InterPARES Trust

Study Name:		Retention & Disposition in a Cloud Environment
Team & Study Number:		#06
Research domain:		Control
Document Title:		Literature Review for Retention & Disposition in a Cloud Environment
Status:		Final
Version:		1
Date submitted:		July 20, 2014
Last reviewed:		July 20, 2014
Author:		InterPARES Trust
Writer(s):		Patricia C. Franks, Researcher (SJSU) Karla Harriott, Graduate Research Assistant (SJSU) Anousheh Shabani, Graduate Research Assistant (UBC)

Document Control

Version history			
Version	Date	By	Version notes
1	July 20, 2014	P. Franks, K. Harriott, A. Shabani	

Literature Review
Prepared for
Retention and Disposition in a Cloud Environment (#06)
An InterPARES Trust project
July 20, 2014

Introduction

The purpose of this literature review is to provide a synthesis of existing literature related to records retention and disposition in a cloud environment and to compare that with the way in which retention and disposition is conducted in a closed system, such as an Electronic Records Management System (ERMS), behind the walls of an organization. Two research questions that the literature review seeks to address are:

- How does the use of cloud services affect our ability to retain and dispose of records in accordance with the law and other applicable guidelines?

- What can be done to mitigate any risks arising from the gaps between our ability to apply retention and disposition actions to manage records residing within the enterprise and those residing in the cloud?

Searches were conducted within the SJSU Martin Luther King online library and Google Scholar using keyword combinations of the word "cloud" + (protection, retention, preservation, records management, information governance, destruction, deletion, data integrity, compliance, standards). Articles that were peer reviewed and published no earlier than 2009 were key criteria.

Google searches were conducted to locate white/technical papers sponsored by software vendors that correlate information governance in the cloud environment with sound records management principles for retention and disposition. Additionally, online resources provided by representative cloud providers were examined to ascertain their documented retention and disposition features, if any.

Key records management standards and guidelines were examined (primarily ISO 15489, DoD 5015.2 and MoReq2010) as they inform software retention and disposition functional requirements. Laws, in particular privacy laws, that impact records management principles of retention and disposition within Canada and the United States were examined.

A key theme throughout the body of the literature is that the cloud is an ecosystem consisting of cloud providers (data centers), customers (individuals and organizations), digital device manufacturers and bandwidth providers (cable and telecommunication companies), content companies (software vendors), and legal and regulatory regimes

(policy and law makers).[1] Consequently retention and disposition control results in complex management challenges and decisions—there is no one-size fits all scenario.

This research was conducted with the InterPARES Trust project objectives of records control within the cloud environment in mind.

Major Areas Central to Retention and Disposition in a Cloud Environment

The following sections explore five themes identified within the body of the articles, laws, standards and white papers reviewed for this project: risk analysis and risk management, legal regimes and standards, information governance, emerging approaches to conducting retention and disposition, and mixed trust response. The topics are not arranged in any specific order of importance.

Risk analysis and risk management:

The literature indicates that an organization needs to understand all the risk factors that pertain to their information assets to meet their business mission and needs. Once risks are identified—such as sensitive and confidential information, compliance issues, privacy, security, access controls, ownership, and vendor environment—they must be mitigated and actively managed for the cloud system. Articles that address risk analysis and management abound, and many of the authors provide checklists, toolkits, and other resources to help the user identify and mitigate risks before trusting their digital assets to a cloud environment.

Dutta et al. cite legal and technology complexities as comprising the top ten critical risks of cloud computing for organizations.[2] Grounds et al. cite eDiscovery risks due to the mismanagement of retention policies and the inability to implement legal holds successfully in the cloud environment.[3] They provide a checklist of questions to be used to vet cloud providers.

