Agreements between Cloud Service Providers and their Clients: A Review of Contract Terms

Robert McLelland, Yvette Hackett, Grant Hurley, Daniel Collins
InterPARES Trust

ABSTRACT: This paper explores the terms currently available in contracts between cloud service providers and their clients. It creates a framework of key term categories that should exist in contracts to fulfill the records needs of organizations. It then compares contracts from companies to determine how well these contracts meet the record keeping needs.

Introduction

Cloud technology is being increasingly offered as a service that allows its clients to readily and scalable store large amounts of business and personal information on far away servers, and then access this information on demand from anywhere in the world. The degree to which these services appear to enable global business activities for a lower cost has resulted in the rapid adoption of cloud services. Despite the speed with which cloud services have begun to be utilized, there remain large concerns regarding the recordkeeping ramifications of such services.

This paper reports on some of the findings of a study that was undertaken as one of the first stages of the InterPARES Trust Project, which aims to develop “frameworks that will support the development of integrated and consistent local, national and international networks of policies, procedures, regulations, standards and legislation concerning digital records entrusted to the Internet, to ensure public trust grounded on evidence of good governance, and a persistent digital memory.” (InterPARES Trust) The goal of this project, titled *Project 10 - Contract Terms with Cloud Service Providers*, was to conduct a survey of currently available cloud service agreements available to an average, low-level consumer in order to gain an understanding of the terms of service that are currently available. The knowledge gained from this project will hopefully be used by other aspects of the InterPARES Trust research effort, namely Project 14, which aims to establish a check-list of requirements from a records management, archival, and legal perspective for cloud service agreements. The agreements that Project 10 looked at were from the United States, Canada, and Europe. This paper will primarily focus its discussion on the agreements that were looked at from European companies.

Overview of the Cloud

Prior to discussing the nature of service agreements between providers and their clients, it is first necessary to establish the foundation in which this research was conducted. This section will introduce concepts within the cloud and the agreement structures that were found by the research group.

Types of Cloud

Cloud services can be provided to clients in a variety of ways. (Rackspace Inc., 2011, p. 3) (Barnes, 2010) The first is what is called a “public” cloud. Although this appears to refer to a cloud owned or used by a public body, in reality this model describes the use of cloud infrastructure by an unknown number of undisclosed clients. (Barnes, 2010)

The next type of cloud service implementation is a “private” cloud. This model describes a service in which the client purchases exclusive use of cloud infrastructure. This type of implementation can be provided remotely but it may also be provided at the client’s site. (Ibid) It may even be owned and administered by the client for its employees. This model is more expensive than the public model, but can offer better security and privacy.

The third type of cloud implementation that is available is a “hybrid” cloud. This describes a model in which infrastructure is both public and private. (Ibid) This model would likely be used for clients who have some information that is not sensitive enough for concern about storage in a public and cheaper infrastructure, but also has information that requires more security.

The final type of cloud is referred to as a “community cloud,” where a specified group of clients all share the same cloud service. (Ibid) This permits clients have the security of knowledge of who else is utilizing infrastructure, while still gaining some of the cost benefits of public cloud.

The cloud providers examined in this study tended to offer all of these forms of implementation. The most common, however, was that of the public model, most likely due to the cost savings it promises clients.

Types of Cloud Services

Cloud services are most commonly offered in three types - Infrastructure as a Service, Software as a Service, and Platform as a Service. (Rackspace Inc, 2011, p. 3)

Infrastructure as a Service (IaaS) refers to the provision of access to hardware (e.g. hard disks, servers, etc.). (Barnes, 2010) This service allows the client to rent IT infrastructure on an as-needed basis, permitting it to increase and decrease infrastructure capacity when needed. This service is beneficial to the clients who purchase it because it is often much cheaper than owning and maintaining it outright.

The second type, Software as a Service (SaaS), refers to the remote access of software hosted on the service provider’s infrastructure by the client. (Ibid) This service enables a client organization to access software it may not need to purchase a full license to or receive updates to the software on a subscription basis rather than purchasing new licenses annually.

Platform-as-a-Service (PaaS) is the third type of service commonly found. This service involves the hosting of an environment by the service provider in which a client can build its own software. (Ibid)

These types of clouds and services are combinable with each other to taylor to the needs of different clients, and many service providers offer a mix and match option. This requires service providers to have multiple small agreements available for different services, which will be discussed more in the next section. This research project focused primarily on public cloud and infrastructure-as-a-service as they are the most likely to contain business records.

Types of Contracts

One of the first things that the research team learned was that there is lack of uniformity within cloud contracts themselves. Many providers use a tiered contract structure, with an overarching contract supplemented by several more specific agreements.

