap contracts (where the contract is indicated by mere use) (Zimmeck, 453). Furthermore, traditional legal issues such as unconscionability might be an issue when dealing with parties with unequal bargaining powers as is often the case with cloud contracts (Zimmeck, 458).

Likewise, there is little question of the importance of privacy and security in relation to cloud computing given the ease of transferring and sharing information, often across jurisdiction borders. Case law and related articles that deal specifically with privacy in the cloud underscore that not only do different jurisdictions approach privacy different with different guiding laws, but depending on the jurisdiction, specific industries and sectors of industry might be governed by different laws. In Canada, for example, the literature demonstrates that the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") governs private sector organizations in most provinces; however, certain provinces have different governing legislation. (Gratton, 3). In the United States, a sectorial approach to privacy legislation exists (Billings, 241) so that certain industries have different regulating bodies created for different industries potentially affecting cloud computing (Ryan, 507). Additionally, differing jurisdictions have different case law precedents that can change quickly. For example, in Ontario, recently the Court of Appeal confirmed the new tort "seclusion from intrusion" that might have series repercussions for institutions in Ontario that deal with personal information (*Jones v. Tsige*, [2012] ONCA 32, 108 O.R. (3d) 241; Ha-Redeye, 23). Thus, it is clear from the literature that privacy law, with respect to the cloud, is complex and governing law depends on many factors thus making it particularly important for records managers and archivists alike to consider the prevailing legal paradigm in their particular region and industry.

Another important issue with respect to cloud contracts is the issue of conflict of laws, which refers in general to the legal jurisdiction in which any legal action will take place. Given that data stored in the cloud generally passes through many jurisdictions it can be viewed as potentially subject to a phenomenon that has been called "superterritoriality" (Billings, 214). The authors note that where no choice of law provision exists, different jurisdictions turn to different legal tests to determine personal jurisdiction (Maddex 10-12) though, with cloud contracts, typically there is consideration given to choice of law in the body of documents that creates the contract. (Wang, 596) More specifically, the literature confirms that while it may be possible for large organizations to negotiate nuanced and comprehensive choice of law provisions, most often it is the cloud service provider that dictates such a choice, and, of course, this reality might have serious potential ramifications on the part of the contracting parties.

Such provisions can also lead to complications with sub-contractors (Wang 598) and can also be further complicated by the issue of data localization. In certain jurisdictions, in certain industries, a wide variety of laws (Chander 680) require that data remain within the physical boundaries of a country or jurisdictional area. (Aaronson, 5) Such requirements add challenges to those wanting to contract in the cloud. In short, the literature supports that this is a complex area where that demands serious forethought on the part of contracting parties.

5.3 Recordkeeping Standards, Cloud Computing Contract Standards, and Related Articles

In order to consider the requirements of recordkeepers and archivists when storing and working in the cloud, the authors considered various standards and guidelines established by international organizations that deal with recordkeeping requirements. This consideration started with ISO's report *ISO 15489-1* (ISA 2001, 1), a report that ultimately grew to become ISO's standard for records management. This standard establishes the guidelines for how records should be kept and maintained in public and private organization, regardless of the form

in which the records are being kept. *ISO 15489*-1 does not, however, include a direct consideration of archival preservation. Therefore, the authors turned to additional ISO sources such as ISO's report *ISO 14721* in order to augment their review of relevant standards.

*ISO 14*721 offers a reference model for an open archival information system with the aim of permitting a designating community to preserve records and information kept in a digital environment. (ISO 2012). This standard was consulted in order to approach the analysis of cloud service agreements from an archival perspective. Approaching the issues from an archival perspective, where information may need to be preserved indefinitely. This is particularly important for this project, given that any organization that considers this type of long-term preservation will need to carefully examine relevant clauses within the cloud provider contracts.

The authors also considered *ISO 14721: Space Data and Information Transfer Systems – Open Archival Information System Reference Model*, which was issued by the ISO in 2012. This standard was reviewed to consider the roles, responsibilities, and expectations of cloud providers and their clients as well as with the aim to consider specific requirements related to the preservation environment. ISO 14721 provides a framework for consideration of cloud providers as well as clarifying the concepts needed by non-archival organizations such as cloud providers to be effective participants in the preservation process.

Additionally, the authors also consulted the Association of Record Managers and Administrators International's *Generally Accepted Recordkeeping Principles* (ARMA International 2013). This source creates an outline of concepts that a recordkeeping program should meet in order to be effective. These principles share many similarities to the ISO standards, in particular *ISO 15489-1*, but offer less description of what might constitute and ideal records management environment. The authors also consulted the European Commission's *Model Requirement for the Management of Electronic Records* (2009). These requirements specially provide guidelines to records in a digital environment and include a consideration of how a system should implement audit trails, access restrictions, destruction, and backup for digital records.

Additionally, the literature review included an examination of efforts to standardize cloud service agreements. For example, in 2014, the European Commission published a guide entitled *Cloud Service Level Agreement Standardization Guidelines* (European Commission 2014). These guidelines identify topics of particular concern to those dealing with information being stored with cloud providers, as well as offering recommendations of service level objectives (*Cloud Service Level Agreeement Standardization Guidelines,* 15-36). A review of this document confirms many similar areas of concern identified by this project.

Another set of guidelines regarding cloud computing can be found in the policy produced by the Public Records Office of Victoria, Australia (2012, 7). This policy identifies two primary risks to organizations that use the cloud: the leaking of sensitive information and potential loss of information. These guidelines require that all agencies of the Victorian government conduct risk assessment before engaging in the cloud. Such risk assessments should focus on the implementation of the cloud on all legislation, standards, and policies and on all agreements between agencies and cloud service providers in order to ensure the security of data, to ensure that data ownership remains with the agency, and to ensure than the agency is established as the controller of the data. (7-8).

6. Comparative Analysis

Following the initial literature review, the authors conducted a comparative analysis of recordkeeping standards, legal requirements, and cloud contracts. In general, the authors noted that since recordkeeping requirements are identified in legislation, regulations policies, and standards, and since these sources will vary from jurisdiction to jurisdiction and organization to organization, both the requirements for maintaining control over records created, received and stored, as well as the systems that facilitate and support them, will vary. Nonetheless, records, which serve both as documentary evidence of legal transactions and also to support the critical operations of an organization clearly have high value and must be managed properly throughout their life cycle. Additionally, records that contain personal or sensitive information must be identified in accordance with applicably privacy and freedom of information legislation when they are received, managed, and disposed.

According to the records management and recordkeeping community, the potential risks associated with the cloud include the following: unauthorized access to information and records; privacy breaches; loss of access to, and management of, records (which impacts record authenticity and integrity), lack of transparency regarding account management, server location, data destruction and data recovery (Ferguson-Boucher and Converty, 2011; Public Records Office Victoria, 2012). From a records management perspective, before entering into a cloud contract, it is therefore imperative that organizations carefully review the contractual agreement not only to determine the degree to which the cloud service might meet the organization's strategy but also to assess the risks.

Moreover, it is important to recognize that, unlike traditional approaches to outsourcing information, where technology services are negotiated directly with the provider, cloud computing introduces IT services on a grand scale. For example, cloud computer uses online platforms for deliver and circulates data on server farms scattered across the globe while relying on generic terms and conditions to govern their contractual relationship with customers. This means that, as a result, customers might be unaware of the location of the service infrastructure, or if subcontractors are involved. In addition, this distributed characteristic to cloud computing might present obstacles to enforce breaches of contract, especially in instances that involved security and privacy (Public Records Office Victoria, 2012).

Additionally, another challenge with respect to understanding cloud contracts exists: the terms and conditions may be contained in a single document hosted on the provider's website, but in other instances it might be contained in a set of documents which outline the terms that govern the relationship between the customer and the cloud service provider (Bradshaw, Millard, and Walden 2011, 192). Examples of such documents include a service level agreement (SLA), terms of service, acceptable use policy, or a privacy policy. If the cloud service is provided for free, the SLA is not included (ibid.). Please note that for this project, all available binding documents were consulted.

It is also important to note that at present, at an international level, no standardized SLA for cloud computing exists. However, at a regional level, as mentioned above, European cloud SLA standardization guidelines exist. In addition, there is an initiative by the SLA underway, entitled *ISO / International Elecrotechnical Committee New Proposal 19086: Information Technology – Distributed Application Platforms and Services – Cloud Computing – Service Level*

Framework and Terminology (ISO 2013). Nonetheless, without an international standard for cloud computing SLAs, those considering agreeing to cloud contracts to support records management and/or digital preservation must individually assess all relevant terms and conditions. In particular, considerations regarding records management and recordkeeping as well as legal duties must be considered.

In some cases, the legal principles stressed above in the section on Cloud Case Law (such as contract law, privacy/security of data, jurisdiction/conflict of laws) are echoed within the recordkeeping standards; however, it's equally true that these recordkeeping standards also focus on additional risks and requirements. To explore this further, the authors considered *ISO 15489-1: Information and Document – Records Management Part 1* (which was issued by the ISO in the Fall of 2011) in detail in order to identify recordkeeping requirements that should be taken into consideration when an organization considers entering into a cloud contract to manage and store their records. While ISO 15489-1 is technology-neutral, the comprehensive nature of the standard ensures it is suitable for addressing both current records and non-current records such as those that have been set aside for future reference. Specifically, it includes sections on records system design and implementation (ISO 2001, section 8) and records management processes and controls (ISO 2001, section 9), which support the creation and maintenance of authentic, reliable, and useable records as well as protecting the integrity of those records for as long as required (ISO 2001, section 6).

ISO 15489-1 also addresses the characteristics of authoritative records; that is, those records that correct reflect what was communicated, decided, or the action that was taken while supporting the needs of the business or used for accountability purposes (ISO 2001, section 7). According to this standard, there are four key characteristics of authoritative records: 1) authenticity (an authentic record is one which is what it purports to be); 2) reliability (a reliable record is one whose contents are accurate and the persons who have been responsible for its creation hold the authority to do so); 3) integrity (a record has integrity if it can be proven that it has remained complete and unaltered after being set aside); and 4) usability (a useable records is one that can be located, retrieved, presented, and interpreted). This standard also outlines that, in addition to content, authoritative records should also contain or be linked to: metadata that documents the structure of a record; the business context, and documents that participate in the same activity. (ISO 2001, section 7).

Thus, a review of both laws and recordkeeping standards reveal several key issues relating to cloud contracts. These specific considerations, discussed below in more detail in section 7, are: 1) data ownerships; 2) availability, retrieval and use; 3) data retention and disposition; 4) data storage and preservation; 5) data security, privacy, and confidentiality; 6) data location and cross-border data flows; and 7) issues related to end of service or contract termination. While recordkeepers in different jurisdictions and within different types of organizations will stress the risks inherent in each of these specific considerations with differing levels of emphasis, the recordkeeping and legal literature reveal that each should be considered in turn for efficacy and risk.

In order for the authors to examine real world contracts within this project, the following cloud services providers (previously identified in InterPARES Trust Project 10) were selected for further analysis in the present study: the Google Cloud Platform (United States), the Pathway Communciation CloudPath (Canada), and the Green Qloud (Iceland). However, other

providers' terms and conditions have been analyzed in the course of the research, and these three specific providers do not constitute isolated examples. In the present study, we do not recommend for or against any particular cloud service provider (or the use of cloud services in general). These were selected for their international representation, online availability of terms and agreements, and limited resources. The authors have attempted to consult the most current terms and provisions documents available on the cloud providers' websites; however, it is recognized that these documents can be updated at any point. Indeed, the cloud provider generally reserves the right to vary contract terms by posting an updated version on their website, often noting that continued use of the service by the customer is considered to demonstrate acceptance of any new terms and conditions (Bradshaw, Millard, and Walden 2011, 202). These specific considerations have been approached with an interdisciplinary mindset, with considerations of both the legal framework and the degree to which terms and conditions meet recordkeeping requirements.

