Cloud Service Contracts: An Issue of Trust / Les contrats de service d'informatique en nuage: Une question de confiance

Jessica Bushey, Marie Demoulin, Robert McLelland

Canadian Journal of Information and Library Science, Volume 39, Number 2, June juin 2015, pp. 128-153 (Article)

Published by University of Toronto Press
DOI: *https://doi.org/10.1353/ils.2015.0009*

Cloud Service Contracts: An Issue of Trust

Les contrats de service d'informatique en nuage : Une question de confiance

Jessica Bushey
School of Library, Archival and Information Studies, University of British Columbia
jbushey@mail.ubc.ca

Marie Demoulin
École de bibliothéconomie et des sciences de l'information, Université de Montréal
marie.demoulin@umontreal.ca

Robert McLelland
Delta Museum and Archives
robertmclelland@gmail.com

Abstract: This article compares cloud service contracts with records management and archival needs to determine whether or not those needs are met by currently available, boiler-plate contracts. It finds that, in general, the requirements of storing and preserving authentic records are not met by current cloud service agreements. It ends by proposing a checklist of requirements for recordkeeping professionals to utilize in negotiating or choosing contracts to better support the needs of authentic records in the cloud.

Keywords: cloud, authenticity, contracts

Résumé : Cet article envisage les contrats de services informatiques en nuage au regard de la gestion des documents d'archives et des besoins archivistiques, afin de déterminer si ces besoins sont satisfaits par les contrats standards actuellement disponibles. Il en ressort qu'en général, les exigences de stockage et de conservation des documents sous une forme authentique ne sont pas satisfaites par les accords actuels de services informatiques en nuage. L'article se termine en proposant une grille de lecture à l'attention des professionnels de la gestion et de la conservation des documents, à utiliser dans les négociations ou la sélection des contrats, afin de mieux répondre aux besoins de conserver des documents authentiques dans l'informatique en nuage.

Mots-clés : informatique en nuage, authenticité, contrats

Introduction

Cloud-based services are increasingly becoming a key part of how organizations worldwide conduct business activities. Encompassing a large array of possible models, the term "the cloud" describes a service wherein a client may purchase scalable access to information technology (IT) infrastructure for the creation, use, management, and/or storage of information. The ease with which large

amounts of information can be affordably stored and accessed from anywhere with an Internet connection has made these services an attractive option for organizations of various types. Despite this advantage, the risks of adopting cloud-based services are largely unrecognized and not well understood, which can result in cloud customers using services that do not meet with the best practices and legislation governing the management and storage of information and business records.

Research milestones

This article reports on research being conducted by the InterPARES Trust (ITrust) project on current cloud service contracts from a records management, archival, and legal perspective. ITrust (2013–18) is a multinational, interdisciplinary research project exploring issues concerning trust of digital information and records in the online environment (InterPARES Trust 2014). The research discussed in this article builds upon an earlier study conducted by ITrust entitled Project 10: Contract Terms with Cloud Service Providers, which explored the extent to which cloud service contracts met general records management requirements. The findings of this study revealed that the majority of selected cloud providers' contracts did not meet records management requirements. With this foundation, the current study aims to examine the issues further from the archival point of view and incorporate a stronger legal framework. The study is guided by the overarching research question: how effective are cloud service providers' terms and agreements at addressing the needs of records managers and archivists?

At this early stage in the research, the qualitative content analysis of selected cloud service providers' terms and agreements, recordkeeping standards, and legal requirements have been conducted and the results are discussed in this article, along with a preliminary set of recommendations/draft checklist for both cloud providers and customers to consider. The research that is described does not constitute the entirety of the project's work but, rather, reports on the research conducted thus far, in an effort to share preliminary findings with records managers and archivists as well as lawyers and cloud service providers and encourage feedback.

Terminology

There are several terms used throughout this article, which may be interpreted differently depending upon the disciplinary viewpoint. In an effort to provide consistency across ITrust research projects, definitions available in the *InterPARES 2 Dictionary* have been used whenever possible (InterPARES 2 Project 2015). In the context of recordkeeping standards and/or legal acts, which utilize specific terms and provide definitions, all attempts have been made to clarify usage to the reader and include citations. There is an absence of standardized terminology across cloud service contracts that refers to customer content (that is, data, information, and records); therefore, throughout this article the term data refers to the smallest meaningful units of information. The term information refers to an assemblage of data intended for communication either through

space or across time. The term record refers to a document made or received in the course of a practical activity as an instrument or a by-product of such activity that is set aside for action or reference.