Ferguson-Boucher et al. explore legal, technical and operational concerns of storing corporate assets in the cloud. They also provide a toolkit for the assessment of risk and information governance elements that must be considered before making the decision to move to the cloud.[4]

---

[1] J. Rayport and A. Hayward, "Envisioning the Cloud: The Next Computing Paradigm," Marketspace, 2009, http://www.hp.com/hpinfo/analystrelations/Marketspace_090320_Envisioning-the-Cloud.pdf
[2] A. Dutta, G. Peng, and A. Choudhary, "Risks in enterprise cloud computing: The perspective of it experts," *The Journal of Computer Information Systems* 53, no. 4 (2013): 39-48.
[3] Alison Grounds and Ben Cheesbro, "Cloud Control: eDiscovery and Litigation Concerns with Cloud Computing," *The Computer and Internet Lawyer* 30, no. 9 (2013): 23-31.
[4] K. Ferguson-Boucher and N. Convery, "Storing Information in the Cloud – A Research Project," *Journal Of The Society Of Archivists* 32, no.2 (2011): 221-239. doi:10.1080/00379816.2011.619693

According to Salido et al., the risks an organization faces when moving to the cloud must be analyzed and then harmonized to meet the challenges presented by the cloud environment. A Risk/Gap analysis matrix is offered that builds on the Information Lifecycle Model elements, technology domains, and the regulatory environment of an organization. [5]

Different types of cloud systems may pose different risks. Géczy et al. discuss the benefits and risks of managing digital assets in a hybrid cloud system.[6]

Gold poses a practical discussion of risks not only to security but also in the language used for insurance policies and contract agreements for control of data with cloud providers.[7]

Changes to legal regimes and standards for the cloud:

Case law is still nascent for cloud computing issues, and the literature shows that once data is in the hands of the cloud provider it can be disclosed due to police or government investigations (USA Patriot Act) or, in some parts of the world, obtained through bribery. When managing information in the cloud environment, retention and disposition issues no longer entail local storage but global and cross-border issues with multiple jurisdictional laws, especially pertaining to privacy. One way that cloud providers are responding to this dilemma is to locate physical data centers in various geographic regions. Other legal issues pertain to Terms of Service (ToS) and Contract Agreement language that leaves the customers vulnerable to privacy and ownership issues that varies with each cloud provider. Additionally, there are interoperability issues with cloud providers or their sub-contractors, and when customers wish to withdraw their data in a usable form at time of departure or migration, they have no recourse. Several authors hint to the need for changes to legal structures and standards for the cloud.

According to *Bashir et al.*, contracts and ToS do not protect customer data from misuse of data or disclosure of data to third parties by cloud service providers.[8]

---

[5] J. Salido and D. Cavit, *Trustworthy computing: A guide to data governance for privacy, confidentiality, and compliance* (Redmond, WA: Microsoft, 2010), http://www.microsoft.com/en-us/twc/privacy/data-governance.aspx

[6] P. Géczy, N. Izumi, and K. Hasida, "Hybrid cloud management: Foundations and strategies," *Review of Business & Finance Studies* 4, no.1 (2013): 37-50, http://search.proquest.com.libaccess.sjlibrary.org/docview/1445008520?accountid=10361

[7] J. Gold, "Protection in the cloud: Risk management and insurance for cloud computing," *Journal of Internet Law* 15, no. 12 (2012): 1-28.

[8] M. Bashir, J. Kesan, C. Hayes, and R. Zielinski, "Privacy in the cloud: Going beyond the contractarian paradigm," Annual Computer Security Applications Conference, Orlando, FL, December 2011, https://acsac.org/2011/workshops/gtip/Bashir.pdf

Ion et al. cite that the expectation of privacy is not typically written into cloud provider service agreements. Cloud users potentially do not even know if and when their data is being accessed by other users.[9]

In *Kesan et. al*, the authors propose baseline regulations to identify minimum requirements the cloud provider must implement in order to protect certain sensitive information, including fraud detection and prevention, data encryption, and security breach notifications. Furthermore, the authors propose a legal regime that defines secondary use of personal identifiable information by cloud providers and other third parties. They emphasize two rights users have in controlling their data: the right to serve a notice-and-takedown order, and the right to have data converted to an acceptable format to ensure data mobility at time of departure.[10]

The National Institute of Standards and Technology (NIST) Cloud Computing Program presents a long-term goal to foster interoperability, portability, and security in the cloud.[11]

Ovadia discusses the Open Cloud Manifesto and the creation of a standard for the flow of data between the storage environment and where the data is utilized.[12]

Pitt cites Software-Defined Network (SDN) technology (a part of the Open Networking Foundation) as a solution to deal with trans-border data flow facilitated with open-flow protocols.[13]

Information governance of cloud content:

Information governance ensures that retention and disposition meets records management principles and the ISO 15489 standard for a records management program. A prominent theme identified throughout the literature is the involvement of the cloud provider in educating organizations about information governance and the possible emergence of a new cloud service model IGaaS (Information Governance as a Service).