7. Specific Considerations

7.1 Data Ownership

When considering whether or not to work in the cloud, the issue of data ownership – that is, whether the party that stores the data in the cloud retains ownership – must be considered. However, given that information that is accessed and stored in the cloud is in digital form, the issue of ownership is not necessarily the same as ownership over information that is transcribed onto a physical medium (Oxford v. Moss, [1979] 68 Cr. App. R. 183]). Nonetheless, it is reasonable to argue that this issue can be approached similarly to intellectual property rights, confidentiality and privacy rights, as well as contract law (Reed 2010, 1). Indeed, recordkeeping standards approach data ownership with the view that records may be physically stored with one organization even though the responsibility and management control may reside with either the creating organization or another appropriate authority. As a result, records stored in electronic systems require arrangements that distinguish between the ownership of the records and the storage of the records (ISO 15489-1, s.8.3.4). For simplicity, in general, this project operated under the assumption that data ownership does not require a physical medium.

The issue of data ownership in the cloud is further complicated not only because digital information is of an intangible nature but also because of the infrastructure of cloud computing itself. In cloud computing, an individual or organization may entrust their information and records to a cloud provider but also use the provider's platform and applications in the cloud to create further information and records. The provider might create a great deal of information related to these operations (such as data processing, management, marketing, etc.) that it might use for several purposes. Some have argued that information generated by the customer and stored in the cloud does not belong to the service provider but, rather, that the customer retains ownership and the provider is merely authorized to do specific operations with the data to provide the service (Reed 2010, 17).

The ownership of metadata generated by the service provider regarding the customer's information and operations in the cloud can raise more questions. For the customer, metadata can be important to demonstrate that the security of the data has been preserved; however, it appears that metadata can be owned by the service provider who generated it for internal

purposes such as managing the cloud and ensuring the use and quality of the service (Reed 2010, 9). Beyond specifying ownership of metadata, the contract terms and conditions should determining both whether and how the customer has a right to access and use metadata for recordkeeping purposes either during the contractual relationship or at the end of service (see below for further discussion under the heading "End of Service: Contract Termination").

When reviewing the existing contracts for terms that declare ownership or responsibility for customer information and content, it quickly became apparent that there is both a lack of consistency in terminology and in placement that could easily lead to confusion when organizations are trying to evaluate different service providers. For example, Google is the most declarative and places the notice of being a data processor at the outset of their terms of service. Pathway Communications makes a distinction between client data and information generated during the process of providing the cloud service. In this manner, Pathways Communications is imposing ownership of intellectual property via the terms and conditions. GreenQloud, on the other hand, does not seek to assert intellectual property rights over customer content that has been accessed and stored by their service. None of the three providers explicitly mention the right of the customer to assess internal system metadata or the conditions to use metadata under license. This silence could be problematic if the customer needs to assess internal system metadata for recordkeeping purposes, as the provider might then have the right to deny access to this metadata or to ask for additional fees to facilitate access and/or use. These different approaches on the one hand, and the similar approach regarding silence over metadata on the other, are both potentially problematic for the customer.

In more detail, Google Cloud Platform's terms of service includes section 1 on the provision of services, where Google is identified as "merely a data processor" (section 1.3). By stating this, Google appears to suggest that they, the service provider/data processor, only act upon instructions from the customer. The customer, the data controller, determines the purposes and means of processing personal information and customer content. This can be seen as an oversimplified approach to the relationship between Google and its customers, especially given that the service provider often makes important decisions about the process of managing and storing customer information and content. Other sections also address this issue: section 3 on customer obligations assigns responsibility for customer data to the customer (section 3.1). Section 3.6 assigns responsibility to the customer for the management of intellectual property and section 3.2 assigns to the customer the responsibility of protecting the privacy and legal rights of end users. This section also directly references the *Digital Millennium Copyright Act* and stresses that copyright holders must manage their online intellectual property (section 3.6).

In Pathway Communication CloudPath's terms of service, two sections are particularly applicable regarding the issue of data ownership. Section 8, on client data, assigns to the customer the exclusive responsibility for the storage, care, custody, and control of client data (section 8.3). Additionally, towards the end of the terms of service, section 20 addresses ownership of intellectual property. In this section the cloud provider claims ownership of any intellectual property developed by Pathway during the performance of cloud services (section 20.1).

GreenQloud's end-user license agreement addresses data ownership in section 5, its section on the customer's responsibility. In it, it assigns to the customer responsibility for the

technical operation of customer content with the provided service (section 5.1a), managing customer content in a manner that complies with Icelandic laws on privacy and trade secrets (section 5.1b) and addressing any claims related to customer service (section 5.1c).

7.2 Availability, Retrieval and Use

The ability to have information and records immediately available to an organization to fulfill their current and future business needs is one of the driving forces behind organizations considering adopting the cloud. Not only is this a question of efficiency but recordkeeping standards and legal responsibilities also stress its importance. Recordkeeping standards, such as *ARMA International's Generally Accepted Recordkeeping Principles* (2013) emphasize that records must be available for access and retrieval in a timely and efficient manner. Availability and retrieval is also a legal issue given that it is closely linked to statutory or constitutional rights to have access to certain data. More specifically, availability is a fact and access is a right, but the latter cannot be satisfied without the former (Vermeys, Gauthier, and Mizrahi 2014, 86).

In general, data protection laws ensure that individuals have a right to access their own personal information held by an organization, whether public or private. This is the case in Canada and in Europe, and in certain industries in the United States (where privacy is regulated by industry). In Canada, for example, rights are protected under the *Privacy Act*, the *Personal Information protection and Electronic Documents Act* (PIPEDA), and provincial statutes deemed to be essentially similar.

Likewise, many jurisdictions provide a general right of access to information held by public bodies and government organizations. In Canada, such a right is granted by the *Access to Information Act* and by equivalent provincial statues. Similar legislation have been adopted in the United States and Europe that also outline that organizations must be able to provide access to the requested information within a period that may vary, depending on the legislation, from twenty to thirty days. While twenty to thirty days might seem reasonable from a technological point of view, one has to consider the time needed to process from the request, identify all the requested documents, and evaluate whether some information should fall under one of the exemptions from access stated by law. In this respect, the availability of the stored data implies also the availability of the infrastructure, hardware, and software that facilitate the retrieval and readability of the data (Vermeys, Gauthier, and Mizrahi 2014, 88). In instances where information stored in a cloud-based service provided by a third party delays the process and an organization is unable to meet their legally mandated time constraints, that organization remains liable and might expose itself to a complaint that could lead to any number of specific sanctions.

All three of the selected cloud service providers claim service availability of 99.99 percent. While this is close to 100%, it is important to recall that even when a promise of 99.9% uptime is made, this amounts to as much as 9 hours of downtime over the year, and, moreover, it has been noted that "… in reality all major cloud service providers have experienced significant outages over the past five years that would violate the uptime guarantee." (Srinivasan 2014, 86-87). Analysis of the terms and conditions regarding availability, retrieval, and use of the customer contents reveals the use of SLA to present monthly uptime percentages. Uptime percentages are calculated by dividing the total number of minutes in a month minus the

number of minutes of downtime in a month by the total number of minutes in that month. Service credits are supplied in the event of failure to meet performance standards; however, the list of exceptions is long and is on the customer to determine which types of outages, downtime, unavailability, losses, delays, or problems actually constitute a failure and quality for service credit.

More specifically, Google Cloud Platform provides a separate document entitled *Data Processing and Security Terms*, in which they agree to make customer data available to the customer in accordance with the terms of the agreement. There is also an additional clause, in which Google will assist the customer in the deletion and migration of customer data in the event that the customer is unable to do so; however, this service requires a fee. Pathway Communications CloudPath's SLA addresses this issue in section 4 on performance standards. In this section, Pathway agrees to provide target percentages and time period for each of their cloud-based services (that is, cloud server hosts, cloud storage, network, and cloud migration). GreenQloud's SLA addresses availability in their uptime section. Divided into three areas: data centre power, public network, and cloud instance uptime, GreenQloud guarantees 100 percent uptime. In the event of downtime, credit is allotted to the customer's account. The duration of downtime that qualifies for credit is: twenty minutes of data centre downtime, one hour of cloud instance downtime, and any length of public network downtime.

7.3 Data Storage and Preservation

When considering cloud service providers, organizations need to consider how data will be stored and preserved after they are no longer in use by the organization. The manner in which records are preserved impacts both the quality of the records and their capacity to be used for accountability purposes. Additionally, depending on the jurisdiction, evidence law can directly or indirectly impose certain requirements on the processing of the data to ensure a strong evidentiary value of the information that is before that particular court. For example, in civil law jurisdictions (such as Quebec, France, or Belgium), the integrity of the electronic record is a formal condition to recognize it as the legal equivalent of paper record – that is, as "writing" within the hierarchy of the means of evidence. This integrity must be preserved throughout the lifecycle of the record.

Despite its importance, determining what actions are required by a system that stores records for the long term and provides preservation of digital information can be challenging for organizations. This is especially true if cloud providers are not transparent about the infrastructure and processes involved in providing cloud based storage. Indeed, the task of maintaining information and records throughout changing technologies, new data formats, and evolving requirements for use requires navigating and adhering to recordkeeping standards aimed at digital preservation.

In turn, recordkeeping standards aimed at digital preservation state that systems selected by an organization for storing electronic records should ensure that the records held within the system remain accessible, authentic, reliable, and useable throughout any changes made to the system. If the system provider implements changes, then audit trails and process metadata should be made available to the organization (ISO 2001, section 9.6). Planned migration and/or emulation of elements such as hardware, software, and/or operating systems

by the electronic records system provider should not impact the authenticity, reliability, or usability of the records held within the system (section 8.3.5).

Analysis of the selected cloud providers' terms and conditions reveals that the responsibility for backing up data rests with the customer. Google's terms and conditions states that the customer is responsible for backing up the application, project, and customer data (Google 2014). Indeed, the activities related to the storage of data or records for any length of time are generally referred to by cloud providers as backup procedures. Moreover, the actions to preserve or the activity of preservation are absent from all terms and conditions documents.

Pathway Communications CloudPath's terms and conditions agreement includes section 8 on client data. In this section, the provider states that it is the responsibility of the client to ensure the proper storage, care, custody, and control of client data, including regular backups of client data to non-Pathway systems to "ensure against loss or corruption" (section 8.3). Although Pathway Communications admits to creating backups of their systems on a periodic basis, this cloud provider does not guarantee customer access to these "snapshots" (section 8.1). Alternatively, Pathway Communications CloudPath will provide data backup as a fee-based service (section 4.3.1 and section 5.1.4), which includes both integrity checks on backup sessions (section 4.2.4) and support for restoring client data due to a failure of the pathway's backup system (section 4.6.3). However, it is important to recognize that there are a number of limitations listed in relation to backup services and pathway's backup system (section 4.6). Additionally, the cloud provider includes terms that make it clear that scheduled maintenance may impact customer data; therefore, customers are required to back up their data to a non-Pathway location before scheduled maintenance occurs (section 5.1.4).

GreenQloud's end-use licence agreement and terms of service agreement includes section 10 on security and backup. In this section, the customer is deemed responsible for maintaining appropriate backup of customer content. The terms include reference to the customer's responsibility to protect their content by performing "routine archiving". Clearly, organizations concerned about their responsibilities for data storage and preservation need to reflect carefully upon their responsibilities and the specific contract they are considering.

7.4 Data Retention and Disposition

Within organizations, records management divisions and preservation activities rely on data retention and disposition schedules to perform information governance. Such schedules must remain compliant with increasingly complex legal and regulatory environments. Recordkeeping standards suggest that decisions made by the organization on the subject of the retention and disposition of records should be carried out and implemented by the electronic system. More specifically, the electronic system should be capable of producing audit trails to track disposition activities (ISO 2001, section 8.3.7).