In archival science, records are considered trustworthy if they are reliable (that is, they can stand for the facts they are about), accurate (that is, the records are precise, correct, and free of error or distortion), and authentic (that is, the records are what they purport to be and are free from tampering or corruption). It is important to understand that authenticity is established by assessing the identity (that is, the whole of the characteristics of a record that uniquely identify it and distinguish it from any other record) and the integrity of a record (that is, the quality of being complete and unaltered). The recordkeeping standard, *ISO 15489-1: Information and Documentation—Records Management Part 1*, which was issued by the International Standards Organization (ISO) in the fall of 2001, addresses authenticity and integrity separately, in that an authentic record is what it purports to be and a record has integrity if it can be proven that it has remained complete and unaltered after being set aside (ISO 2001). There is an absence of standardized terminology across cloud service contracts to refer to confidentiality, privacy, and security. Admittedly, it is beyond the scope of this article to discuss these terms in depth, therefore working definitions in the context of the ITrust project and its focus on cloud computing are provided. Confidentiality refers to the expectation that private facts entrusted to another will be protected and not shared without consent. Privacy refers to control over access and use of personal information. Security is the state of being protected from unauthorized access.

Methodology

Taking an interdisciplinary approach, the authors explored literature on cloud services and the terms and agreements in the areas of archival science, records management, and law. The literature review (discussed in second section of this article) identified key concerns regarding cloud contracts and balancing the specific needs of cloud service customers within the complex infrastructure and service delivery of large cloud providers. Furthermore, it identified several initiatives and guidelines, which address the challenges being faced by agencies and organizations considering the adoption of cloud-based services.

The second phase of the study involved the comparative analysis of selected cloud provider terms and agreements with recordkeeping standards and legal framework (discussed in the third section of this article). The analysis (presented in the fourth section) reveals several issues, in particular, gaps in the existing cloud provider contracts regarding the availability of metadata assigned to data, the ability to audit data, uncertainty about where the data are stored, difficulties in destroying and migrating data, and difficulties in establishing the authenticity of the data stored within these services. The recommendations (presented in the fifth section) are an attempt to address the gaps. The aim of the research is to provide a checklist to guide records managers and archivists through the process of assessing cloud provider contracts and determining if the agreements meet

recordkeeping standards and legal requirements specific to their organization and/or institution. The authors recognize that larger organizations can, and probably do, negotiate better contracts for their services, but many smaller organizations or members of organizations cannot do so or choose not to do it. Potentially, the checklist could be used within an organization to communicate the needs of records mangers and archivists to administration and IT support.

Literature review

The literature review undertaken in the course of this research was done to establish primarily a foundation for what the requirements for a recordkeeping system should be regardless of the medium, to review current research on cloud service agreements and their legal frameworks, and to determine what current standardization efforts exist for cloud service agreements.

Summary of the ITrust's Project 10

As stated earlier, the findings of Project 10: Contract Terms with Cloud Service Providers presented the impetus for the current study. Project 10 selected nine cloud service providers from Canada, the United States, and Europe in an effort to address a wider range of jurisdictions. Providers' online contracts were analysed, and a set of fifteen categories of contract terms was identified. Passages of the cloud provider contracts were classified as meeting, or not meeting, the general records management needs. The findings of the study reveal that most of the selected cloud provider contracts do not meet general records management requirements.

Recent studies on cloud computing

As part of the literature review, the authors explored recent studies on cloud computing, which stem from the areas of archival science, records management, and law. Through this review, the authors learned that cloud service terms and agreements tend to be broken into several legal documents (Bradshaw, Millard, and Walden 2011). The agreements include a general document for services, such as the terms of service, a document for more specific service such as the service level agreement, and documents covering other general areas such as the privacy policy and the acceptable use policy (ibid.). In addition, research has found that there very little standardization of terms exists across providers' agreements (Baset 2012). The authors of this article also took into account the literature by legal scholars, which examines privacy and security issues raised by the cloud's adoption. The authors noticed that several studies have been conducted to examine the legal framework for the use of cloud-based services by the federal and provincial authorities (Vermeys, Gauthier, and Mizrahi 2014).