To maintain effective information governance in the cloud, Blair suggests including "preservation of metadata" and "enforcement of retention periods" as two key

---

[9] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun, "Home is safer than the cloud!: Privacy concerns for consumer cloud storage," Symposium on Usable Privacy and Security, Pittsburgh, PA, July 2011, https://www.vs.inf.ethz.ch/publ/papers/iion-cloud-2011.pdf

[10] J. Kesan, C. Hayes, and M. Bashir, "Information privacy and data control in cloud computing: Consumers, privacy preferences, and market efficiency," *Washington & Lee Law Review* 70, no. 1 (2013): 341-472.

[11] NIST Cloud Computing Program, *US Government Cloud Computing Technology Roadmap Volumes I, II, and III,* (Gaithersburg, MD: NIST, 2014), http://www.nist.gov/itl/cloud/index.cfm

[12] S. Ovadia, "Navigating the challenges of the cloud," *Behavioral & Social Sciences Librarian* 29, no. 3 (2010): 233-236.

[13] D. Pitt, "Trust in the cloud: The role of SDN," *Network Security* 2013, no. 6 (2013): 5-6, http://dx.doi.org/10.1016/S1353-4858(13)70039-4

components of service agreements and contracts.[14] *Hoke* advises records managers to apply ARMA International's Generally Accepted Recordkeeping Principles (GARP) to internal policies and procedures before making the move to the cloud. The author also explains how each of the principles in GARP applies to cloud computing.[15]

McLean cites that cloud computing is seeing a shift of IT departments from support roles to strategic partners with corporate governance responsibilities.[16]

A qualitative research conducted by *Ross et. al* indicates that information governance is the nexus of strategy and technology. The authors encourage the creation of processes and new employee and executive training in order to support and encourage information governance strategies.[17]

In a white paper, *Autonomy* examines how the power of cloud computing facilitates information governance in the cloud for all formats of information—structured, semi-structured, and unstructured for archiving, eDiscovery, compliance, records management, and data protection.[18]

A Gimmal white paper examines the Gimmal model of applying and implementing the Generally Accepted Recordkeeping Principles of retention and disposition in an automated manner for electronic records.[19]

According to Pierre Van Beneden, CEO of RSD, "An information governance strategy and platform has become a must-have for today's global companies." RSD Glass is an Information Governance as a Service (ISaaG) solution that helps mitigate risks and lower the costs associated with storing information in the cloud.[20]

---

[14] B. Blair, "Governance for protecting information in the cloud," *Information Management* 44, no. 5 (2010): 1, http://search.proquest.com.libaccess.sjlibrary.org/docview/1033603283?accountid=10043

[15] E. J. G. Hoke, "Challenges to governing remote information," *Baseline,* http://www.baselinemag.com/c/a/IT-Management/Challenges-to-Governing-Remote-Information-709978/

[16] V. McLean, "Head in the Cloud?" *New Zealand Management* 59, no. 77 (2012): 44-47.

[17] P. Ross, and M. Blumenstein, "Cloud computing: The nexus of strategy and technology," *Journal of Business Strategy* 34, no. 4 (2013): 39-47, doi: 10.1108/JBS-10-2012-0061.

[18] Autonomy, "Best practices for cloud-based information governance," Autonomy, 2013, http://www.informationweek.com/whitepaper/Infrastructure/Network-Systems-Management/making-the-move-to-the-cloud-best-practices-adv-wp1347981072?articleID=191705703

[19] Gimmal, "Emerging practices for electronic record disposition," Gimmal, 2012, http://www.gimmal.com/Resources/Pages/Gimmal-Whitepaper-Emerging-Practices-for-Electronic-Record-Disposition.aspx

[20] Reuters, "RSD Information Governance Momentum Continues Into 2014," http://uk.reuters.com/article/2014/03/31/ma-rsd-idUKnBw315282a+100+BSW20140331

Tero promotes the concept of cloud providers expanding their role in the cloud with deployment of information governance solutions and education of customers.[21]

In order to meet the needs of financial and highly regulated industries, *Viewpointe* promotes OnPointe, a cloud information governance solution for private clouds employed by the business.[22]

Emergence of new approaches to handle R & D in the cloud:

New approaches to apply retention policies and enforce deletion are emerging; however, it appears that such solutions are heavily Information Technology, computer, and software oriented. RIM professionals and archivists are not often key stakeholders in the process.