The first tier of this agreement structure features what are called the “Terms and Conditions (TaC),” the “Terms of Service (ToS),” or similarly named documents. These agreements tend to contain language that applies to all the services offered by the provider such as conditions for service termination, legal protections for the service provider in terms of content uploaded by the client, and copyright terms. In general, these contracts describe the client’s obligations when using the service, and they are clearly meant to protect the service provider more than the client.

The second tier of agreements contains the Service Level Agreements (SLA), which provide language for specific services with one SLA being found per service. A study by IBM Research on SLAs identified terms such as “service guarantee metrics” which quantify “availability (e.g., 99.9%), response time (e.g., less than 50ms), disaster recovery and fault resolution time (e.g., within one hour of detection) and how compensation will be calculated and reimbursed for a fault in service. (Baset, 2012. p. 57) Availability or uptime can be offered based on a tiered payment structure. The SLAs also tend to offer service guarantees on a basis of time periods as well as at different granularities. For example, time periods may be measured in requests to the service per minute, hour, day, week, etc., and service interruption may be measured by service, data centre, etc. (Ibid p. 58)

Although this tiered structure is very common amongst service providers. Not every service provider has both a ToS/TaC and SLAs. Some providers have a ToS/TaC and only SLAs for particular services; some have only ToS/TaCs. It is not always immediately apparent how many contracts a service provider requires. When contracts are available on a service provider’s website, they are often difficult to find, though presumably they would be presented to a client as a part of the “signup” process.

Contracts also can change quickly and the non-static nature of these contracts could cause problems. Most contracts require the provider to notify the client of any changes to the contract. While this could not be tested in the course of this project, clients should learn whether cloud service providers have adopted the same notification method as many large organizations, such as banks, credit card companies and social media sites. They notify the client that changes have occurred, but leave it to the client to discover the nature of the changes and their potential impact.

Methodology

This project was undertaken with the goal of assessing current cloud service agreements to determine whether they met the needs of a recordkeeping environment. To do this, the project participants first established baseline criteria for what a cloud service agreement should guarantee to be usable as a recordkeeping tool. This criteria was created by conducting a literature review of recordkeeping standards and white papers from sources such as ARMA International, advice generated by national archival institutions such as the National Archives of Australia and the United States and ISO standards. These sources outlined both the requirements and goals of recordkeeping systems in general, as well as specific concerns that organizations and recordkeeping professionals hold about utilizing the cloud. Additionally, new requirements at times suggested themselves to the research team after assessment began on cloud service contracts and these new requirements would be added to the criteria and the agreements would be reassessed. Ultimately, the research team developed a table containing 15 categories of agreement terms that describe all identified recordkeeping requirements. In essence, these categories were what the research team felt should exist in the ideal agreement.

Companies were selected from North America (Canada and the United States) and Europe. This was done because the research team was interested in how differences in legislation such as privacy legislations and the susceptibility to the Patriot Act might change cloud service agreements. Companies were selected through a combination of their profile and by conducting simple internet searches, and the availability of agreements from the companies.

The companies selected from North America were Google (United States), Amazon (United States), Rackspace (United States), and Profitbricks (United States, also Germany), Telus (Canada), Storagepipe (Canada), Titanfile (Canada), Pathway Communications (Canada), and OpenText Corporation (Canada). The companies selected from Europe were City Network (Sweden), CloudSigma (Switzerland), GreenQloud (Iceland), and T-Systems (Germany).

Although all these companies were reviewed by the project team, agreements were not readily available for all of them. Due to the ground work nature of this project for the rest of InterPARES trust, it was determined that expediency was important, and that only companies whose contracts could be found online would ultimately be assessed. The full report on this project for InterPARES Trust contains a description of each company reviewed, however for the purposes of this conference paper, only the European companies will be fully discussed.

CityNetwork

The Swedish internet services company CityNetwork provides, in addition to domain and hosting services, a cloud platform for cloud storage through an API and scalable services depending on user needs.

The company markets its SLA as “an SLA you can trust” in its General Conditions for My CityCloud document (CityNetwork, 2011) and Service Level Agreement (CityNetwork) page that contains the basic services offered by the company and the individual roles and responsibilities of the company and a contracted client.

CloudSigma

CloudSigma is a Switzerland-based IaaS public cloud services provider. The company utilizes six documents available on its website: an Acceptable Use Policy (CloudSigma, 2012a), a Copyright Notice (CloudSigma, 2012b), a Privacy Policy (CloudSigma, 2013a), a Service Level Agreement (CloudSigma, 2013b), and a Terms of Service (CloudSigma, 2013c). Where the SLA outlines CloudSigma’s service guarantees to clients, the Acceptable Use Policy and the Copyright Notice enforce the behavior of users. The ToS document gives greater granularity to these prior documents, including clauses limiting liability and giving no warranty in addition to terms surrounding contract termination and data protection.