Sometimes, in some cases, disposition actions might require the transfer of the records from one electronic system to another. Recordkeeping standards dictate that such transfer should not alter the authenticity, reliability, integrity, or usability of the records. Instead, authorized records destruction must be performed in a manner that preserves the confidentiality of the information. Additionally, the process of record destruction should include all copies throughout the system and related metadata (ISO 2001, section 9.9). Unfortunately,

this can raise difficulties for the metadata generated that is owned by the service provider in relation to the customer's data and operations in the cloud as the provider could refuse to destroy the metadata they have created if still useful for internal management purposes (for example, statistics, service improvement, and so on).

Despite its importance for recordkeepers, an analysis of the selected cloud providers' terms and conditions reveal an absence of terms that address data retention or deletion according to customer-stipulated schedules or recordkeeping requirements. Google Cloud Platform's data process and security terms include section 5 on data correction, blocking, exporting and deletion, in which Google provides the customer with the ability to delete customer data in accordance with the functionality of the selected service. Google agrees that, once the customer deletes their data and it is no longer recoverable by the customer, Google will delete or render permanently inaccessible this customer-deleted data within a maximum period of 180 days.

Such an approach brings up concerns for the customer. In the case of data whose destruction is required by law under a specific schedule, for example, the legal schedule could be overruled by up to six months. The customer would remain liable for such an infringement, as it is his legal duty to use procedures or services that ensure the destruction of the data within the specified timeframe. Additionally, in the context of organizations that are required by law to delete certain types of records, more information about how customer data are rendered permanently inaccessible is required. It is not clear from the terms and conditions, for example, if "inaccessible" data would be available to law enforcement through an e-discovery request. Thus, in this area, the legal and recordkeeping demands do not tend to be adequately addressed in existing terms and contracts.

7.5 Security, Confidentiality, and Privacy

The related issues of security, confidentiality, and privacy are exceptionally important for those wanting to contract in the cloud. As noted above in the section on Terminology, these concepts are closely linked. However, in general, the researchers adopted the view the issue of privacy as relating to the consumer's right to ensure their information remains safe from other parties; the issue of confidentiality as encompassing the concept of one party who has access to information refraining from disclosing it to another; and the issue of security as dealing with the idea of ensuring that the system is secure and safe from outside parties gaining access to data. More specifically, security is a control measure implemented throughout the electronic records system that maintains privacy by preventing unauthorized access, destruction, alteration, or removal of records.

From a recordkeeping perspective, maintaining the privacy of data through access control is of crucial importance. Access to records stored in electronic systems should be managed to ensure the integrity of the records and protect against unauthorized access, use, alteration, or destruction. Moreover, any change in the format of records transferred to the system and/or delivered to the user should be specified. Additionally, the electronic system should be capable of producing audit trails and/or access logs to demonstrate that records are being protected from unauthorized access, use, alteration, or destruction (ISO 2001, section 8.3.6). There should be a process where the system captures and maintains metadata associated

with the access, retrieval, and use of records within the electronic system. An example would include metadata that is embedded or linked to records in addition to metadata generated by the electronic system during processes associated with the management of records (section 8.3.2). In the case of a system malfunction or security breach, the service provider should notify the customer immediately and, furthermore, should demonstrate the integrity of the system by providing access to tracking that reveals the movement and uses of records within the record system (section 8.2.3 and section 9.8.1)

From a legal perspective, such security measures are demanded in general under data protection legislation. Additionally, sectorial regulations at the provincial, national, or international level, such as those related to financial markets (such as the *Sarbanes-Oxley Act* or the *Basel Accords*) must also be considered. As noted above in the discussion on data preservation, the evidentiary value of the record relies upon the actions taken on the data throughout its entire lifecycle to preserve its integrity and authenticity, which includes security measures. More specifically, the duty to ensure the confidentiality and privacy of the data is a very common legal requirement that can be found in hundreds of different statutes and regulations (Vermeys, Gauthier, and Mizrahi 2014, 95 n401). When considering these broad issues, this project mainly focused on security conditions with regard to personal data.

In Canada, for example, according to the principles set out in the Model Code for the Protection of Personal Information, included in Schedule 1 of PIPEDA:

> …an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. (Principle 4.1.3)

Similar provisions can be found in most regulations to ensure the protection of personal data. It is important to note that the fact that the data has been transferred to a third party processor does not also transfer the accountability of the organization. In such a situation, it is interesting to note that the contract is considered to be a key element to ensure security (Office of the Privacy Commissioner of Canada 2009, 9). Therefore, organizations considering the use of cloud-based services should pay special attention to the service provider's contract terms regarding security, privacy, and confidentiality with particular consideration of whether the provider explains how this security is ensured through technical, physical, and organizational measures.

Analysis of the cloud provider's terms and conditions reveals different degrees of addressing these security, privacy, and confidentiality issues. Of the three selected cloud providers, Google's Cloud Platform is the only one that includes a separate document entitled *Data Processing and Security Terms*, which is made available through a hyperlink buried deeply in section 15 of Google's terms of service. Indeed, this document addresses security terms at length, both pertaining to the physical infrastructure required to provide the services as well as personal data under customer content and account information. Typically, the degree to which cloud providers will deliver security measures to customers appears to be reliant on the types of services being offered (such as managed or non-managed) and whether or not the customer chooses to pay additional fees. Moreover, when the terms and conditions addressed controls

on access and use of customer data, they focused on assigning responsibility to the customer for managing access restrictions to their account and their content.

In more detail, Google Cloud's *Data Processing and Security Terms* deals with the provision of security services in section 1. In this section, the provider states that all facilities that store and process the application and customer data must adhere to security standards set forth by the "industry" (section 1.3). Additionally, in section 4 on data security, the cloud provider addresses the implementation of appropriate technical and organizational measures to protect customer data from accidental loss, unlawful deletion, alteration, or unauthorized access (section 4.1). In the event of a "data incident," Google agrees to notify the customer after the incident has been identified and notifies them of measured performed to secure the customer's personal data (section 4.3). The contract further discusses security terms in Appendix 2 - Security Measures – which includes information regarding data centre and network section (section 1), access and site controls (section 2), and data (section 3). These security measures are both physical and virtual, addressing infrastructure security and measures taken to protect unauthorized persons from gaining access to the system and data centres; the multi-tenant environment on Google-owned servers; access controls for administrators and end users; logging capabilities available to the customer (that is, audit trails); as well as the process for handling hardware failure and performance errors.

Regarding the specific issue of access and confidentiality, Google explicitly considers customer data to be the customer's confidential information (section 15.15). Google contracts to not disclose a customer's information, except to the persons who need to access it to fulfill Google's obligation under the agreement and who, in turn, have agreed to keep the information confidential (section 7). In Appendix 2, Google recognizes the multi-tenant environment used by Google-owned servers and states that the customer will be given control over specific data-sharing policies (section 3a). Indeed, Google states that the combination of policies and functionality of selected services will enable to the customer to determine the product-sharing settings that will be applicable to end users for specific purposes. Additionally, Google makes available to the customer certain logging capabilities. The wording of the document seems to imply that customers must shape their access controls to the existing functionality of Google services, though, and this might not accommodate customization based on requirements promulgated by recordkeeping standards.

By comparison, Pathway Communications CloudPath's terms of service include section 4 on scope and limitations of the services. In this section, the cloud provider includes terms for non-managed services. On the specific subject of security, Pathway Communications takes responsibility for the physical security of both the hardware (networking, storage, and servers) and the software that hosts the cloud services (section 4.1.5). Also in section 4, the terms of service for fee-based managed services include support for server monitoring and response (section 4.3.2) and firewalls (section 4.3.5). Additionally, services deemed "specialty services" are excluded, and these include such services as migration services and restoring customer data (section 4.4. and section 4.6.3). The responsibility for monitoring access to customer data is addressed in Pathway Communications CloudPath's terms of service in section 9 on unauthorized access. In this section, Pathway declines responsibility for unauthorized access to customer data 9section 9.2) and states that the customer is responsible for maintaining security of their access credentials and for all activities that occur under their account (section 9.1).

Finally, GreenQloud's end-use license agreement and terms of service include section 10 on other security and backup. In this section, the provider assigns responsibility for maintaining appropriate security protection of customer content to the customer. In two sections, (section 2 on the customer's account and section on acceptable conduct), the document states that access to GreenQloud's services through a customer account is the responsibility of the customer, regardless of whether the activities are undertaken by the account holder or their employees. There is no mention of audit trails or access logs in the terms of service. Thus, the diversity of approach amongst these three sample providers underscores how important it is for the organization that is considering contracting in the cloud to closely review their legal and recordkeeping responsibilities in light of the potential agreement.

7.6 Data Location and Cross-border Data Flow

Given the nature of cloud computing, where the processing and storage services can be provided on-demand by using several of the cloud provider's resources throughout the globe, the issue of data location and cross-border data flow takes on increased importance. Legal concerns regarding cloud computing in this area focus on the issue that the customer's data may be stored or processed in different locations and unknown jurisdictions (Bradshaw, Millard, and Wlden 2011, 206). From a legal perspective, this is mainly viewed as potentially problematic where data is stored outside the customer's jurisdiction because the customer might be subject to different laws and forced to appear in court in different jurisdictions if problem arise. Additionally, there is a concern not only about the customer being subject to data protection laws but also to foreign laws that allow investigation agencies access to any data stored in a provider's jurisdiction. In terms of recordkeeping standards, the discussion focuses not on jurisdiction but on location, with the imperative that electronic records system should be able to tract the location of records as they move throughout the system (ISO 2001, section 9.8.3).

The question of foreign agencies potentially being able to review data when outside the organization's local jurisdiction is often related to the most famous example of the *USA Patriot Act – the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* [H.R. 3162, Pub. L. 107-56, 115 Stat 272], replaced in June 2015 by the *USA Freedom Act – Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act* [H.R. 2048, Pub.L. 114–23]. For the recordkeeping community, numerous concerns are linked to these and similar type of acts, however, the applicability of such laws and their links to data location can be based on erroneous assumptions and, therefore, deserves closer examination.

For example, despite common misunderstanding, in Canada neither the *Federal Privacy Act* nor *PIPEDA* prohibits the use of cloud-based services by public or private bodies, even if such services imply a transfer of data outside the country. In general, Canadian provincial laws also do not restrain cross-border data flows, with the exception of British Columbia, Nova Scotia, and Quebec (Klein 2008, 4 and 14; Vermeys, Gauthier, and Mizrahi 2014, 45, 112) As outlined by Klein:

> Much of the confusion stems from the mistaken belief that Canadian privacy laws require Canadian organization to shield personal information from a foreign

> government's ability to lawfully access that information. Most countries, including Canada, have laws permitting government agencies to access personal information within their jurisdiction for national security and law enforcement purposes. Despite the fact that some of these law potentially permit broader government access than the USA Patriot Act (such as the United Kingdom), transfers that may be subject to the USA Patriot Act are the source of the most confusion and misinformation. (Klein 2008, 4)

Indeed, one common misunderstanding regarding data location and cross-border data flows seems to be that only data stored in the United States is subject to the *Patriot Act/Freedom Act*[1]. In fact, according to this act, the US government enjoys widespread powers to access data not only on servers located within the United States but also stored anywhere with a cloud-service provider than is registered in the United States or that conduct continuous and systematic business in the United States (Van Hoboken, Anrbak, and Van Eijk 2012, 36; Vermeys, Gauthier, and Mizrahi 2014, 49). Moreover, as alluded to above, similar laws in other governments, including Canada, have been adopted. Therefore, it should be recognized that wherever data are stored, whether or not in the cloud, organizations might be subject to orders to disclose information to governmental authorities (Office of the Privacy Commissioner of Canada 2005, n.pag.); Vermeys, Gauthier, and Mizrahi 2014, 49).