A number of cloud providers are being investigated by the R & D team. ArchiveSocial, Microsoft Azure, Microsoft, Cloud Kite, Egnyte, Gimmal, GoGrid, Google Apps, HP Records Manager, IBM Cloud, Office 355, Rackspace, Smarsh, and CenturyLink were among the products/services examined. Product documentation reflects that the data centers of most vendors are designed to be compliant with physical and network security, for example Statement of Accounting Standard number 70 (SAS70), SSAE, ISO 27001, US-EU Safe Harbor, HIPPA or GLBA Compliant. Only Autonomy Records Manager, which can be deployed as either a private or hybrid solution, mentioned adherence to ISO 15485, DoD 5015.02, and VERS.[23] .

Askhoj et al. suggest remodeling the OAIS with a Platform-as-a-Service (PaaS) Layer, Software-as-a-Service (SaaS) Layer, Preservation Layer, and Interaction Layer in order to preserve records in the cloud.[24]

According to *Li et al.*, "scalable management of data retention policies" can be achieved by encrypting data stored in the cloud and securing the key at a secure data center.[25]

---

[21] V. Tero, "Information Governance in the Cloud," IDC, 2010, http://www.emc.com/collateral/analyst-reports/1010-idc-paper.pdf

[22] Viewpointe, "Information governance and cloud computing: Approaches for regulated industries," Viewpointe, 2013, http://www.ciosummits.com/Information_Governance_and_Cloud_Computing_Approaches_for_Regulated_Industries.pdf

[23] Autonomy, "Autonomy Records Manager," Autonomy, 2012a, http://www.hp.com/hpinfo/newsroom/press_kits/2012/FallBizPrinting/Autonomy_Records_Manager_Datasheet.pdf

[24] J. Askhoj, Shigeo Sugimoto, and Mitsuharu Nagamori, "Preserving records in the cloud," *Emerald* 21, no. 3 (2011): 175-187, http://dx.doi.org/10.1108/09565691111186858

[25] J. Li, Sharad Singhal, Ram Swaminathan, and Alan H. Karp, "Managing Data Retention Policies at Scale," *IEEE Transactions on Network and Service Management* 9, no. 4 (2012): 393-406.

Muthulakshmi et al. propose a framework called Cloud Information Accountability (CIA) that will allow users to audit their data as well as copies made without their knowledge in the cloud environment.[26]

Nicolaou et al.[27] *and Rabinovici-Cohen* et al.[28] recommend that all data, both in transit and at rest, should be encrypted.

In their article, *Rabinovici-Cohen* et al. introduce SIRF (self-contained information retention format) as a means of authenticating data stored in a cloud system.[29]

Srinivasan proposes a cloud security infrastructure for customers to control their virtual machine, monitor the access logs of cloud providers, and protect their data by holding the encryption key on-site.[30]

Tang et al. propose FADE (file assured deletion) encryption technology to implement and execute retention and disposition policies. This technology will also facilitate complete data withdrawal when switching vendors.[31]

Cohasset Associates presents EMC Data Domain Retention Lock, which is compliant with the MoReq2010 criteria of discreetness, completeness, immutability, and destructibility.[32]

Hitachi Data Systems explains that Hitachi Content Platform (HCP) ensures retention and disposition in the cloud environment, enables litigation hold or release, and provides assurances for data segregation in a multi-tenancy environment.[33]

---

[26] V. Muthulakshmi, A. Ahamed Yaseen, D. Santhoshkumar, and M. Vivek, "Enabling Data Security for Collective Records in the Cloud," *International Journal of Recent Technology and Engineering* 2, no.1 (2013): 163-167.