GreenQloud

GreenQloud is an Iceland based company that offers IaaS, PaaS, backup, and SaaS in public, private, and hybrid models. In addition to this, GreenQloud’s privacy policy states that "GreenQloud with headquarters in Iceland, abides by regulations set by Icelandic law [provides external link], which has adopted most of the European Economic Area (EEA) regulations [provides external link]." (GreenQloud)

GreenQloud utilizes a two-tier contract model, employing an End-User License Agreement (GreenQloud, 2013), which provides more general terms as well as a Service Level Agreement (GreenQloud, 2014), which has service specific language.

T-Systems

T-Systems is a German company that specializes in providing information services on an enterprise level. One of the services that it offers is what it calls Zero Distance, which is a suite of cloud based services. (T-Systems, 2014a) T-Systems also offers to help its clients customize their cloud services through what it calls Cloud Readiness and Management Services. (T-Systems, 2014b)

Literature Review

As previously stated, the term categories were developed by combining accepted recordkeeping requirements and needs with concerns expressed from the professional recordkeeping community as well as the information technology community. Both the recordkeeping professionals and IT professionals identified a need for:

- Storage specifications (primarily hardware)
- Security of the infrastructure (both physical and technological)
- Access authority
- Data segregation (physical)
- Regularity of access

Meanwhile, articles written by recordkeeping professionals generally agreed that the following was should be concerns for any organization entering the cloud:

- Disposal scheduling and proper disposal methods
- Jurisdiction of storage
- Records loss or premature destruction
- Loss of value as evidence
- Long-term viability
- Loss of confidentiality/protection of privacy.

Unsurprisingly, the concerns expressed by recordkeeping professionals could also largely be found in accepted recordkeeping standards and guidelines. ISO 15489, for example, lays out what a recordkeeping system should contain, including elements such as the ability to retain and properly dispose of records at any time and in a way that permits audit trails, requirements for physical protection of records media, timely and efficient access, and capture and classification. (International Standards Organization, 2001, pp. 10-16) The ARMA International Generally Accepted Recordkeeping Principles, meanwhile, lays out eight principles that are necessary for a strong recordkeeping system: accountability, integrity, protection, compliance, availability, retention, disposition, and transparency. (ARMA International, 2014) All of these principles and requirements would still be necessary in a cloud storage system and would therefore need to be addressed in contract clauses.

From this literature review and the iterative process of agreement assessment, the research group settled on 15 categories. These categories were placed into 4 groups of other like categories.

Group 1 includes all contract term categories related to the ability to destroy records. This group could not be encompassed by just one category, as the literature tended to have different apprehensions related to destruction: RIM professionals were concerned with destruction as part of a retention and disposition policy, as well as ensuring no copies would remain with the service provider at the end of the contract.

Group 2 was used to encompass different situations that affect a client’s ability to access records whenever necessary, and how such access will be ensured.

Group 3 encompasses term categories that deal with a client’s ability to trust the records that are stored within the cloud service.

Group 4 covers a client’s control over records and the information contained within them such as their legal rights over the information and their responsibilities to protect personal information.

Identified Categories of Contract Terms

The 15 categories and their group placement are as follows:

Group 1: General Destruction Guarantee

Requires language guaranteeing that records can be destroyed when the end of the client's retention period is reached and no copies whether backups or otherwise would remain.

This category is drawn from a combination of sources and is regularly mentioned by RIM professionals when writing about moving records into the cloud. (Stuart, Bromage, 2010, p. 221; Ju, Wu, Fu, Lin, 2011, p. 1768; Ferguson-Boucher, 2011, p. 64; National Archives of Australia, 2013; National Archives and Records Administration, 2013; Council of Australasian Archives and Record Authorities, 2010, pp. 10-11; Blair, 2010) It is also a requirement in all of the professional standards that were consulted during the course of this research. (International Standards Organization, 2001, ; ARMA International, 2013; Department of Defense, 2007; European Commission, 2008, pp.14-16)

Group 1: Specific Destruction Method

Requires language specifying the method by which records will be destroyed to ensure that it is acceptable to the client and that it is in accordance with record keeping requirements.