Another related issue that can cause concern is the possibility that requests to access information might not be made known to the organizations. With respect to the *Patriot Act/Freedom Act*[2], for example, "…a company subject to a section 215 order cannot reveal that the FBI has sought or obtained information from it." (OIPC Canada 2005). It has been suggested that if an organization chooses to store personal data in the cloud, it should inform individuals "…that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction." (OIPC Canada 2009, 8-9).

Indeed, such proactive measures underscores another aspect to this issue: even if the law does not prohibit the transfer of personal data outside of Canada, it remains incumbent upon organizations to assess the risks of jeopardizing the integrity, security, and confidentiality of personal information entrusted to third-party service providers, wherever they are located (Office of the Privacy Commissioner of Canada 2009, 7 and 9). Additionally, it is equally important for those organizations in locations such as British Columbia or Nova Scotia to determine whether the use of cloud-computing servers based outside the country would be prohibited; however, without entering into too much detail, these specific exceptions do not apply to private bodies and provide for several exceptions. (Klein 2008, 11; Vermeys, Gauthier and Mizrahi 2014, 51).

In Quebec, where restrictions are imposed for the storage of personal data outside the province, public and private bodies must ensure than the personal data will receive an equivalent level of protection under local privacy laws than they would under Quebec privacy laws. Determining whether this onus has been met demands forethought. For example, while it

[1] When the Freedom Act provides similar provisions than the Patriot Act, the present study will mention them both.

[2] This rules remained applicable after the adoption of the Freedom Act, although the so called "section 215" referred to the specific section numbers of the Patriot Act.

has been recognized that equivalent protection is offered by other provincial and federal privacy laws in Canada and by European laws, some doubts might be raised regarding the storage of data in the United States (Vermeys, Gauthier, and Mizrahi 2014, 117; compare Klein 2008, 11). The issue remains mired in confusion and without clear guidance on whether, for example, encryption technologies might offer the possibilities of protecting data before storage in the cloud (Vermeys, Gauthier, Mizrahi 2014, 129 and Canellos 2013). Thus, each organization is left with the responsibility of carefully weighing how this issue might affect them.

Other jurisdictions, such as the European Union, also have addressed this issue. It is well known that the European Union has adopted a restrictive legal framework with regard to the transfer of personal data outside Europe. As a result, privacy laws of the country of destination must offer the same level of protection as EC Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (EC Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, [1995] OJ L281). With respect to Canada, The European Commission has officially considered Canada as providing an adequate level of protection for personal data transferred from the European Union to recipients subject to *PIPEDA* (EC Decision 2002/2 pursuant to Directive 95/46/EC on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act, [2002] OJ L002, 13). With respect to the United States, companies may comply on a voluntary basis to the Safe Harbor international privacy principles, a program settled by the US department of Commerce in consultation with the European Commission and officially recognized as offering an adequate level of protection (EC Decision pursuant to Directive 95/46/EC on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, [2000] OJ L215, 7). However, on October 6, 2015, the European Court of Justice declared the European Commission's as invalid (CJEU, *Schrems vs. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650). According to this judgment, the Safe Harbor principles would provide an inadequate level of protection to the personal data that are transferred to the US, with regard to the EC Directive 95/46. On February 2, 2016, the United Sates and the European Commission agreed on a new framework for transatlantic data flows called the EU-US Privacy Shield (European Commission 2016, n. pag.).

Finally, before leaving a review of the key legal and recordkeeping issues on this subject, another related potential problem should be highlighted. Not only might a decision to use the cloud and thus locate data in other jurisdictions run counter to responsibilities on the part of the organization, but organizations should also be aware of the potential applicability of the issue of conflict of laws. In the event that litigation ensues, if the parties have not specified the law government in contract, they might find themselves obligated to be involved in a court proceeding in another jurisdiction (Goh 2014, 59). If no clause is included, determining forum differs according to the particular jurisdiction; however, most cloud service contracts will include a term that deals with choice of forum for settling disputes and, in general, the contract will reflect that the cloud provider has selected a jurisdiction that is compatible with its own legal system (for example, Pathway Communications' choice of law reflects that it is based in Ontario, Canada). Thus, it is imperative that an organization considers the ramifications on its own business in light of the choice of law provision in the contract.

In considering the three sample contracts in more detail, Google Cloud Platform's terms of service includes section 1 regarding the provision of the services. This section outlines that the cloud provider asserts the right to transfer, process and store "an application and customer data in the United States or any other country in which Google or its agents maintain facilities…" (section 1.3 and section 8.1). Google stresses that it is, and will remain, enrolled in the Safe Harbor program and will adopt a solution that achieves compliance with the terms of EC Directive 95/46 (section 1.5). Additionally, the terms of service expressly state that the customer has the obligation to protect the privacy and legal rights of its end user under all applicable laws, including the communication of a privacy notice, the obtaining of any required consent, and the obligation to inform end-users that the data will be processed by Google (section 3.2). The terms also stipulate that, notwithstanding any non-disclosure agreement that might exist, Google will disclose confidential information to the extent required by the applicable legal process and under certain conditions (section 7).

Furthermore, Google Cloud Platform's data processing and security terms also include section 8 on data transfers. In this section, the provider states that the customer may select where "certain customer data will be stored permanently, at rest" (section 8.2). While these terms appear to be linked to specific services, it is unclear exactly what might constitute data "stored permanently" or what data "at rest" might mean. Additionally, if a customer is not a US city, country or a state government entity, then all claims related to the cloud services will be governed by California law and litigated in the federal or state courts of Santa Clara county in California (section 15.10).

Similar conflict of laws provisions reflect the head offices of the other two contract providers. Pathway Communications CloudPath's terms of service includes section 28 on governing law. This section outlines that the agreement is governed by the laws of the province of Ontario and that all disputes arising from cloud-based services will be addressed in that specific jurisdiction (section 28.1). Likewise, GreenQloud's end-user license agreement and terms of service include section 5 on the customer's responsibilities, in which compliance with Icelandic law is required. In short, it is imperative that organizations ensure not only that the issue of conflict of laws has been addressed in the contract and that the relevant provisions would be deemed acceptable.

7.7 End of Service: Contract Termination

The issue of contract termination also requires consideration from both a legal and recordkeeping point of view. In the event that the relationship with a cloud provider ends, the organization needs assurance that it can gain access to the information and that any data left behind in the third-party system will be deleted by the cloud provider (Bradshaw, Millard, and Walden 2011, 203). Services might be terminated for several reasons, instigated by either party, or simply due to the scheduled end of the contract. Organizations should be aware of contract termination procedures before adopting cloud services. This can be particularly important when dealing with free services (Bradshaw, Millard, and Walden 2011, 196). Typically, contract for paid services address the duration of the service and the necessary steps required to terminate the contract, whereas free services typically do not have a fixed duration and may reserve the right to close inactive accounts.

Recordkeeping standards also address the discontinuation of a records system. In general, the discontinuation of a particular records system constitutes an event that should not preclude ongoing access to those records formerly held by the system. More specifically, system providers should ensure the removal of all records and associated metadata from the system in a manner that does not impact record authenticity, reliability, usability, and integrity. Additionally, in cases of account termination, the records system provider should ensure that all records and associated metadata are transferred to the organization in a manner that does not impact record authenticity, reliability, usability, and integrity (ISO 2001, section 8.5). Archival organizations using third-party services for long-term preservation of their archival records must have a formal contingency plan in the event that the archives or a third provider ceases to operate (ISO 2012, section 3.2.5).

When examining the selected cloud provider terms and conditions, it became apparent that the contracts tended to deal with this issue in two related, but different areas: suspension of services and termination of services. Suspensions typically respond to customer violations of the cloud service and require investigation by the cloud provider to determine restoration of the service and access to customer content, or deletion of the account and customer content. Termination of services is distinct and may be the final result of a suspension, the result of inactivity, or the response to end of contract terms.

In Google Cloud Platform's terms of service, section 8 deals with termination. In it, the contract outlines three types of termination: termination for breach (section 8.2), termination for inactivity (section 8.3), and termination for convenience (section 8.4). In the event of termination, the terms and services outlines that the customer is obliged to delete the software, any application, instance, project, and customer data and moreover, that, upon request, each party will return or destroy confidential information of the other party (section 8.5). Google also reserves the right to terminate services in the event of account inactivity exceeding 180 days (section 8.3).

Pathway Communications Cloud Path's terms of service also deal with what happens after termination. Section 8, on client data, states that the customer will not have access to their data during a suspension or following termination (section 8.1). In addition, it also outlines that, unless written modification is agreed upon, the cloud the cloud provider is free to delete client data fro the system within seven days of termination of the account (section 8.4). Section 14 on service suspension or termination outlines the reasons for which the cloud provider can suspend or terminate services without liability. These include unauthorized access by a third party (section 14.1.4) and overdue payment (section 14.1.6). The cloud provider will give "reasonable advance notice" of suspension of service; however, they are not obligated to refund payment and may prevent customers from accessing their data (section 14.2). Finally, in the case of a breach of contract, notice of account termination will be sent to the customer (section 16).

GreenQloud's end-use license agreement and terms of service deals with suspension or termination in section 6. This section outlines violations of the agreement that will result in suspension or termination of the customer's account. During investigation of the suspected violation, it notes that all accounts will be suspended. The cloud provider will not refund the customer for suspending or terminating accounts that are a result of violations of the agreement, but that it will try to notify the customer before suspension or termination. In the event that there has been account suspension without cause, the cloud provider will provide

fourteen days advance notice. Furthermore, section 7 on effect of termination outlines that the customer is responsible for all fees and charges for in-process tasks that were completed by the cloud provider after the date of termination. Retrieval of customer data following termination is only available to clients that have paid for post-termination use of the provider's services. Thus, to conclude, similar to the other issues discussed above, the terms on this important subject vary and a careful review is called for.

8. Findings and Conclusions

In short, based on the author's analysis of selected cloud providers' terms and agreements, the findings reveal that some boilerplate contracts, without additional fee-based services, are ineffective at meeting the recordkeeping and legal needs of organizations. While some of the agreements do at least address some of the issues that constitute the needs of records management and preservation, these sections clearly are written to favor the service provider rather than the customer. In part, this is likely related to the boilerplate nature of these agreements that can be easily entered into by anyone, but also have the potential to expose the service provider to risk. This reality is further complicated by the fact that some of the companies offer similar terms but differ in their implementation, the method of measurement (as in percentage terms of SLAs) an in how recompense is offered. Another significant concern involves the tendency of the service provider to retain ownership of metadata created in positioning the service, which carries with it potentially significant ramifications for the organizations.

Thus, it is clear that records managers and archivists need to carefully identify and study relevant regulatory and legal fragment in which the organization operates in order to weight the risks associated with the potential cloud-based service. Indeed, areas such as public records requirements, access/freedom of information, protection of privacy requirements, accountability requirements, security requirements, data location requirements or restrictions to cross-border data flows, evidentiary requirements, and intellectual and copyright indicates differing degrees of compliance and should definitely be considered as part of the organization's recordkeeping strategy (Public Records Office Victoria 2013, 6). While it is true in general that private organizations that do not deal with public records are not typically subject to as rigorous a regulatory environment, records managers and archivists still need to base their decisions on the availability of service required, the ability to execute records scheduling and disposition, as well as the assurance of record reliability and authenticity, data privacy, long-term access, and system security. In any event, the provisions related to the end of the contract should be carefully examined to ensure the possibility of a complete restitution of the data in a format that preserves their authenticity. Likewise, any consideration needs to ensure the traceability of any associated metadata as well as include a guarantee that all of the customer's data are permanently and immediately destroyed after any restitution.

Of significant note, it is possible that, within the context of cloud services some needs of records managers may not even be possible given the very nature of the cloud. Despite its potential cost saving nature, the infrastructure necessitates that the infrastructure stores in a manner where information is stored alongside information from other clients making physical destruction much ore challenging. Another example is the reality that the client's data may pass through jurisdictions that will not allow the customer to maintain adequate control or may expose the customer to overly challenging legal and recordkeeping repercussions. At the very

least, the organizations needs to weigh the risks and rewards carefully before signing a contract with a cloud provider.