[27] C. Nicolaou, A. Nicolau, and G. Nicolau, "Auditing in the cloud: Challenges and opportunities," *The CPA Journal* 82, no. 1 (2012): 66-70.

[28] S. Rabinovici-Cohen, M. Baker, R. Cummings, S. Fineberg, and J. Marberg, "Towards SIRF: Self-contained information retention format," The 4th Annual International Conference on Systems and Storage, Haifa, Israel, June 2011, doi: 10.1145/1987816.1987836.

[29] Ibid.

[30] S. Srinivasan, "Is security realistic in cloud computing?" *Journal of International Technology and Information Management* 22, no. 4 (2013): 47-66.

[31] Y. Tang, P. P. Lee, J. C. Lui, and R. Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion," *Security and Privacy in Communication Networks* 50 (2010): 380-397.

[32] Cohasset Associates, *MoReq2010: EMC Data Domain Retention Lock Compliance Edition* (Chicago, IL: Cohasset Associates, 2013), http://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf

[33] Hitachi Data Systems, *Introduction to Object Storage and Hitachi Content Platform* (Santa Clara, CA: Hitachi Data Systems, 2013), http://www.hds.com/assets/pdf/hitachi-white-paper-introduction-to-object-storage-and-hcp.pdf

Mixed trust response to retaining information in the cloud

There seems to be a tension between the economic benefits of cloud services and potential legal and security risks. Clearly cloud computing is a trend, but is it still too early to measure its success?

Ajero enumerates the benefits enjoyed by end users who store their music files in the clouds.[34]

Greengard notes executives are embracing the cloud as having a positive impact on the bottomline, thus overshadowing any negative issues.[35]

A White paper by *Nasuni* depicts a case study with a law firm that is using Nasuni cloud storage because of assurances of reliable security and data retention of client files that are highly sensitive and confidential. The experience has been deemed a resounding success for the law firm.[36]

On the other hand, Katzan indicates managers are skeptical about moving to the cloud due to concern over obsolescence and security issues.[37]

Pearson discusses two key barriers of cloud adoption: lack of consumer trust and complexity of compliance, which can be remedied with accountability (and the use of detective and preventive controls).[38]

Venters cites that C-level executives express concern regarding the security of their off-site data, especially multi-tenancy security and compliance issues.[39]

According to Wang and Wang, large enterprises, especially multinational enterprises, typically have complex technologies, systems, cultures, and politics, which provide barriers to adoption. The authors suggest development of decision-modeling tools to aid in the selection process and service agreement negotiations.[40]

---

[34] M. Ajero, "Random access: Can we trust our studio materials to the "cloud"?" *American Music Teacher* 62, no. 1 (2012): 50-51, http://www.thefreelibrary.com/Random+access%3A+can+we+trust+our+studio+materials+to+the+%22cloud%22%3F-a0299885768

[35] S. Greengard, "Building Clouds That Are Flexible and Secure," *Baseline*, http://www.baselinemag.com/cloud-computing/building-clouds-that-are-flexible-and-secure/

[36] Nasuni, "*Law Firm Uses the Cloud to Uphold Stringent Security and Data Retention Requirements,*" Nasuni, 2011, http://www.nasuni.com/case-studies/gesmer-updegrove-llp

[37] H. Katzan, "On the Privacy of Cloud Computing," *International Journal of Management and Information Systems* 14, no. 2 (2010): 1-12.

[38] Siani Pearson, "Towards Accountability in the Cloud," *IEEE Internet Computing* 15, no. 4 (2011): 64-69.

[39] W. Venters, and E. Whitley, "A critical review of cloud computing: Researching desires and realities," *Journal of Information Technology* 27 no. 3 (2012): 179-197.

[40] H. Wang, W. He, and F. Wang, "Enterprise cloud service architectures," *Information Technology & Management* 13, no. 4 (2012): 445-454, doi:10.1007/s10799-012-0139-4.

Conclusion

Cloud computing is complex, and similarly retention and disposition in the cloud becomes complex due to issues that include multi-tenancy, cross-border legal concerns, and assurances that copies in multiple locations are disposed of according to a disposition schedule or successfully "frozen" if a legal hold is required.