This is drawn from requirements on how records will be destroyed in a digital environment. "Knowing" that a record is destroyed is paramount, as even records stored on backup could be subject to e-discovery. A client would need to know how copies of their records could be ensured destruction by the service provider when the time for their disposal arrives. Degaussing, physical destruction, and reformatting are examples of acceptable methods of digital record destruction. (Shepard, Yeo, 2002 p. 171) ISO 15489 recommends that records be reformatted or overwritten, (International Standards Organization, 2001, p. 21) and that records stored off site from an organization require documentation as proof of destruction. (Ibid)

Group 1: Destruction on Contract Termination

Requires language guaranteeing that any remaining records of the client can be retrieved by the client or will be destroyed by the service provider at the time the contract concludes.

Any records remaining with the service provider after contract termination could still pose a security risk to the client.(Stuart and Bromage, 2010, p. 223) RIM professionals and RIM bodies recommend receiving assurances that no information or records will remain with the service provider at the end of the contract. (Ibid; Council of Australasian Archives and Records Authorities, 2010, pp. 12-13)

Group 2: Service Continuity

Requires language guaranteeing that service will not be ended without warning and that should the service no longer be offered by the service provider, the client will have adequate time to retrieve its records from the service prior to the cessation of access.

Some RIM professionals expressed concerns that records would be unavailable should service suddenly cease. (Rennie, 2010, pp. 14-16) The inability to access records when needed can be disastrous to organizations. The Economist Intelligence Unit reports that 47% of businesses state that they could endure less than a day without access to their records. (Economist Intelligence Unit, 2007, p. 2) The same study cites a National Archives and Records Administration's claim that 25% of businesses that experienced an IT outage of as few as 2 days went bankrupt. (Ibid)

Group 2: Outages

Requires language guaranteeing the client that its records will be available for the vast majority of the time (i.e. 99.99% of the time).

This category also comes from the potential danger to a client if information is inaccessible for periods of time. A contract would need to guarantee a high level of uptime for the service and include a description of the compensation to the client that will result from less than maximum uptime.

Group 2: Disaster Recovery Plan

Requires language describing the provisions of the provider's disaster recovery plan in the event that damage occurs to the servers or their ability to connect to the Internet.

Vital records need to be recovered quickly in the event of a disaster. (European Commission, 2008, p. 48) Records in the cloud are ultimately stored physically somewhere, and are therefore at risk of disaster just as paper records or onsite digital records are. (Council of Australasian Archives and Records Authorities, 2010, p. 10; Blair, 2010, p. 3) Should a cloud service provider experience a disaster, a client would want reasonable knowledge of how its information would be recovered by the service provider prior to entering into the contract. Ideally, the extent to which a service provider would go to recover information would be contractually described. (Blair, 2010, p. 3; Cunningham, 2010, p. 7)

Group 3: General Security Provisions

Requires language that guarantees a level of security to the client for its records (i.e. at least the same level of security as the company provides for its own records).

This category is drawn from the need to protect the integrity of records. All standards that were reviewed discussed the importance of security and controlled access to records. (International Standards Organization, 2001 pp. 12-13; European Commission, 2008, pp. 41-45; Department of Defense, 2007, pp. 49-53) A client should be guaranteed that the service provider will provide security for information in its custody.

Group 3: Physical Security Specifications

Requires language that guarantees specific security for the physical servers and the physical location in which they reside.

This category is related to Group 3: General Security Provisions, but pertains specifically to information about physical security. Given that the records' physical location will be on servers controlled by the service provider, the client will need to know what precautions are in place to control physical access to the servers and their content pursuant to ISO 15489-2. (International Standards Organization, 2001, p. 12) Additionally, a white paper published by the Cloud Security Alliance identifies threats to the physical location of records can emerge in the form of malicious insiders. (Cloud Security Alliance, 2010)

Group 3: Technological Security Specifications

Requires language that guarantees specific security for the technology on which the records are stored (i.e. the use of firewalls).

This category also comes from the ISO 15489 requirement for controlled access. (ibid) Given that clients will not be able to monitor the traffic on the cloud service provider's infrastructure themselves, a contract would need to guarantee a certain level of security to ensure records are not accessed without permission. Threats can come in forms such as hackers attacking the service by transmitting malicious software to a public IaaS and weaknesses to the interface software. (Cloud Security Alliance, 2010, pp. 8-9)

Group 3: Tiered Security Provisions

Requires language that guarantees specific enhanced security which can be adjusted to match the identified sensitivity of record.

This category acknowledges that certain records are more sensitive than others. Should a client decide to take on the risk of storing these sensitive records in the cloud, terms should indicate what protections will be afforded to them. An example of this is records containing personal identifiable information. ISO requires that access controls be put in place for records of this nature, (Ibid) as well as being required by governing bodies such as in the European Union's Privacy Directive. (European Union Privacy Directive Article 17, section 2) In addition, RIM literature lists protection of privacy as a concern of moving into the cloud. (Blair, 2010, p. 3)

Group 4: Territory of Storage

Requires language that guarantees the political territory where records will be stored and backed up throughout the entirety of their life within the cloud service (i.e. would the records be stored in the United States, the European Union, etc.).