We hope that the checklist for cloud service contracts will be used by records professionals to verify the extent to which potential contract terms meet records' requirements, and to communicate these requirements to other stakeholders.

References

ARMA International. 2013. “Generally Accepted Recordkeeping Principles.” Retrieved from http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles.

Baset, Salman. 2012. "Cloud SLAs: Present and Future." ACM SIGOPS Operating Systems Review (2): 57-66.

Bradshaw, S., Millard, C., and Ian Walden. 2011. “Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services.” International Journal of Law and Information Technology 19 (3): 187-223.

Canada. 1983. Privacy Act, RSC 1985, c P-21.

Canada. 2000. Personal Information Protection and Electronic Documents Act (PIPEDA), SC 2000, c 5

Canada. 1983. Access to Information Act, RSC 1985, c. A-1

Canellos, D. 2013. “Adopting the Cloud While Adhering to Domestic & Foreign Government Regulations”. http://safegov.org/2013/10/2/adopting-the-cloud-while-adhering-to-domesticforeign-government-regulations

Court of Justice of the European Union. *Schrems vs. Data Protection Commissioner.* C-362/14, ECLI:EU:C:2015:650. http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031

European Commission Decision nr 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, Official Journal of the European Communities nr L 002 , 4th April 2002, 13.

European Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Official Journal of the European Communities nr L 215, 25th August 2000, 7.

European Commission. 2008. "MoReq2 Specification." http://www.moreq2.eu/moreq2

European Commission. 2014. “Cloud Service Level Agreement Standardisation Guidelines.” Brussels, Belgium.

European Commission. 2016. “EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield”. Press release. February 2, 2016. http://europa.eu/rapid/press-release_IP-16-216_en.htm

European 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 of the European Communities nr L 281, 23th November 1995, 31.

Ferguson-Boucher, K., and Nicole Convery. 2011. “Storing Information in the Cloud – A Research Project.” Journal of the Society of Archivists 32 (2): 221-239.

Goh, E. 2014. “Clear skies or cloudy forecast? Legal challenges in the management and acquisition of audiovisual materials in the cloud”. Records Management Journal 24(1): 56-73.

Google. “Google Cloud Platform: Data Processing and Security Terms,” https://developers.google.com/cloud/terms/data-processing-terms.

Google. 2014. “Google Cloud Platform: Terms of Service,” https://developers.google.com/cloud/terms/.
GreenQloud. 2013. “EULA and Terms of Service,” https://www.greenqloud.com/eula/.
GreenQloud. “Privacy Policy,” https://www.greenqloud.com/privacy-policy/.
GreenQloud. 2014. “Service Level Agreement,” https://www.greenqloud.com/sla/.
InterPARES 2 Project. 2015. “InterPARES 2 Dictionary,” http://interpares.org/ip2/display_file.cfm?doc=ip2_dictionary.pdf.
ISO. 2001. “ISO 15489-1,” http://www.wgarm.net/ccarm/docs-repository/doc/doc402817.PDF.
ISO. 2012. “ISO 14721,” http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284.
ISO. 2013. “ISO/IEC NP 19086,” http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902.
JISC Legal Information. 2011. User Guide: Cloud Computing Contracts, SLAs and Terms & Conditions of Use. Legal Guidance for ICT Use in Education, Research and External Engagement. http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2135/JISC-Legal-Cloud-Computing-and-the-Law-Toolkit-31-August-2011.aspx
Klein, Kris. 2008. “Applying Canadian Privacy Law to Transborder Flows of Personal Information from Canada to the United States: A Clarification”. Industry Canada. https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00508.html
Office of the Privacy Commissioner of Canada. 2005. Bank's notification to customers triggers PATRIOT Act concerns. PIPEDA Case Summary #2005-313. https://www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp
Office of the Privacy Commissioner of Canada. 2009. “Processing Personal
Data Across Borders. Guidelines”. https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf
Pathway Communications. 2014. “CloudPath: Acceptable Use Policy,” http://cloudpath.pathcom.com/services/legal/aup/.
Pathway Communications. 2014. “CloudPath: Privacy Policy,” http://cloudpath.pathcom.com/services/legal/privacy-policy/.
Pathway Communications. 2014. “CloudPath: Service Level Agreement,” http://cloudpath.pathcom.com/services/legal/sla/.
Pathway Communications. 2014. “CloudPath: Terms of Service,” http://cloudpath.pathcom.com/services/legal/terms/.
Public Record Office Victoria. 2012.“Cloud Computing: Implications for Records Management, V.1.0.” State of Victoria, Australia. http://prov.vic.gov.au/wp-content/uploads/2012/04/Issues-Paper-Cloud-Computing.pdf
Public Record Office Victoria. 2013. “Cloud Computing Decision Making, V. 1.0.” State of Victoria, Australia. http://www.unimelb.edu.au/unisec/privacy/pdf/PROVCloud_Computing_Guideline_1.pdf
Reed, Chris. 2010. “Information ‘Ownership’ in the Cloud.” Legal Studies Research Paper No. 45. Queen Mary University of London, School of Law. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.
United States. 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act). H.R. 3162, Pub. L. 107-56. http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.
United States. 2015. Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping Dragnet-collection and Online Monitoring Act (USA Freedom Act). H.R. 2048, Pub. L. 114–23. https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf

Van Hoboken, Joris, Axel Anrbak, and Nico Van Eijk. 2012. “Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act”. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534

Vermeys, Nicolas, Gauthier , Julie, and Sarit Mizrahi. 2014. “Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le Gouvernement du Québec.” Working paper. Laboratoire de cyberjustice. Université de Montréal. http://www.cyberjustice.ca/wordpress/wp-content/uploads/2014/08/%C3%89tude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-Qu%C3%A9bec.pdf

Checklist for Cloud Service Contracts

Final version

This work is made available through a **Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License**
http://creativecommons.org/licenses/by-nc-sa/4.0/

Title:	Checklist for Cloud Service Contracts
Status:	**FINAL**
Version:	1.0
Date submitted:	February 2016
Last reviewed:	May 2015 – February 2016
Author:	InterPARES Trust Project
Writer(s):	Jessica Bushey, Marie Demoulin, Elissa How and Robert McLelland
Research domain:	North American Team – Legal – NA14

The following Checklist for Cloud Service Contracts is the final product of research being conducted by the InterPARES Trust Project on current cloud service contracts from a records management, archival, and legal perspective. InterPARES Trust (2013-2018) is a multi-national, interdisciplinary research project exploring issues concerning trust in digital records and data in the online environment. For more information see: https://interpares.org.

The target audience for this document is records managers, archivists, chief information officers, and others who are assessing cloud services for their organization. The aim of this document is to provide a tool to:

- gain an understanding of boilerplate cloud service contracts;
- verify if potential cloud service contracts meet their needs;
- clarify recordkeeping and archival needs to legal and IT departments;
- communicate recordkeeping and archival needs to cloud service providers.

This checklist is a tool for consideration only and does not constitute legal advice. We do not recommend for or against any particular cloud service provider (or the use of cloud services in general). Individuals and organizations should consult legal counsel if they want legal advice on a particular contract.

Checklist for Cloud Service Contracts Intended Audience: Records Managers and Archivists[3]				
Question	**Y**	**N**	**?[4]**	**Notes**
1. Agreement				
▪ Is the effective start date of the agreement clearly stated?				
▪ Is there an explanation of circumstances in which the services could be suspended?				
▪ Is there an explanation of circumstances in which the services could be terminated? (See also Section 8)				
▪ Is there an explanation of notification, or an option to subscribe to a notification service, in the event of changes made to the terms governing the service?[5]				
2. Data Ownership and Use				
▪ Do you retain ownership of the data that you store, transmit, and/or create with the cloud service?				
▪ Does the Provider reserve the right to use your data for the purposes of operating and improving the services?				
▪ Does the Provider reserve the right to use your data for the purposes of advertising?				
▪ Does the Provider reserve the right to use, or				

[3] The Checklist is primarily a tool for assisting organizations in assessing typical issues in boilerplate cloud computing legal agreements, in which the organization has to deal with legal agreements proposed by the Provider. The secondary application of the Checklist is to provide an overview of recordkeeping issues that are relevant to cloud computing services and should be addressed in the terms of the agreement. It is strongly recommended that any organization proceeding with the procurement of cloud computing services, in which a custom contract is being drafted, should carefully review and obtain all necessary legal advice on the specific terms of use.

[4] The "?" column indicates a situation in which the contract is unclear, or the question is not applicable to your situation.

[5] Some cloud service agreements, especially services in the public cloud, include clauses allowing the provider to change the terms of the agreement at any time at their sole discretion. Therefore, if possible, organizations should consider deleting this right, or making this right subject to the organization's agreement to any change, or ensuring the Provider is obligated to notify the organization well in advance of any changes.

make your data available as anonymized open data (through standard APIs)?				
▪ Does the Provider's compliance with copyright laws and other applicable intellectual property rights restrict the type of content you can store with the cloud service?				
▪ Do the Provider's terms apply to metadata?[6]				
▪ Do you gain ownership of metadata generated by the cloud service system during procedures of upload, management, download, and migration?				
▪ Do you have the right to access these metadata during the contractual relationship? (See also Section 8)				
3. Availability, Retrieval, and Use				
▪ Are precise indicators provided regarding the availability of the service?				
▪ Does the degree of availability of the data meet your business needs?				
▪ Does the degree of availability of the data allow you to comply with freedom of information (FOI) laws?[7]				
▪ Does the degree of availability of the data allow you to comply with the right of persons to access their own personal data?[8]				
▪ Does the degree of availability of the data allow you to comply with the right of authorities to legally access your data for investigation, control, or judicial purposes?				
▪ Are the procedures, time, and cost for restoring your data following a service outage clearly stated?				

[6] Metadata ensure that records can be discovered, retrieved and used. They are critical for ensuring the authenticity of the record over time. They can be generated by your organization or by the Provider. It is therefore important to specifically address metadata in the contract in order to clarify issues such as ownership, access, retention and disposition during the service and after its termination.

[7] In general, freedom of information laws allow access by the general public to information held by national governments.

[8] In some countries there is a Privacy Act to protect the privacy of individuals with respect to personal information about themselves held by public *and/or* private bodies, and provide individuals with a right of access to that information.

4. Data Storage and Preservation				
4.1. Data Storage				
▪ Does the Provider create backups of your organization's data?				
▪ If your organization manages external records (e.g., customer data), does the Provider create backups of your customer's data?				
▪ Do the Provider's terms apply to any backup created?[9]				
▪ In the event of accidental data deletion, does the Provider bear responsibility for data recovery?				
4.2. Data Preservation				
▪ Are there procedures outlined to indicate that your data will be managed over time in a manner that preserves their usability, reliability, authenticity, and integrity?[10]				
▪ Are there procedures to ensure file integrity during transfer of your data into and out of the system (e.g., checksums)?				
▪ Is there an explanation provided about how the service will evolve over time (i.e., migration and/or emulation activities)?				
▪ Does the system provide access to audit trails concerning activities related to evolution of the service?				
▪ Will you be notified by the Provider of changes made to your data due to evolution of the service?				
▪ Can you request notification of impending changes to the system related to evolution of the service that could impact your data?				

[9] Notably in terms of ownership, access, security, retention and disposition during the service and after its termination.
[10] Usability, reliability, authenticity and integrity might be defined in the contract (e.g., in a Definition section or in a Glossary). It is recommended to verify if your organization and the Provider have a common understanding of these concepts.