Recordkeeping standards

In seeking to identify general recordkeeping requirements, the authors of this article consulted standards and guidelines that have been established by international bodies and organizations. Their primary source for identifying these requirements was the ISO's report *ISO 15489-1* (ISO 2001, 1), which became

their standard for records management. This source provides an overview for how records management should be carried out in public and private organizations, regardless of how the records are being kept and what form they take. The *ISO 15489-1*, however, does not include archival preservation of records in its requirements, and so additional sources such as the ISO's report *ISO 14721* were used to augment this need (ISO 2012).

ISO 14721 is the ISO's reference model for an open archival information system, which permits a designated community to preserve records and information that is created and kept in a digital environment (ISO 2012). The authors used this standard to approach the analysis of cloud service agreements from an archival perspective, in which information may need to be preserved indefinitely. This is an important issue, especially in light of what clauses need to exist within cloud provider contracts to support this type of long-term preservation.

In addition to these standards, the authors of this article also consulted the Association of Records Managers and Administrators (ARMA) International's *Generally Accepted Recordkeeping Principles*® (ARMA International 2013), which create an outline of concepts that a recordkeeping program should meet to be effective. These principles share a good deal with the standards created by the ISO, specifically *ISO 15489-1*, but provide less description of an ideal records management environment.

Also included in our literature review was the European Commission's *Model Requirements for the Management of Electronic Records* (2009). These requirements were included because they provide guidelines specific to records in a digital environment, such as how a system should implement audit trails, access restrictions, destruction, backup, and so forth for digital records.

Cloud computing contract standards

The authors included in their literature review efforts to standardize cloud service agreements. One effort, in particular, is the recently published guide from the European Commission entitled the *Cloud Service Level Agreement Standardization Guidelines* (European Commission 2014). This guide identifies topics for concern relating to information being stored with cloud providers and makes recommendations of service level objectives for inclusion in service level agreements (15–36). Many of the service level objectives identified by this guide express similar areas for concern identified by both the ITrust Project 10 and this article.

An additional set of guidelines can be found in the policy produced by the Public Records Office of Victoria, Australia (2012, 7) on the use of cloud computing. This policy identifies the leaking of sensitive information and the loss of information as the primary risks of using the cloud. It requires that agencies of the Victorian government conduct risk assessments on the implementation of the cloud before engaging in it; on all legislation, standards, and policies; and on all agreements between agencies and cloud service providers to ensure the security of data, that the ownership of the data remains with the agency, and that the agency is established as the controller of the data (7–8).

Comparative analysis recordkeeping standards, legal requirements, and cloud contracts

Recordkeeping requirements are identified in legislation, regulations, policies, and standards. Depending upon the nature of the business or organization and the applicable law, the requirements for maintaining control over records created, received, and stored, along with the systems that facilitate and support them, will vary. Records, which serve as documentary evidence of legal transactions and support the critical operations of the organization, have a high value and must be managed properly throughout their lifecycle. In addition, records that contain personal or sensitive information must be identified when they are created or when they are received and managed (including disposition) in compliance with applicable privacy and freedom of information legislation and statutes. The adoption of cloud-computing services to facilitate and support organizational activities involving the creation, receipt, use, and storage of information and records must be approached with caution due to the potential risks associated with the cloud.

In brief, the records management and recordkeeping community has identified the following risks to business use of cloud-computing services: unauthorized access to information and records stored in the cloud; privacy breaches; loss of access to, and management of, information and records stored in the cloud; alteration of information and records stored in the cloud (impacting record authenticity and integrity); and the lack of transparency regarding account management, server locations, data destruction, and data recovery (Ferguson-Boucher and Convery 2011; Public Records Office Victoria 2012). Therefore, before implementing cloud-based services, agencies, organizations, and institutions should carefully review the contractual agreements of the cloud-service providers, assess the risks, and determine the degree to which they meet the organization's strategy with regard to records management and recordkeeping.