There is a lack of a strong voice of RIM professionals in cloud computing innovations. Scholarly RIM literature on retention and disposition in the cloud is still emerging and underscores the importance of this InterPARES Trust project.

References

Ajero, M. "Random access: Can we trust our studio materials to the "cloud"?" *American Music Teacher* 62, no. 1 (2012): 50-51. http://www.thefreelibrary.com/Random+access%3A+can+we+trust+our+studio+materials+to+the+%22cloud%22%3F-a0299885768

Askhoj, J., Shigeo Sugimoto, and Mitsuharu Nagamori. "Preserving records in the cloud." *Emerald* 21, no. 3 (2011): 175-187. http://dx.doi.org/10.1108/09565691111186858

Autonomy. "Autonomy Records Manager." Autonomy, 2012a. http://www.hp.com/hpinfo/newsroom/press_kits/2012/FallBizPrinting/Autonomy_Records_Manager_Datasheet.pdf

Autonomy. "Best practices for cloud-based information governance." Autonomy, 2013. http://www.informationweek.com/whitepaper/Infrastructure/Network-Systems-Management/making-the-move-to-the-cloud-best-practices-adv-wp1347981072?articleID=191705703

Bashir, M., J. Kesan, C. Hayes, and R. Zielinski. "Privacy in the cloud: Going beyond the contractarian paradigm." Annual Computer Security Applications Conference, Orlando, FL, December 2011. https://acsac.org/2011/workshops/gtip/Bashir.pdf

Blair, B. "Governance for protecting information in the cloud." *Information Management* 44, no. 5 (2010): 1. http://search.proquest.com.libaccess.sjlibrary.org/docview/1033603283?accountid=10043

Cohasset Associates. *MoReq2010: EMC Data Domain Retention Lock Compliance Edition*. Chicago, IL: Cohasset Associates, 2013. http://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf

Dutta, A., G. Peng, and A. Choudhary. "Risks in enterprise cloud computing: The perspective of it experts." *The Journal of Computer Information Systems* 53, no. 4 (2013): 39-48.

Ferguson-Boucher, K., and N. Convery. "Storing Information in the Cloud – A Research Project." *Journal Of The Society Of Archivists* 32, no.2 (2011): 221-239. doi:10.1080/00379816.2011.619693

Géczy, P., N. Izumi, and K. Hasida. "Hybrid cloud management: Foundations and strategies." *Review of Business & Finance Studies* 4, no.1 (2013): 37-50. http://search.proquest.com.libaccess.sjlibrary.org/docview/1445008520?accountid=10361

Gimmal. "Emerging practices for electronic record disposition." Gimmal, 2012. http://www.gimmal.com/Resources/Pages/Gimmal-Whitepaper-Emerging-Practices-for-Electronic-Record-Disposition.aspx

Gold, J. "Protection in the cloud: Risk management and insurance for cloud computing." *Journal of Internet Law* 15, no. 12 (2012): 1-28.

Greengard, S. "Building Clouds That Are Flexible and Secure." *Baseline*. http://www.baselinemag.com/cloud-computing/building-clouds-that-are-flexible-and-secure/

Grounds, Alison and Ben Cheesbro. "Cloud Control: eDiscovery and Litigation Concerns with Cloud Computing." *The Computer and Internet Lawyer* 30, no. 9 (2013): 23-31.

Hitachi Data Systems. *Introduction to Object Storage and Hitachi Content Platform*. Santa Clara, CA: Hitachi Data Systems, 2013. http://www.hds.com/assets/pdf/hitachi-white-paper-introduction-to-object-storage-and-hcp.pdf

Hoke, E. J. G. "Challenges to governing remote information." *Baseline.* http://www.baselinemag.com/c/a/IT-Management/Challenges-to-Governing-Remote-Information-709978/

Ion, I., N. Sachdeva, P. Kumaraguru, and S. Čapkun. "Home is safer than the cloud!: Privacy concerns for consumer cloud storage." Symposium on Usable Privacy and Security, Pittsburgh, PA, July 2011. https://www.vs.inf.ethz.ch/publ/papers/iion-cloud-2011.pdf

Katzan, H. "On the privacy of cloud computing." *International Journal of Management and Information Systems* 14, no. 2 (2010): 1-12.