5. Data Retention and Disposition				
▪ Are you clearly informed about the procedure and conditions for the destruction of your data?[11]				
▪ Will your data (and all their copies, including backups) be destroyed in compliance with your data retention and disposition schedules?				
▪ If so, will they be immediately and permanently destroyed in a manner that prevents their reconstruction, according to a secure destruction policy ensuring confidentiality of the data until their complete deletion?				
▪ Is there information available about the nature and content of the associated metadata generated by the cloud service system?				
▪ Will the Provider destroy associated metadata upon disposition of your data?				
▪ Will the Provider deliver and/or give access to audit trails of the destruction activity?				
▪ Will the Provider supply an attestation, report, or statement of deletion (if required by your internal or legal destruction policies)?				
6. Security, Confidentiality, and Privacy				
6.1. Security				
▪ Does the system prevent unauthorized access, use, alteration, or destruction of your data?				
▪ Is your data secure during procedures of transfer into and out of the system?				
▪ Does the system provide and give you access to audit trails, metadata, and/or access logs to demonstrate security measures?				
▪ Will you be notified in the case of a security breach or system malfunction?				
▪ Does the Provider use the services of a subcontractor?				
▪ Does the Provider offer information about the identity of the subcontractor and its tasks?				

[11] For example, is this operation automatic or does it require your authorization? Does the Provider offer a "freeze" function to temporarily suspend the disposition of a group of data and/or metadata against the instructions of the disposition schedule? Will you be made aware of, or are you able to specify, the method of disposition?

▪ Are subcontractors held to the same level of legal obligations as the Provider of the cloud service?				
▪ Is a disaster recovery plan available or does the contract consider what happens in the event of a disaster?				
▪ Does the Provider offer any information regarding past performance with disaster recovery procedures?				
6.2. Confidentiality				
▪ Does the Provider have a confidentiality policy in regards to its employees, partners, and subcontractors?				
6.3. Privacy				
▪ Does the Provider's terms include privacy, confidentiality, or security policies for sensitive, confidential, personal or other special kinds of data?				
▪ Is it clearly stated what information (including personal information[12]) is collected about your organization, why it is collected and how it will be used by the Provider?				
▪ Does the Provider share this information with other companies, organizations, or individuals without your consent?				
▪ Does the Provider state the legal reasons for which they would share this information with other companies, organizations, or individuals?[13]				
▪ If the Provider shares this information with their affiliates for processing reasons, is this done in compliance with an existing privacy, confidentiality, or security policy?				
6.4. Accreditation and Auditing				
▪ Is the Provider accredited with a third party certification program?				
▪ Is the Provider audited on a systematic, regular, and independent basis by a third-party in order to demonstrate compliance with security,				

[12] Including personal information about your employees, customers, partners, providers, collaborators, etc.
[13] For example, do you know that your information may be accessible to law enforcement and national security authorities of different jurisdictions?

confidentiality, and privacy policies?				
▪ Is such a certification or audit process documented?				
▪ Do you have access to information such as the certifying or audit body and the expiration date of the certification?				
7. Data Location and Cross-border Data Flows				
7.1. Data Location				
▪ Do you know where your data and their copies are located while stored in the cloud service?				
▪ Does it comply with the location requirements that might be imposed on your organization's data by law, especially by applicable privacy law?				
▪ Do you have the option to specify the location, in which your data and their copies will be stored?				
▪ Do you know where metadata are stored and whether they are stored in the same location as your data?				
7.2. Cross-border Data Flows				
▪ Will you be notified if the data location is moved outside your jurisdiction?				
▪ Is the issue of your stored data being subject to disclosure orders by national or foreign security authorities addressed?				
▪ Does the Provider clearly state the legal jurisdiction in which the agreement will be enforced and potential disputes will be resolved?				
8. End of Service – Contract Termination[14]				
▪ In the event that the Provider terminates the service, will you be notified?				
▪ Is there an established procedure for contacting the Provider if you wish to terminate the contract?				
▪ If the contract is terminated, will your data be transferred to you or to another Provider of your choice in a usable and interoperable format?				

[14] The end of the service is a key moment that needs to be addressed in the contract in order to specify the procedure to follow, the obligations and responsibilities of both parties and the destination of all data before the contractual relationship is terminated.

▪ Is the procedure, cost, and time period for returning/transferring your data at the end of the contract clearly stated?				
▪ At the end of the contract, do you have the right to access the metadata generated by the cloud service system?				
▪ At the end of the contract and after complete acknowledgement of restitution of your data, will your data and associated metadata be immediately and permanently destroyed, in a manner that prevents their reconstruction?				
▪ Is there an option for confirmation of deletion of records and metadata by the organization prior to termination of services with the Provider?				
▪ Is there an option for the client to terminate the service agreement without penalty in the event that the Provider of the cloud service changes?				

Appendix B – Annotated Bibliography

InterPARES Trust Project

Title:	Trust in Cloud Service Contracts
Status:	**Annotated Bibliography**
Version:	1.0
Date submitted:	May 5, 2015
Last reviewed:	May 5, 2015
Author:	InterPARES Trust Project
Writer(s):	Jessica Bushey, Elissa How, Robert McLelland
Research domain:	North American Team – Legal – NA14

The following Annotated Bibliography is divided into four areas: Cloud Computing Services - Legal, which includes articles and studies that explore the legal aspects of cloud-computing and specifically cloud-service contracts; Related Case Law and Decisions, which includes cases and decisions relevant to cloud provider contracts; Cloud Computing Services – Recordkeeping, which includes articles and studies that explore the roles and relationships between Cloud service Providers and Organizations that perform recordkeeping activities and provide guidance for records managers and archivists considering adoption of third-party cloud-based services; and Recordkeeping Standards and Related Articles, which presents a number of key standards that inform recordkeeping practices and should be considered when assessing cloud-service contracts for recordkeeping within a public body, an institution or a private organization.

Cloud Computing Services - Legal

Billings, John T. "European Protectionism in Cloud Computing: Addressing Concerns over the PATRIOT Act." *CommLaw Conspectus,* 21 (2013): 211-231. http: //scholarship.law.edu/commlaw/vol21/iss1/8/.

> This scholarly article, written by a JD candidate in the United States, provides a detailed examination of the provisions of the PATRIOT Act in order to consider whether European countries should be avoiding US cloud service providers for privacy reasons. The author concludes that while there is solid cause to be concerned about the privacy of data in the cloud given the PATRIOT Act, avoiding US cloud service providers does not necessitate that the PATRIOT Act will not apply. Moreover, the author argues that access might be granted through Mutual Legal Assistance Treaties. Additionally, the author contends that within the European Union there exist laws that allow for access to consumer information.

Bradshaw, Simon, Christopher Millard and Ian Walden. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." *International Journal of Law and Information Technology* 19, no.3 (2011): 187-223. DOI: 10.1093/ijlit/ear005

> This paper is a research product of the Cloud Legal Project at the Centre for Commercial Law Studies at the University of London, UK. The paper presents the findings of a survey and analysis of the standard Terms and Conditions (T&C) offered by a range of cloud computing providers in the context of the European legal system. The report contrasts traditional IT outsourcing with cloud computing services noting that customers of cloud services may require varying degrees of resources over time (i.e., on-demand procurement) and may not be aware of the location of where the service infrastructure is located. Lastly, standard T&C are entered into via an online process. As part of the T&C analysis, twenty terms common to all documents were identified and analyzed: contract, applicable law, jurisdiction, arbitration, acceptable use, variation of contract terms, data

integrity, data preservation, data disclosure, data location/transfer, monitoring by provider, rights over service/content, proprietary rights and duties, warranty, direct liability, indirect liability, limit of liability, indemnification, service credits and service availability.

Bradshaw, Simon, Christopher Millard and Ian Walden. "Standard Contracts for Cloud Services." In *Cloud Computing Law*, edited by Christopher Millard, 39-72. Oxford: Oxford Scholarship Online, 2014. DOI: 10.1093/acprof:oso/9780199671670.003.0003

This chapter in *Cloud Computing Law* is a follow-up by the same authors to the 2011 examination of cloud Terms of Service contracts outlined above ("Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services"). In this subsequent work, those previously studied contracts were revisited (if they still existed) alongside a handful of additional contracts. The similarities and differences were examined and reported upon.

Faulkenberry, Regina M. "Reviewing and Negotiating Cloud Computing Vendor Contracts." *Journal of Health & Life Sciences Law* 6, no.3 (2013): 119-154. http://www.healthlawyers.org/JHLSL.

This academic article provides a comprehensive summary of contractual clauses that those in the American health industry should keep in mind when negotiating with cloud computing vendors. The article uses concrete examples and provides a guide for current trends. The article underscores the lack of directly applicable laws and the complex nature of negotiating such contracts. In particular, it offers a brief examination of the few potentially applicable cases in the States as well as discussing in detail the various clauses and considerations that the author deems as crucial for any health organization entering in to such a contract.

Ha-Radeye, Omar. "New Tort of Intrusion Upon Seclusion and Electronic Health Records." *Lorman Educational Services Live Seminar*. Toronto, December 4, 2014. http://ssrn.com/abstract=2533987.

This article, written by an Ontario lawyer, was offered in conjunction with a seminar in December 2014 on Medical Records Law in Ontario. It is well supported, with many footnotes, though there is no bibliography and does

not appear to have been published in a peer-reviewed journal. Nonetheless, it provides not only a summary of *Jones v. Tsige* but also offers a very recent reflection on potential ramifications for the new tort of intrusion upon seclusion and how it might impact privacy law in Canada. The overall tenor of the paper is that the new tort might have major impact for Canadian health companies that deal with health data.

Klein, Kris. "Applying Canadian Privacy Law to Transborder Flows of Personal Information from Canada to the United States: A Clarification". Industry Canada. 2008. Last modified May 11, 2009. https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00508.html

This 2008 article has been archived on Industry Canada's website. The author, Kris Klein, is a lawyer practicing in Ontario. The paper examines the application of Canadian privacy law in situations where personal information of Canadians is transferred outside Canadian borders "for processing purposes." The paper clarifies what is permitted and what is not permitted when transferring personal information of Canadians out of Canada and into the United States of America. In the conclusion the author states that transborder data flows of personal information is permitted as long as it is reasonable, the process for doing so is transparent, notice is provided and there are safeguards in place.

Maddex, Stephen J. and Ruba El-Sayegh. "Personal Jurisdiction in Canada: can U.S. Defendants Be Subject to Suit With No Meaningful Contacts?" *NYSBA Inside* 29, no.1 (2011): 10-12.
http://www.mcmillan.ca/Files/132154_Personal%20Jurisdiction%20.pdf

The authors, lawyers at McMillan LLP in Ottawa, discuss how, in the United States, the question of personal jurisdiction is predicated on a "minimal contacts" test and a series of cases which protect the defendant's right to due process. On the other hand, in Canada, the law is not as well settled, but recent case law suggests that the threshold in Canada is "substantially lower" than in the United States. To this end, it examines the 2011 Ontario CA case in *Van Breda v. Village Resorts Limited*, 2010 ONCA 84 which examined the question in detail from a Canadian perspective with a "real and substantial connection" test.

Oppenheim, Charles. "Cloud Law and Contract Negotiation." *El professional de la información* 21: no. 5 (2012): 453-457. DOI: http://dx.doi.org/10.3145/epi.2012.sep.02.

> The author, previously a Professor of Information Science at Loughborough University in London, examines contracts for cloud computing in this brief article that includes a bibliography but no citations. It offers some concerns for those who would like to contract with cloud service provides and also includes a checklist of over twenty questions that should be asked of a cloud service supplier before signing up. The author advocates adding into the contract a clause of adherence to international security standards.

Pasquale, Frank and Tara Adams Ragone. "Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing." *Stanford Technology Law Review* 17 (2014): 595-652. https://journals.law.stanford.edu/stanford-technology-law-review/online/protecting-health-privacy-era-big-data-processing-and-cloud-computing

> This article, written by two American law professors, is an in-depth examination of changes that should be considered by those in the US health industry who are contracting for cloud services. It focuses on specific provisions of HIPAA for must of the paper and therefore is largely industry specific; however, it offers some general recommendations and underscores the complexity of cloud contracts as well as the potential liability of contracting organizations for business associates under HIPAA.