This category was chosen largely due to the requirements found in legislation and directives, such as the European Union Privacy Directive Article 25, or the requirements for public bodies of British Columbia to store personal information within Canada (British Columbia Freedom of Information and Protection of Privacy Act, Section 30.1).

Group 4: Copyright/Ownership

Language that guarantees that the client will retain full copyright to the records and information and that ownership of any metadata that is applied to the records stored within the cloud service will also remain with the client.

This category was drawn from RIM professionals' concerns over assurances that information placed into storage in the cloud will remain under the copyright of the client. This idea has been expanded to include copyright over the metadata applied to the records by the cloud service provider as such metadata would be necessary to ensure its authenticity.

Group 4: General Privacy

Language that refers to general privacy provisions.

Group 4: Privacy Policy

Language that refers to a privacy policy.

Group 4: Privacy Legislation

Language that refers to privacy legislation.

The three last categories in group 4 were all drawn from organizations' obligations under various privacy and protection of personal information legislation. These three categories of terms would be necessary for a client to understand the full scope of a service providers' attitude and responsibilities towards personally identifiable information that is stored within the cloud infrastructure. Existing contracts often referred to privacy, a privacy policy, and privacy legislation in separate clauses, so the Terms were also separated in the table.

Privacy is a common concern among professionals and references to it are frequent in the literature. (Ferguson- Boucher, 2011, p. 64. Also Stuart and Bromage, 2010, pp. 220 and 223) A study at the Fordham University School of Law found that student data is often being placed in cloud computing services whose contract terms do not adequately protect student privacy. This study recommends contract terms that more directly address privacy. (Reidenberg, Russell, Kovnot, Norton, Cloutier, and Alvarado, 2013, pp.71-72) Standards of practice such as ISO 15489 also advise that there are regulatory requirements related to privacy in information storage. (International Standards Organization, 2001, p. 14)

Findings in Agreements from European Companies

The table below was created to display the findings of the assessment of European cloud service provider agreements. Each company has a box that corresponds with each term category. Language that corresponds with these categories is listed in each box, including the name of the agreement and the section with the pertinent language. Language that is positive towards the category is highlighted in green, while language that is negative towards the category is highlighted in red.

nmary of Contract and Service Ter red by Cloud Service Providers -Eu			
	City Network	**CloudSigma**	**GreenQloud**
ry	**Europe (Sweden)**	**Europe (Switzerland)**	**Europe (Iceland)**
1: General Destruction Guarantee	not addressed	not addressed	not addressed
1: Specific Destruction Method	not addressed	not addressed	not addressed
1: Destruction on Contract Termina	not addressed	not addressed	not addressed
2: Service Continuity	al Conditions - 5	of Service 3.13 and 10.2	ser License Agreement - 6
2: Outages	al Conditions - 5	Sigma Service Level Agreement	Qloud - Service Level Agree
2: Disaster Recovery Plan	dressed	of Service - 3.11	dressed
3: General Security Provisions	not addressed	of Service - 10.6 and Service Leve nent	ser License Agreement - 10
3: Physical Security Specifications	not addressed	not addressed	not addressed
3: Technological Security Specifica	not addressed	of Service - 10.6 and Service Leve nent	not addressed
3: Tiered Security Provisions	not addressed	of Service - 10.6	not addressed
4: Territory of Storage	not addressed	Sigma Privacy Policy	not addressed
4: Copyright/Ownership	not addressed	not addressed	not addressed
4: General Privacy	al Conditions - 9	of Service - 12	Qloud Privacy Policy
4: Privacy Policy	al Conditions - 9	any Privacy Policy	Qloud Privacy Policy

4: Privacy Legislation	al Conditions - 9	not addressed	not addressed

City Network

Group 2: Service Continuity - Group 2: Outages - General Conditions for My City Cloud s. 5(a):

“In case of a breakdown, errors or no access to the services, customer can be reimbursed based on SLA available here: http://www.citynetwork.eu/100-uptime-guaranteed. Breakdown time starts after it is reported by the client and lasts until it is fixed. Total reimbursement is limited to a maximum of a monthly fee for a month in question.” (CityNetwork, 2011)

In this language City Network stands by a 100% uptime guarantee for which the company is willing to reimburse customers if and downtime occurs. These terms are qualified by sections 5(b) and (c) of the General Conditions that explain that any client error, including misuse of the service, or attacks from third parties, or scheduled maintenance downtime, that cause breaks in availability will not be subject to reimbursement. In section (d) the policy gives clients seven days to make claims for downtime reimbursement. The company’s informal Service Level Agreement page gives the reimbursement amount as “5% of the total monthly fee for each 3 hours interval.” (CityNetwork)

Group 4: General Privacy – Group 4: Privacy Policy – Group 4: Privacy Legislation – General Conditions – 9

“a) City Network manages Customer data according to personal data protection act. Customer data is not available to any third party. The exception is a situation in which the Customer violates the terms of the agreement, or the authority will require the provision of such data.” (CityNetwork)

This language encompasses the 3 privacy areas of Group 4. It provides that the company adheres to the Personal Data Protection Act, providing reasonable assurances to its client about the safety of that client’s data.