Unlike traditional approaches to outsourcing information technology services, in which the services were negotiated directly with the provider, cloud computing introduces IT services on a grand scale. Cloud computing utilizes online platforms for delivery, circulates customer data throughout server farms scattered across the globe, and relies on generic terms and conditions to regulate their contractual relationships with customers. As a result, customers may be unaware of where the service infrastructure is located and if there are sub-contractors involved. In addition, the distributed characteristic of cloud computing may present obstacles to enforcing breaches of contract, especially in cases that involve security and data privacy (Public Records Office Victoria 2012).

Formally, the terms and conditions may be contained in a single document hosted on the provider's website or in a set of documents containing the terms governing the relationship between the customer and the cloud service provider (Bradshaw, Millard, and Walden 2011, 192). In general, these documents may include a service level agreement (SLA), terms of service, acceptable use policy, and privacy policy. If a cloud service is provided for free, the SLA is not included (ibid.). For the purposes of this study, all available documents were consulted and are referred to by their title throughout the following analysis.

At present, a standardized SLA for cloud computing does not exist at an international level. However, at a regional level, we already mentioned the existence of the European cloud SLA standardization guidelines. In addition, an initiative by the ISO is underway, entitled *ISO / International Electrotechnical Committee New Proposal 19086: Information Technology—Distributed Application Platforms and Services—Cloud Computing—Service Level Agreement Framework and Terminology* (ISO 2013). In the absence of an international standard for cloud-computing SLAs, organizations and archival institutions considering adoption of cloud computing to facilitate and support records management and/or digital preservation must assess cloud service providers' terms and conditions before implementation, taking into account not only their records management and recordkeeping needs but also their legal duties.

Recordkeeping requirements and cloud provider terms and conditions

The following analysis utilizes the *ISO 15489-1: Information and Documentation – Records Management Part 1*, which was issued by the ISO in the fall of 2001, to identify recordkeeping requirements that should be taken into consideration when an organization assesses cloud-computing services for managing and storing their records. *ISO 15489-1* is technology neutral and includes sections on records system design and implementation (section 8) and records management processes and controls (section 9), which support the creation and maintenance of authentic, reliable, and useable records and protect the integrity of those records for as long as required (ISO 2001, 6). The comprehensive nature of the standard makes it suitable for addressing current records (that is, in use by the organization) and non-current records (that is, no longer in use but set aside for future reference).

ISO 15489–1 also identifies the characteristics of authoritative records, which are records that correctly reflect what was communicated, decided, or the action taken and support the needs of the business, and they can be used for accountability purposes (ISO 2001, 7). In addition to content, authoritative records should also contain, or be linked to, metadata that documents the structure of a record, the business context, and the links between documents that participate in the same activity (7). According to the ISO standard, the characteristics of authoritative records are authenticity (that is, an authentic record is what it purports to be), reliability (that is, a reliable record is one whose contents are accurate and the persons responsible for its creation have the authority to do so), integrity (that is, a record has integrity if it can be proven that it has remained complete and unaltered after being set aside), and usability (that is, a useable record is one that can be located, retrieved, presented, and interpreted). Throughout this article, reference will be made to these characteristics, as defined by *ISO 15489–1*.

In addition, *ISO 14721: Space Data and Information Transfer Systems—Open Archival Information System Reference Model*, which was issued by the ISO in 2012, is used in the following analysis to address the roles, responsibilities, and expectations of cloud providers and their clients as well as the specific

requirements related to the preservation environment (ISO 2012). *ISO 14721* provides a framework as well as the concepts needed by non-archival organizations (that is, cloud providers) to be effective participants in the preservation process.

An analysis of cloud-computing terms and conditions documents in the context of recordkeeping standards reveals several key issues for discussion: data ownership; availability, retrieval, and use; data retention and disposition; data storage and preservation; security; data location and data transfer; and end of service—contract termination. For the purposes of this project, the following cloud providers were identified in the ITrust's Project 10 and selected for further analysis: the Google Cloud Platform (United States), the Pathway Communications CloudPath (Canada), and the GreenQloud (Iceland).[1] The rationale for their selection is based on international representation, online access to terms and agreements, and limited resources. Every attempt has been made to consult the most current version of the terms and conditions documents available on the selected cloud providers' websites; however, it is common practice for terms and conditions to be updated. The cloud provider reserves the right to vary contract terms and amend its terms and conditions by posting an updated version to their website, noting that the continued use of the service by the customer is considered to demonstrate acceptance of the new terms and conditions (Bradshaw, Millard, and Walden 2011, 202).