Reed, Chris. "Information 'Ownership' in the Cloud." Legal Studies Research Paper No. 45 (2010). Queen Mary University of London, School of Law. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.

> This paper was written by a professor of Electronic Commerce Law at Queen Mary University of London, School of Law. According to the abstract, it was funded by Microsoft. It examines the complex issue of ownership of information in the context of cloud computing and concludes that three areas of law are particularly germane (copyright, confidentiality, and contract). The article is written in a manner that allows the reader to review different types of information and scenarios and determine which reflects their user-generated content and what the legal implications would be in regards to ownership in the Cloud. In the conclusion the author states that the cloud computing relationship is a patchwork of ownership rights,

shared between the provider and their client (i.e., user). The author also addresses ownership of information generated by the provider. It also concludes that, while much remains unclear, appropriately drafted contracts can provide clear guidance and standard terms of service contracts with cloud computing providers also likely will address some of these key legal areas.

Reed, Chris and Alan Cunningham. "Ownership of Information in Clouds." In *Cloud Computing Law*, edited by Christopher Millard, 142-168. Oxford: Oxford Scholarship Online, 2014. DOI: 10.1093/acprof:oso/9780199671670.003.0006.

This chapter in *Cloud Computing Law* offers a summary of ownership issues with respect to information in clouds. It discusses the legal ramifications (and considerable uncertainties) of data ownership in the cloud, with a particular focus on laws relating in general to the protection of confidential information or trade secrets as well as regarding copyright and the need in a number of instances to clearly contract to protect rights. It also outlines the complicating factor of competing jurisdictional issues.

Ryan, James. "The Uncertain Future: Privacy and Security in Cloud Computing." *Santa Clara Law Review* 54, no. 2 (2014): 497-525. http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2778&context=lawreview

The author, a law student at Santa Clara University School of Law, offers an introduction to the challenges of interpreting the law in the United States regarding privacy and security in cloud computing. Essentially, he argues that these laws are piecemeal, antiquated, and meant for other industries. This leads to unpredictability and instability in interpreting the legal framework. This, in turn, is detrimental to both service providers and consumers alike. He advises embracing a framework such as exists in the European Union – an approach that he views as representing an attempt to regulate cloud computing directly.

Srinivasan, S. "Cloud Computing Security." In *Cloud Computing Basics* by S. Srinivasan, 81-100. New York: SpringerBriefs in Electrical and Computer Engineering, 2014. DOI 10.1007/978-1-4614-7699-3_5.

This chapter, written by a business professor from an American perspective (published in February 2014), is meant to be an introduction to security

issues in cloud computing in general. It reads like an introductory textbook and includes review questions for students at the end of each chapter. As such, despite being from a series for electrical and computer engineering, it is accessible for those not widely versed in the technological aspects of cloud security. The author offers current introductory facts, basic explanations, and advice regarding what to consider when deciding to enter into a contract.

Stiven, Janet A. "The Cloud: Emerging Issues in Business and Intellectual Property Law: Preparing and Advising Your Clients on Cloud Usage." *DePaul Business & Commercial Law Journal* 12 (2014): 421-436.

This article appears to be a transcript of a lecture given by Janet A. Stiven (Vice President and General Counsel at The Moody Bible Institute of Chicago) at a Symposium at the DePaul College of Law in March 2014. She advises lawyers to consider a number of key considerations when choosing a cloud service provider, most specifically to conduct due diligence. She also advises considering applicable standards.

Van Hoboken, Joris, Axel Anrbak, and Nico Van Eijk. "Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act". *Social Science Research Network,* November 27, 2012. DOI: http://dx.doi.org/10.2139/ssrn.2181534.

This report is written by legal scholars based in the United States and the Netherlands; thus providing a discussion of cloud-based services in the context of two different legal frameworks. The authors point out that government agencies in both the United States and the Netherlands have legal powers to obtain access to cloud data. Furthermore, both countries can work together to extend their powers of jurisdiction further into the cloud. The report discusses information confidentiality, security, and privacy in the context of educational and research institutions contracting cloud-computing services for the purposes of accessing, managing and storing information and records relating to their institutional activities. In the conclusion, the authors suggest that control over information is at risk in the cloud computing environment.

Vermeys, Nicolas, Julie Gauthier and Sarit Mizrahi. "Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le Gouvernement du Québec." Working paper. Laboratoire de cyberjustice, Université de Montréal. 2014.

http://www.cyberjustice.ca/wordpress/wp-content/uploads/2014/08/%C3%89tude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-Qu%C3%A9bec.pdf

This paper presents an academic study on the legal implications of the use of cloud computing services for the Government of Québec. In the first part, the document presents different types of cloud services and gives examples of governmental uses in Canada, the United States, the United Kingdom and Australia. In the second part, it examines different legal issues in light of the legal framework of Quebec and Canada, such as access and availability, integrity, privacy, security and confidentiality.

Wang, Faye Fangei. "Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction." *European Business Law Review* 24, no.5 (2013): 589-616. http://bura.brunel.ac.uk/bitstream/2438/8330/5/FullText.pdf

This article is aimed at a legal audience and focuses on interpreting major legal cases on jurisdiction in the EU and US and hypothesizing how these cases might be construed when dealing with cloud computing. It offers several suggestions about how negotiation might lead to sophisticated jurisdictional clauses and underscores that well thought through clauses in contracts are the best potential method to allow the contractor to dictate jurisdiction.

Zimmeck, Sebastian, "The Information Privacy Law of Web Applications and Cloud Computing." *Santa Clara High Technology Journal* 29, no. 3, (2012): 451-487. http://digitalcommons.law.scu.edu/chtlj/vol29/iss3/1

In this examination of an American approach to privacy and cloud computing, the author examines relevant considerations for privacy law issues in cloud computing. The author suggests that if a valid contract is entered into then the body of US federal constitutional and state law may become secondary. The first half of the article considers what constitutes a valid contract with particular focus on clickwrap and browsewrap contracts. The article states that it was supported by research grants both from the University of California, Berkeley and by Google.

Relevant Case Law and Decisions

Club Resorts Ltd. v. Van Breda, [2012] S.C.R. 572.

> This Supreme Court of Canada decision examines the issue of jurisdiction. It deals with two Canadians injured in separate accidents while in Cuba. Both cases brought the issue of jurisdiction to the fore at the trial level, where both trial judges decided in favour of the plaintiffs and granted jurisdiction. The cases were heard together at the Court of Appeal – where the appeal was dismissed, and again heard then dismissed in a 7-0 ruling at the Supreme Court of Canada. The case gives guidelines on establishing jurisdiction with the common law with the "real and substantial test".

*Jones v. Tsi*ge, [2012] ONCA 32, 108 O.R. (3d) 241

> This Ontario Court of Appeal case establishes a proper course of action for a newly recognized tort called the tort of intrusion upon seclusion. Although this case and new tort is relatively recent and it's ramifications are still to be determined, it potentially opens a new avenue of liability to any company dealing with organizations that deal with data, in particular sensitive records such as banking, health records, information relating to sexual practices and orientation, employment, or diary or private correspondence. At a minimum, Canadian record managers should be aware of this tort.

Mazzonna c. DaimlerChrysler Financial Services Canada Inc. / Services financiers DaimlerChrysler inc., 2012 QCCS 958.

> This Quebec Superior Court decision involves the loss of personal information when a data tape went missing while being shipped between DaimlerChrysler's offices in the United States to Quebec. While the judge agreed that the defendants did not meet their obligations towards the petitioner to store, keep, and transfer information safely, the petitioner could not demonstrate that she suffered compensable damages and, as a result, her class action application was dismissed.

Cloud Computing Services - Recordkeeping

Barnes, Frederick. "Putting a Lock on Cloud-Based Information." *ARMA International – Information Management*. 2010. http://content.arma.org/IMM/JulyAug10/IMM0710puttingalockoncloud-basedinformation.aspx.

> This article is a non-academic work that seeks to provide records managers with an introduction to cloud storage technologies. The article briefly summarizes what the technology is and its various iterations. It then briefly outlines seven concepts that records managers should consider before using the cloud for information storage: privilege user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability. The article goes on to describe five layers of protection that a client and service provider should implement to protect data in the cloud. This article is useful because it very concisely describes professional concerns about cloud storage.

Baset, Salman. "Cloud SLAs: Present and Future." *ACM SIGOPS Operating Systems Review*. 2012. http://www.cs.columbia.edu/~salman/publications/baset-sla-osr.pdf

> This article is a study funded by IBM comparing the terms found within the Service Level Agreements of five cloud service providers. The study found that SLAs tend to differ in their use of jargon, how they measured timeframes, and how they measured accessibility. The study also found that the SLAs are primarily worded for the protection of the service providers, and that most SLA's place the responsibility for reporting outages on the cloud service clients.

Blair, Barclay T. "Governance for Protecting Information in the Cloud." ARMA International's Hot Topic: Making the Jump to the Cloud? How to Manage Information Governance Challenges. 2010. http://www.arma.org/docs/hot-topic/makingthejump.pdf?sfvrsn=0.

> This article is a non-academic work that seeks to describe the challenges of the cloud from a records management perspective. The article briefly describes how the cloud works as "hardware as a service" and as "software as a service". It then describes six concerns that exist with the use of cloud storage for information within organizations: availability of information, e-

discovery, retention, privacy, use of multiple providers, and the portability of information. It concludes by offering ways in which records manager can become involved early in the process of implementing these services so as to ensure that records are protected.

Cloud Security Alliance, "Top Threats to Cloud Computing V1.0." *Cloudsecurityalliance.org*. March 2010. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

This White Paper seeks to describe the various threats to information that can exist for an organization that utilizes cloud technology. It describes seven threats: Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service & Traffic Hijacking.

Council of Australasian Archives and Records Authorities. "Advice on managing the recordkeeping risks associated with cloud computing." *ADRI*. (2010). http://prov.vic.gov.au/wp-content/uploads/2011/05/ADRI_statement_re_cloud_computing_v1-0_July_2010.pdf

This paper seeks to provide information and advice to archives of the Australasian region on the nature of cloud computing and the implications its use has for records stored within.

Cunningham, Patrick. "IT's Responsibility for Security, Compliance in the Cloud." Hot Topic: Making the Jump to Cloud. : 6-10. 2010. http://www.arma.org/docs/hot-topic/makingthejump.pdf

This article is part of a series of three articles published by ARMA International for organizations planning on moving into the cloud. This article presents an IT perspective, outlining some of the risks that organizations will face as they place their records into cloud storage and IT's responsibilities to mitigating said risks.

Ferguson- Boucher, Kirsten. "Cloud Computing: A Records and Information Management Perspective." *Security & Privacy, IEEE*. 9. no. 6 (2011): 63 - 66. http://cadair.aber.ac.uk/dspace/bitstream/handle/2160/11640/ieee_managing_information_in_the_cloud.pdf?sequence=1

> This article seeks to outline the concerns and considerations that records manager should be aware of as their organizations move information into the cloud. The paper begins by briefly explaining cloud computer and the different models that are available. It then lists some benefits of moving to the cloud as well as RIM concerns: compliance e-discovery; integrity and confidentiality; service availability and reliability; service portability and interoperability; information retrieval and destruction; and loss of governance, integration, and management. The paper then discusses how the cloud affects an organization's responsibility for their records and states that policies and procedures will need to be amended to incorporate the changes brought by the cloud, but does not state specifically what the changes should be. In regards to litigation it then states that contracts should ensure that records are available and reliable in the case of litigation. The paper wraps up by stating it is up to each organization to determine what information it is willing to store in the cloud, which the paper has established as an uncertain environment.

Hickling Arthurs Low, Science & Technology Policy Research and Analysis Resource team. "Primer on Policy Implications of Cloud Computing." Government of Canada. 2012. http://open.canada.ca/data/en/dataset/514c7974-b894-5ff1-bee6-0617e183d1ca.

