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.