The key issues will be addressed using an interdisciplinary approach, in which the specific recordkeeping requirement and legal framework will be identified and contrasted with selected sections from the cloud providers' terms and conditions documents. The degree to which the terms and conditions meet recordkeeping requirements will be discussed, along with the implications for recordkeeping activities within the organizations and archival institutions.

Data ownership

The authors of this article recognize that information in digital form accessed and stored in the cloud cannot be owned in the same manner as physical objects, at least not in the way as information transcribed onto a physical medium.[2] However, it can be controlled at a similar level by intellectual property rights, confidentiality or privacy, and contracts (Reed 2010, 1). For simplicity, this article will operate under the assumption that data ownership does not require a physical medium. The recordkeeping standards approach data ownership by stating that records may be physically stored with one organization, but the responsibility and management control may reside with either the creating organization or another appropriate authority. Records stored in electronic systems require arrangements that distinguish between the ownership of the records and the storage of the records (ISO 2001, s. 8.3.4).

However, data ownership in the cloud is a complex issue, not only because of the intangible nature of digital information but also because of the infrastructure of cloud computing itself, in which an individual or organization may entrust their information and records, along with others, to a cloud provider

and use the provider's platform and applications in the cloud to create further information and records, while the provider may create a great deal of information related to these operations for several purposes (for example, data processing, management, marketing, and so on).

It can be reasonably understood that information generated by the customer and stored in the cloud does not belong to the service provider (Reed 2010, 17) but, rather, that the provider is authorized to do specific operations with it to provide the service. Metadata generated by the service provider about the customer's information and operations in the cloud can raise more issues. These metadata can be important for the customer to further demonstrate that the integrity and the security of the data have been preserved. However, this information is owned by the service provider, who generated it for internal purposes—that is, to manage the cloud and ensure the use and quality of the service (Reed 2010, 9). Beyond the ownership issue, the contract terms and conditions should determine whether and how the customer has the right to access and use this metadata for recordkeeping purposes, during the contractual relationship but also at the end of the service (see the discussion later in this article).

Analysis of the terms and conditions documents for terms that declare ownership or responsibility for customer information and content reveals a lack of consistency in terminology and placement, which may lead to confusion when organizations are trying to evaluate several different service providers. Google is the most declarative and places the notice of being a data processor at the outset of their terms of service, whereas Pathway Communications makes a distinction between client data and information generated during the process of providing the cloud service. In doing so, Pathway Communications is imposing ownership of intellectual property via the terms and conditions. GreenQloud does not seek to assert intellectual property rights over customer content accessed and stored in their services. None of the three providers mention in their terms and conditions the right of the customer to access internal system metadata or the conditions to use metadata under license, for instance. As explained earlier, if the customer needs to access internal system metadata for recordkeeping purposes, the provider has the right to deny access to this metadata or to ask for additional fees to facilitate access and/or use.

Google Cloud Platform's terms of service includes section 1 on the provision of the services, in which Google is identified as "merely a data processor" (section 1.3). In doing so, Google identifies as being the service provider/data processor, who only acts upon instructions from the customer. The customer/data controller determines the purposes and means of processing personal information and customer content. This appears to be an oversimplified approach to the relationship between Google and its customers, especially as the cloud service provider often makes important decisions about the processes of managing and storing customer information and content. In section 3 on customer obligations, responsibility for customer data are assigned to the customer (section 3.1), specifically the management of intellectual property (section 3.6) and protecting the privacy and legal rights of end users (section 3.2). In direct reference to

the Digital Millennium Copyright Act, Google relies on copyright holders to manage their intellectual property online (section 3.6).[3]

Pathway Communications CloudPath's terms of service include section 8 on client data, in which responsibility for the storage, care, custody, and control of client data are assigned exclusively to the customer (section 8.3). Towards the end of the terms of service, there is section 20 on ownership of intellectual property, in which the cloud provider claims ownership of any intellectual property developed by Pathway during the performance of cloud services (section 20.1).