Kesan, J., C. Hayes, and M. Bashir. "Information privacy and data control in cloud computing: Consumers, privacy preferences, and market efficiency." *Washington & Lee Law Review* 70, no. 1 (2013): 341-472.

Li, J., Sharad Singhal, Ram Swaminathan, and Alan H. Karp. "Managing Data Retention Policies at Scale." *IEEE Transactions on Network and Service Management* 9, no. 4 (2012): 393-406.

McLean, V. "Head in the Cloud?" *New Zealand Management* 59, no. 77 (2012): 44-47.

Muthulakshmi, V., A. Ahamed Yaseen, D. Santhoshkumar, and M. Vivek. "Enabling Data Security for Collective Records in the Cloud." *International Journal of Recent Technology and Engineering* 2, no.1 (2013): 163-167.

Nasuni. "*Law Firm Uses the Cloud to Uphold Stringent Security and Data Retention Requirements.*"Nasuni, 2011. http://www.nasuni.com/case-studies/gesmer-updegrove-llp

Nicolaou, C., A. Nicolau, and G. Nicolau. "Auditing in the cloud: Challenges and opportunities." *The CPA Journal* 82, no. 1 (2012): 66-70.

NIST Cloud Computing Program. *US Government Cloud Computing Technology Roadmap Volumes I, II, and III.* Gaithersburg, MD: NIST, 2014. http://www.nist.gov/itl/cloud/index.cfm

Ovadia, S. "Navigating the challenges of the cloud." *Behavioral & Social Sciences Librarian* 29, no. 3 (2010): 233-236.

Pearson, Siani. "Towards Accountability in the Cloud." *IEEE Internet Computing* 15, no. 4 (2011): 64-69.

Pitt, D. "Trust in the cloud: The role of SDN." *Network Security* 2013, no. 6 (2013): 5-6. http://dx.doi.org/10.1016/S1353-4858(13)70039-4

Rabinovici-Cohen, S., M. Baker, R. Cummings, S. Fineberg, and J. Marberg. "Towards SIRF: Self-contained information retention format." The 4th Annual International Conference on Systems and Storage, Haifa, Israel, June 2011. doi: 10.1145/1987816.1987836.

Rayport, J. and A. Hayward. "Envisioning the Cloud: The Next Computing Paradigm." Marketspace, 2009. http://www.hp.com/hpinfo/analystrelations/Marketspace_090320_Envisioning-the-Cloud.pdf

Reuters. "RSD Information Governance Momentum Continues Into 2014." http://uk.reuters.com/article/2014/03/31/ma-rsd-idUKnBw315282a+100+BSW20140331

Ross, P., and M. Blumenstein. "Cloud computing: The nexus of strategy and technology." *Journal of Business Strategy* 34, no. 4 (2013): 39-47. doi: 10.1108/JBS-10-2012-0061.

Salido, J. and D. Cavit. *Trustworthy computing: A guide to data governance for privacy, confidentiality, and compliance*. Redmond, WA: Microsoft, 2010. http://www.microsoft.com/en-us/twc/privacy/data-governance.aspx

Srinivasan, S. "Is security realistic in cloud computing?" *Journal of International Technology and Information Management* 22, no. 4 (2013): 47-66.

Tang, Y., P. P. Lee, J. C. Lui, and R. Perlman. "FADE: Secure Overlay Cloud Storage with File Assured Deletion." *Security and Privacy in Communication Networks* 50 (2010): 380-397.

Tero, V. "Information Governance in the Cloud." IDC, 2010. http://www.emc.com/collateral/analyst-reports/1010-idc-paper.pdf

Venters, W., and E. Whitley. "A critical review of cloud computing: Researching desires and realities." *Journal of Information Technology* 27 no. 3 (2012): 179-197.

Viewpointe. “Information governance and cloud computing: Approaches for regulated industries.” Viewpointe, 2013. http://www.ciosummits.com/Information_Governance_and_Cloud_Computing_Approaches_for_Regulated_Industries.pdf

Wang, H., W. He, and F. Wang. “Enterprise cloud service architectures.” *Information Technology & Management* 13, no. 4 (2012): 445-454. doi:10.1007/s10799-012-0139-4.