CloudSigma

Group 2: Service Continuity – CloudSigma Terms of Service s. 3.13 and 10.2

“We will endeavour to provide you with reasonable notice of any suspension under this clause unless it our reasonable belief that an immediate suspension or shorter notice is required to protect our network infrastructure and services to other customers from significant operational or security risk or because we are compelled to do so by law.” (CloudSigma, 2013c)

“You or us may terminate the Agreement by giving thirty (30) days written notice (including without limitation email notice).” (Ibid)

These sections provide some reasonable assurances that the service will not end abruptly so long as the client adheres to the terms of service.

Group 2: Outages – CloudSigma Service Level Agreement

CloudSigma gives three terms for availability in its Service Level Agreement (Ibid) (CloudSigma, 2013b): virtual server availability (100%); network uptime (100%) and network latency (1ms or less). In the same document, it allows users to apply for credit 30 days following a disruption. Credit is defined at “50 times the fees for any period of lack of availability” for any of the above categories. Furthermore, the SLA guarantees “Credit of your entire fee for the previous 30 calendar days in case of permanent loss of your stored data resulting from hardware or software failure of CloudSigma's systems. This provision entirely excludes data loss or corruption resulting from software running within a virtual server." All credits are subject to further limitations including illegal uses of the services or third-party attacks.

Group 2: Disaster Recovery Plan - CloudSigma Terms of Service s. 3.11

"We shall not be responsible for any back up, recovery or other step required to ensure that data and information stored on the CloudSigma network and infrastructure as part of provision of Services to you is recoverable in the case of any data loss, system fault, software failure, hardware failure or other activity which results in any loss of data, information or other item that is being stored as part of our Services." (CloudSigma, 2013c)

CloudSigma absolves itself of a disaster recovery plan by claiming no responsibility for any data loss. Section 4.1.7 on the use of the services gives the direction to "use reasonable security precautions in relation to your use of the Services.

Group 3: General Security Provisions – CloudSigma Terms of Service s. 3.18

"We have no obligation to provide security other than as stated in the Agreement. We disclaim any and all warranties not expressly stated in the Agreement, including the implied warranties of merchantability, fitness for a particular purpose, and non-infringement." (Ibid)

Despite the language in this section, no other security guarantees except basic encryption details (contained in the Privacy Policy) are provided in any of the documents referred to collectively as the "Agreement," particularly the Service Level Agreement. As above, the burden of security provision falls to the user in the Terms of Service.

Group 3: Technological Security Specifications – CloudSigma Privacy Policy

"All Virtual Drive Data is stored encrypted using a 256bit AES-TLX encryption cascade." (CloudSigma, 2013a)

This language provides uncommon detail about the technological security that is employed by CloudSigma.

Group 4: Territory of Storage – CloudSigma Privacy Policy

"All Virtual Drive Data uploaded to CloudSigma is stored securely on our servers in our dedicated rack space in Switzerland." (Ibid)

In this language, CloudSigma again provides a very useful specification to its clients, who are able to know which jurisdiction their records will be stored in and determine if that jurisdiction suits their needs.

Group 4: General Privacy - Group 4: Privacy Policy - Terms of Service 12 and Privacy Policy

"All collection, storing and use of your data are governed by the Privacy Policy." (Ibid)

CloudSigma refers clients to its Privacy Policy, which governs the privacy guarantees offered by the service provider. CloudSigma actually offers different privacy policies for clients in different jurisdictions: Switzerland and the United States.

GreenQloud

Group 2: Service Continuity - End User License Agreement - 6

"If the Company thinks it necessary to suspend a customer's Service without cause, the Company will provide 14 days advanced notice." (GreenQloud, 2013)

This language guarantees that the client will have two-weeks warning of the loss of access to records.

Group 2: Outages – Service Level Agreement

The GreenQloud Service Level Agreement ensures 100% uptime, and offers deductions from the billing cycle for a loss of service. (GreenQloud, 2014)

Group 3: General Security Provisions – End User License Agreement – 10

"…You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content…" (GreenQloud, 2013)

With this language, GreenQloud removes security responsibilities from itself.