GreenQloud's end-user license agreement and terms of service includes section 5 on your responsibilities, in which the customer is assigned responsibility for the technical operation of customer content with the provided service (section 5.1a), managing customer content in a manner that complies with Icelandic laws on privacy and trade secrets (section 5.1b) and addressing any claims related to customer content (section 5.1c).

Availability, retrieval, and use

The importance of having information and records available to the organization to fulfil their immediate and future business needs is one of the driving forces behind the adoption of the cloud. Recordkeeping standards, such as ARMA International's *Generally Accepted Recordkeeping Principles* (2013), emphasize that records must be available for access and retrieval in a timely and efficient manner. Moreover, availability and retrieval is not only a question of efficiency but also a legal issue, as it is closely linked to statutory or constitutional rights to have access to certain data. To be more precise, availability is a fact and access is a right, but the latter cannot be satisfied without the former (Vermeys, Gauthier, and Mizrahi 2014, 86). Another issue is to control who can access the data and to protect the data's integrity and confidentiality, which is more a security issue that will be examined later in this article.

According to the data protection laws in Canada (see Privacy Act, the Personal Information Protection and Electronic Documents Act (PIPEDA), and similar provincial statutes),[4] in the United States, or in Europe, individuals have a right to access their own personal information held by an organization, whether public or private (except, in the latter case, for the US system, which provides for self-regulation by industry). Similarly, a lot of countries provide a general right of access to information held by public bodies and government organizations. In Canada, such a right is granted by the Access to Information Act and by equivalent provincial statutes.[5] Similar legislation has been adopted in the United States and in Europe. According to these laws, organizations must be able to provide access to the requested information within a period that may vary, depending on the legislation, from twenty to thirty days. This may seem quite reasonable from a technological point of view, but one has to consider the time needed to process the request from an administrative point of view, identify all of the requested documents, and evaluate whether some information should fall under one of the exemptions from access stated by law. Therefore, this administrative process cannot be retarded by technical difficulties to retrieve

and access the recorded information. In this respect, the availability of the stored data implies also the availability of the infrastructure, hardware, and software, which facilitates the retrieval and readability of the data (Vermeys, Gauthier, and Mizrahi 2014, 88). Of course, the fact that an organization is using a cloud-based service provided by a third party is not a reason to justify any delay in the processing of the request. In this case, if the organization is unable to provide access to the requested data, they remain liable and expose themselves to a complaint that could lead to specific sanctions.

Analysis of the terms and conditions documents for terms regarding availability, retrieval, and use of customer content reveals the use of SLA to present monthly uptime percentages (that is, total number of minutes in a month minus the number of minutes of downtime experienced in a month, divided by the total number of minutes in a month) and assures customers that cloud services are reliable and continuous. All three of the selected cloud service providers claim service availability of 99.99 percent. Service credits are supplied in the event of failure to meet performance standards; however, the list of exceptions is long and the onus is on the customer to determine which types of outages, downtime, unavailability, losses, delays, or problems actually constitute a failure and qualify for service credit.

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

Data retention and disposition

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

In some cases, disposition actions may require transfer of the records from one electronic system to another. The transfer should not alter the authenticity, reliability, integrity, or usability of the records. Authorized records destruction must be performed in a manner that preserves the confidentiality of the information. The process of record destruction should include all copies throughout the system and related metadata (ISO 2001, section 9.9). This can raise difficulties for the metadata generated, which is owned by the service provider in relation to the customer's data and operations in the cloud. Having ownership of such metadata (see discussion earlier on data ownership), the provider could refuse to destroy his own metadata if they are still useful for internal systems management purposes (for example, statistics, service improvement, and so on).

Analysis of the selected cloud providers' terms and conditions reveal an absence of terms that address data retention or deletion according to customer-stipulated schedules or recordkeeping requirements. Google Cloud Platform's data processing and security terms include section 5 on data correction, blocking, exporting and deletion, in which Google provides the customer with the ability to delete customer data in accordance with the functionality of the selected service. Terms in the terms and conditions assert that once the customer deletes their data and it is no longer recoverable by the customer, Google will delete or render permanently inaccessible the customer-deleted data within a maximum period of 180 days. In the case of data whose destruction is required by law under a specific schedule, the legal schedule could be overruled by up to six months. The customer would remain liable for such an infringement, as it is his legal duty to use procedures or services that ensure the destruction of the data at the right time. In the context of organizations that are required by law to delete certain types of records, more information about how customer data are rendered permanently inaccessible is required. In addition, the terms in their terms and conditions do not clarify if "inaccessible" data would be available to law enforcement through an e-discovery request.