> This paper was developed to advise agencies of the Canadian federal government on moving information and records into the cloud. It provides an overview of cloud services, describes the problems and risks that are associated with records stored in the cloud, and provides examples of how information has been placed into the cloud by public bodies, primarily geographic information.

Ju, Jiehui, Jiyi Wu, Jianqing Fu, and Zhijie Lin. "A Survey on Cloud Storage." *Journal of Computers* 6. no. 8 (2011): 1764-1771. http://ojs.academypublisher.com/index.php/jcp/article/view/jcp060817641771/5924

> This article is an attempt to explain cloud storage from a RIM and technical standpoint. The paper identifies what is calls "determinators" that must be

in place to make cloud storage valuable: elasticity, automatic, scalability, data security, performance, reliability, ease of management, ease of data access, energy efficiency, and latency. It then identifies the various cloud services that are commonly offered by service providers and describes the benefits and detractions for each of these services, particularly in relation to RIM needs.

Kundra, Vivek. *Federal Cloud Computing Strategy*. U.S. Chief Information Officer. February 8, 2011. https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.

This document was issued following the announcement of the US government's "Cloud First" policy. It defines the cloud and gives guidelines for federal agencies to adopt the cloud, including the use of a decision framework.

Lifka, David, Ian Foster, Susan Mehringer, et al. *XSEDE Cloud Survey Report*. Cornell Centre for Advanced Computing. September 2013. http://www.cac.cornell.edu/technologies/XSEDECloudSurveyReport.pdf

This paper is the result of a survey conducted from September 2012 to April 2013 by the XSEDE Cloud Integration Investigation Team to understand how cloud computing is used across a wide variety of scientific fields and the humanities, arts, and social sciences. Data was collected from 80 cloud users from around the globe. The paper gives good primary information about cloud usage in post-secondary research and education.

National Archives and Records Administration. Government of the United States of America. "Frequently Asked Questions about Managing Federal Records In Cloud Computing Environments." 2010. http://www.archives.gov/records-mgmt/faqs/cloud.html

This short document is a list of frequently asked questions provided as a guideline for US Federal Agencies aiming to adopt cloud-based solutions. It offers a basic introduction including definitions and potential strengths and weaknesses to managing records in the cloud.

Ponemon Institute LLC, "Flying Blind in the Cloud The State of Information Governance." Last modified 2010. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-ponemon_institute_flying_blind_in_the_cloud_WP.en-us.pdf.

This article is a study sponsored by Symantec and conducted by the Ponemon Institute on the use of cloud services within organizations around the United States of America and how organizations deal with the increased risk of the technology to their information. The study found that cloud storage and software-as-a-service are the most popular and that few organizations are vetting the cloud the way they vet other services, decisions are being made by individual employees without the input of IT, and few organizations are taking proactive steps to protect themselves from risks associated with the cloud, amongst other findings.

Rennie, Stuart. "Legal Implications of Working in the Cloud." Hot Topic: Making the Jump to Cloud. : 11-16. 2010. http://www.arma.org/docs/hot-topic/makingthejump.pdf

This article is part of a series of three articles published by ARMA International for organizations planning on moving into the cloud. This article presents a legal perspective, outlining some of the risks that organizations will face as they place their records into cloud storage.

Ruttrell, Yasin. "NARA moved email to the cloud at 'lightning speed." *GCN*, December 17, 2013. http://gcn.com/articles/2013/12/17/nara-cloud-email.aspx.

This brief two-page online article recounts some of the challenges faced by the US National Archives and Records Administration when they moved email to the cloud. It discusses issues such as security and cost savings.

State & Local Government Cloud Commission. "The Cloud Imperative: Better Collaboration, Better Service, Better Cost." *TechAmerica Foundation (SLG-CCA*) 2012: 1-48. http://www.techamerica.org/Docs/fileManager.cfm?f=taf_slg_cc.pdf

This paper outlines cloud implementation practices and procedures for local and state governments. Aside from definitions of the cloud, the paper gives recommendations for cloud implementations and defines key contract terms for state and local government officials.

Stuart, Katharine, and David Bromage. "Emerald Article: Current state of play: records management and the cloud." *Records Management Journal* 20, no. 2 (2010): 217 - 225. DOI: http://dx.doi.org/10.1108/09565691011064340.

> This paper outlines the implications of the cloud to records management. The primary audience of this article is records managers and archivists and the article discusses topics on a level that takes this into account, incorporating topics such as diplomatics into its treatment of the issue. The article discusses issues of the lack of fixity, control, destruction, security (including challenges on over taxed virtual machines that cannot generate enough random numbers for encryption), challenges in preserving the records in their context, records stored in the cloud lacking traditional records management treatment, and an inability to access the records. The article concludes by stating that organizations must develop policies and procedures for the cloud prior to moving information into it at all as well as outlining questions that must be asked of service providers:
>
> - "Asking where the records will be stored and processed and trying to find jurisdictions that are complementary to their own;
> - Seeking contractual agreements to obey privacy requirements;
> - Seeking assurance that at the termination of the contract, no trace of the records will be retained by the provider; and
> - Understanding how the provider backs up stored information and can restore your information in case of emergency."

The National Archives, UK. *The National Archives Guidance on Cloud Storage and Digital Preservation.* First Edition. 2014. http://www.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf.

> This report provides guidance on the cloud and its potential role in archival storage. Authored by Charles Beagrie, Andrew Charlesworth and Paul Miller, the report targets public archives, but is useful for a range of organizational contexts. The guide includes separate case studies, further resources for advice, and an appendix on legal issues. The legal requirements are presented as a table in the appendix and are very useful for archivists and information professionals trying to navigate and understand cloud-service provider's contracts.

Recordkeeping Standards and Related Articles

ARMA International. "Generally Accepted Recordkeeping Principles." 2014. http://www.arma.org/docs/sharepoint-roadshow/the-principles_executive-summaries_final.doc.

> The principles of information governance, referred to as Generally Accepted Recordkeeping Principles (the Principles), are promoted by ARMA as high-level characteristics of an effective and sustainable information governance program, which aid in the management of records and information assets in compliance with applicable legal and regulatory frameworks. The Principles are purposefully general in nature and do not address specific organizational structures or regulatory environments in an effort to remain flexible and applicable to wide range of private and public sector organizations. It addresses the Principles of: Accountability (i.e., roles and responsibilities); Integrity (i.e., information generated and managed is authentic and reliable); Protection (i.e., records and information of a private or confidential nature are protected); Compliance (i.e., program is compliant with applicable laws and policies); Availability (i.e., timely and accurate retrieval of records and information); Retention (i.e., records and information are retained according to legal, regulatory, fiscal, and historical requirements); Disposition (i.e., secure disposition of records and information according to applicable laws and policies); and Transparency (i.e., business processes and activities are document and available to personnel and applicable parties).

ARMA International. "Generally Accepted Recordkeeping Principles: Information Governance Maturity Model." 2013. http://www.arma.org/docs/bookstore/theprinciplesmaturitymodel.pdf.

> This factsheet on GARP provides an introduction and overview of the Principles, but goes further and addresses the Maturity Model to define the characteristics of information governance programs. Five levels of maturity in an organization are discussed, from "sub-standard" (i.e., information governance and recordkeeping concerns are not addressed at all) to "transformational" (i.e., integration of information governance has been achieved throughout corporate infrastructure and business processes and both legal compliance and program requirements have been met). For our purposes, cloud-computing infrastructure and services are considered part of the information governance of an organization; therefore, assessment of

cloud-based services in accordance with GARP and the Maturity Model (levels) is a useful exercise.

Crockett, Margaret and Janet Foster. "Using ISO 15489 as an Audit Tool." *The Information Management Journal* (July/August 2004): 46-53. http://www.arma.org/bookstore/files/CrockettFoster.pdf

This article is written by archivists and records managers and is intended to assist information professionals in using ISO 15489 as a tool for assessing an organization's existing records management program. A case study of a small European pharmaceutical company using ISO 15489 to assess compliance of its records management program is presented in the article. For our purposes, the mapping of collected data to ISO 15489 in the form of a checklist provided a useful example to guide our own development of a checklist for assessing cloud computing contracts.

Document Lifecycle Management Forum. "Model Requirements for Records Systems." Vol. 1, Version 1.1. 2010. http://moreq2010.eu/pdf/moreq2010_vol1_v1_1_en.pdf.

This specification outlines the essential elements that an electronic records management system (ERMS) should have to ensure that records are properly managed, can be accessed at all times, are retained for as long as they are needed and are properly disposed of following expiration of the retention period. The functional requirements presented in Moreq 2010 address user groups, classification, metadata, disposition and retention, access and export. In contrast with the previous version, Moreq 2010 introduces the concept of a distributed repository.

European Commission. "Model Requirements for the Management of Electronic Records: Update and Extension." 2008. http://ec.europa.eu/archival-policy/moreq/doc/moreq2_spec.pdf.

The specification addresses the functional requirements for the management of electronic records by an Electronic Records Management System (ERMS). The specification is generic and does not consider platform-specific or sector-specific issues. Additionally, the requirements can be implemented in the context of private and/or public sector organizations. In our case, the specification was reviewed as the basis for

assessing cloud-computing service providers as outsourced records management services.

Goh, Elaine. "Clear skies or cloudy forecast? Legal challenges in the management and acquisition of audiovisual materials in the cloud". *Records Management Journal* 24, no.1 (2014): 56-73. DOI: http://dx.doi.org.ezproxy.library.ubc.ca/10.1108/RMJ-01-2014-0001.

The author, an archival scholar, discusses the effectiveness of records-related and archival legislation in addressing the control, ownership and custody of data and records accessed, managed and stored in the Cloud. Her focus is on analysis of archival legislation in Commonwealth countries, specifically court cases relating to audio-visual materials in Canada, Australia and Singapore. In her discussion, she introduces the model of maritime law as a potential framework for determining ownership and stewardship of data circulating across borders and legal jurisdictions in cloud-based services. Goh concludes that current legislative provisions on copyright and archival acquisition and preservation may be inadequate as they were developed prior to the use of the networked environment for record creation, management and storage.

International Organization for Standardization. ISO 15489-1. Information and documentation – records management – Part 1: General and Part 2: Guidelines. 2001.

The specification is designed to meet the recordkeeping needs of public and private organizations. ISO 15489 is technology-neutral and includes sections on records system design and implementation and records management processes and controls, which support the creation and maintenance of authentic, reliable and useable records, and protect the integrity of those records for as long as required. The high-level functional requirements are addressed in Part 1: General and an overview of the processes and factors to be considered for implementation are addressed in Part 2: Guidelines.

International Organization for Standardization. ISO 14721:2012 – Space data and information transfer systems – Open archival information system (OAIS) – Reference model. 2012.

ISO 14721:2012 permits a designated community to preserve records and information that is created and kept in a digital environment. The Open Archival Information System includes the organization and people that are responsible for preserving information and making it accessible to a designated community. The aim of this standard is to provide a framework for understanding archival concepts needed for long-term preservation and ongoing access to information. The target audience is organizations, including archives, which are responsible for managing information and making it available for the long term. The authors used this standard to approach the analysis of the cloud service agreements from an archival perspective, in which information may need to be preserved indefinitely.

National Institute of Standards and Technology. Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, Joint Task Force Transformation Initiative, U.S. Department of Commerce, April 2013. DOI: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

This document, from the US Department of Commerce, is summarized in the abstract as providing "…a catalogue of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors." (page iii). In regards to cloud-based services, the authors state that organizations are becoming increasingly reliant on information systems that are provided by external providers for business functions. These external information systems include cloud-based services. In the section on external service providers, encryption is suggested as a method of protecting organizational information held in the cloud. In the footnotes, the FedRAMP Ready System is mentioned, which is a third-party audit program in which a Cloud-computing system must be assessed, monitored and approved to receive FedRAMP compliance.