Group 4: General Privacy – Group 4: Privacy Policy – Privacy Policy (GreenQloud)

GreenQloud has a privacy policy that outlines its position on protecting the privacy of its clients. The policy does not make any references towards legislation, however.

Group 4: General Privacy – Group 4: Privacy Policy – Privacy Policy (Ibid)

GreenQloud has a privacy policy that outlines its position on protecting the privacy of its clients. The policy does not make any references towards legislation, however.

Conclusions

The three European companies whose agreements were assessed had language that largely did not meet the categories that were identified by the research team. CloudSigma was by far the most comprehensive in terms of the categories, with language pertaining to a majority of them. In particular, CloudSigma had language that was particularly concerned with the security of the system, which the majority of other companies, including those looked at in North America, did not have. All the company agreements assessed had references to privacy and the amount of time clients could access their information that is stored with the service. It is possible that this is because a majority of clients have these concerns and the agreements reflect this demand.

Further Research

There are a few areas where research should head from these findings within the InterPARES Trust project. The primary area for increased research is with the adaption of the categories for archival institutions. Presently, there are no categories that are focused on the long-term preservation of records that are stored in cloud services. Particular areas for concern are access to the metadata that are assigned to information within cloud services and whether these metadata can be used by an archival institution or the creator to determine the authenticity of the records. There are also concerns over data migration and media obsolescence that have not yet been addressed in the current categories. Records creators and those tasked with the preservation of the records will likely want assurances that information will not be lost because the file formats initially used are no longer supposed or the hardware the information was stored on has become obsolete.

InterPARES Trust Project 14 is currently working on these issues and has begun to reassess the agreements that were initially looked at by Project 10. So far, new assessment criteria have been created that include archival concerns and will be used to illustrate the current state of cloud service agreements in this regard. After this assessment is completed, a checklist will be created to help cloud service clients ensure that necessary recordkeeping needs are being met by the language in their agreements.

Post-Research Publications

In the time since this research was completed, several standards and guides have been prepared by other organizations to attempt to guide clients who are seeking the use of clouds services. These services and guides are as of yet not focused solely on recordkeeping needs, but do include elements that are related.

The most primary example at this time is the Cloud Service Level Agreement Standardisation Guidelines, published by the European Commission in June of 2014. These guidelines have recommendations related to recordkeeping that are comparable to the categories identified by this project. The guidelines refer to these as Service Level Objectives (European Commission, 2014, p. 6), and the include many of the same ideas as this project identified including Performance (p. 15), Security (p. 20), Data Management (p. 27), and Personal Data Protection (p. 31). These concepts describe what the guideline calls Service Level Objects, or elements that should be included in cloud service provider agreements and the guideline breaks them down into smaller concepts where encompass much of what was described by the Project 10 research team. The Performance Service Level Objective, for example, lists availability and the ability to have all data destroyed by the service provider at service termination as objectives of good agreements, similar to the term categories described by Project 10.

Additionally, in August of 2014, the International Standards Organization released ISO/IEC 27018:2014 which provides standards for the handling of personal identifiable information in the cloud and will publish ISO/IEC 27017 in 2015 to provide standards for security of cloud services. These two standards will provide some of the first international advice for storing sensitive information in a cloud environment.

Further research in the wake of these publications the same and additional service agreements would provide an interesting comparison to the assessments of agreements done not just in Europe but in North America as well. Such research would potentially reveal whether the guideline and standards have been implemented by providers and to what degree.

Bibliography

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

BARNES, Frederick (2010). ARMA International, "Putting a Lock on Cloud-Based Information." Last modified 2010. http://content.arma.org/imm/JulyAug10/ IMM0710puttingalockoncloud-basedinformation.aspx. [Last accessed November 17, 2012]

BASET, Salman (2012). "Cloud SLAs: Present and Future." ACM SIGOPS Operating Systems Review. no. 2. PP. 57-66.

BLAIR, Barclay T (2010). "How to Manage Information Governance Challenges." Last modified 2010.. http://www.arma.org/HotTopic/HotTopic910.pdf. [Last accessed November 17, 2012]

CLOUD SECURITY ALLIANCE (2010), "Top Threats to Cloud Computing V1.0." Last modified March 2010. [Last accessed February 4, 2014]

CLOUDSIGMA (2012). “Acceptable Use Policy.” Last updated May 2, 2012. https://www.cloudsigma.com/legal/acceptable-use-policy/. [Last accessed February 3, 2014]

CLOUDSIGMA (2012). “Copyright Notice.” Last updated May 2, 2012.,https://www.cloudsigma.com/legal/copyright-notice/. [Last accessed February 3, 2014]

CLOUDSIGMA (2013). “Privacy Policy.” Last updated May 2, 2012., https://www.cloudsigma.com/legal/privacy-policy/. [Last accessed February 3, 2014]

CLOUDSIGMA (2013). “Service Level Agreement.” Last updated November 11, 2013., http://www.cloudsigma.com/legal/service-level-agreement/. [Last accessed February 3, 2014]

CLOUDSIGMA (2013). “Terms of Service.” Last updated July 1, 2013. http://www.cloudsigma.com/legal/terms-of-service/. [Last accessed February 3, 2014]

CITYNETWORK (2011). “General Conditions for My City Cloud.” Last updated 2011. https://www.citycloud.com/wp-content/uploads/2011/09/SLA-City-Cloud-eng.pdf. [Last accessed February 3, 2014]

CITYNETWORK (n.d.). “SLA (Service Level Agreement) – Dedicated servers, co-location and virtual servers.” https://www.citynetworkhosting.com/sla-service-level-agreement-dedicated-servers-co-location-and-virtual-servers. /. [Last accessed February 3, 2014]

COUNCIL OF AUSTRALASIAN ARCHIVES AND RECORDS AUTHORITIES (2010). "Advice on managing the recordkeeping risks associated with cloud computing." ADRI

CUNNINGHAM, Patrick (2010). "IT’s Responsibility for Security, Compliance in the Cloud." Hot Topic: Making the Jump to Cloud. P. 6-10.

ECONOMIST INTELLIGENCE UNIT (2007), "Business Resilience: Ensuring Continuity in a Volatile Environment." http://graphics.eiu.com/files/ad_pdfs/eiu_Bus_Resilience_wp.pdf. [Accessed November 17, 2012]

EUROPEAN COMMISSION (2014). “Cloud Service Level Agreement Standardisation Guidelines.” Brussels, Belgium.

EUROPEAN COMMISSION (2008). "MoReq2 Specification." http://www.moreq2.eu/moreq2

FERGUSON-BOUCHER, Kirsten (2011). "Cloud Computing: A Records and Information Management Perspective." Security & Privacy, IEEE. 9. no. 6 P. 63 - 66.

GREENQLOUD. "Privacy Policy." GreenQloud Privacy Policy Comments. https://www.greenqloud.com/privacy-policy/ [Last accessed May 18, 2014]

GREENQLOUD. "End-User License Agreement (EULA)." GreenQloud EndUser License Agreement EULA Comments. https://www.greenqloud.com/eula/ [Last accessed May 18, 2014]

GREENQLOUD. "Service-Level Agreement (SLA)." GreenQloud ServiceLevel Agreement SLA Comments. https://www.greenqloud.com/sla/ [Last accessed May 18, 2014]

INTERPARES TRUST. “Research - About Research.” Retrieved September 1, 2014.

INTERNATIONAL STANDARDS ORGANIZATION (2001). ISO 15489 - Information and Documentation - Records Management.

JU, Jiehui, Jiyi Wu, Jianqing Fu, and Zhijie Lin (2011). "A Survey on Cloud Storage." Journal of Computers 6. no. 8 P. 1764-1771.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. Government of the United States of America, "Frequently Asked Questions about Managing Federal Records In Cloud Computing Environments." http://www.archives.gov/records-mgmt/faqs/cloud.html. [Accessed November 22, 2013]

RACKSPACE, INC. "Rackspace Private Cloud." Accessed January 26, 2014. http://www.rackspace.com/cloud/private/.

RACKSPACE INC, (2011). "Understanding The Cloud Computing Stack SaaS, Paas, IaaS." CloudU.

REIDBURG, Joel; Russell, N. Cameron; Kovnot, Jordan; Norton, Thomas B.; Cloutier, Ryan; and Alvarado, Daniela (2013). "Privacy and Cloud Computing in Public Schools". Center on Law and Information Policy. Book 2.

http://ir.lawnet.fordham.edu/clip/2

RENNIE, Stuart (2010). "Legal Implications of Working in the Cloud." Hot Topic: Making the Jump to Cloud. : P. 11-16. http://www.arma.org/docs/hot-topic/makingthejump.pdf [accessed February 4, 2014]

STUART, Katharine, and David Bromage (2010). “Emerald Article: Current state of play: records management and the cloud." Records Management Journal. 20. no. 2 p. 217 - 225. http://dx.doi.org/10.1108/09565691011064340 [accessed November 17, 2012]

U.S. DEPARTMENT OF DEFENSE (2007). “Electronic records management software applications design criteria standard.”http://www.dtic.mil/whs/directives/corres/pdf/501502std.pdf