Data storage and preservation

The manner in which records are stored after they are no longer in active use by the organization impacts the quality of the records and their capacity to be used for accountability purposes. In addition, evidence law directly or indirectly imposes certain precautions on the processing of the data to ensure a strong evidentiary value of the information brought before the court. This is the case in civil law jurisdictions (such as Quebec, France, or Belgium) where the integrity of the electronic record is a formal condition to recognize it as the legal equivalent of a paper record—that is, as "writing" within the hierarchy of the means of evidence. This integrity must be preserved throughout the lifecycle of the record.

Determining what actions are required by a system that stores records for the long term and provides preservation of digital information is challenging for organizations, especially if cloud providers are not transparent about the infrastructure and processes involved in providing cloud-based storage. The

task of maintaining information and records throughout changing technologies, new data formats, and evolving requirements for use requires knowledge of, and adherence to, recordkeeping standards aimed at digital preservation.

Recordkeeping standards state that systems selected by an organization for storing electronic records should ensure that the records held within the system remain accessible, authentic, reliable, and useable throughout any changes made to the system. If the systems provider implements changes, then audit trails and process metadata should be made available to the organization (ISO 2001, section 9.6). Planned migration and/or emulation of hardware, software, and/or operating systems by the electronic records system provider should not impact the authenticity, reliability, and usability of the records held within the system (section 8.3.5).

Analysis of the selected cloud providers' terms and conditions reveal terms that state that the customer is responsible for backing up the application, project, and customer data (Google 2014). In general, activities aimed at storing data and records for any length of time are referred to by cloud providers as backup procedures. The actions to preserve or the activity of preservation are absent from all terms and conditions documents.

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

GreenQloud's end-user license agreement and terms of service include section 10 on other security and backup, in which the customer is deemed responsible for maintaining appropriate backup of customer content. The terms include a reference to the customer's responsibility to protect their content by performing "routine archiving."

Security

Security is a control measure implemented throughout the electronic records system that prevents unauthorized access, destruction, alteration, or removal of records. Among the security measures to be taken, the protection of the con-

fidentiality of the data through access control is of crucial importance. Access to records stored in electronic systems should be managed through controls on access to ensure the integrity of the records and protect against unauthorized access, use, alteration, or destruction. Any change in the format of records transferred to the system and/or delivered to the user should be specified. The electronic system should be capable of producing audit trails and/or access logs to demonstrate that records are being protected from unauthorized access, use, alteration, or destruction (ISO 2001, section 8.3.6). The electronic system should capture and maintain metadata associated with the access, retrieval, and use of records within the electronic system. This includes metadata that is embedded or linked to records as well as metadata generated by the electronic system during processes associated with the management of records (section 8.3.2). In the case of a system malfunction or security breach, the cloud service provider should notify the client organization immediately and demonstrate the integrity of the system by providing access to tracking that reveals the movement and uses of records within the record system (section 8.2.3 and section 9.8.1).

From a legal perspective, such security measures are requested under data protection legislation. Sectorial regulations at a provincial, national, or international level must also be considered—for instance, those related to the financial markets (such as the Sarbanes-Oxley Act or the Basel Accords).[6] As mentioned earlier in the discussion on data preservation), the evidentiary value of the record will depend on the actions taken on the data throughout its entire lifecycle to preserve its integrity and authenticity, which includes security measures. More specifically, the duty to ensure the confidentiality of the data is a very common legal requirement that can be found in hundreds of different statutes and regulations (Vermeys, Gauthier, and Mizrahi 2014, 95 n401). In the following considerations, the authors mainly focus on security requirements with regard to personal data.

According to the principles set out in the Model Code for the Protection of Personal Information, included in Schedule 1 of PIPEDA, "an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party" (Principle 4.1.3). Such a principle can be found in most regulations to ensure the protection of personal data. The fact that the data have been transferred to a third party processor does not transfer the accountability of the organization. In such a situation, it is interesting to note that the contract is considered to be a key element to ensure security (Office of the Privacy Commissioner of Canada 2009, 9). Therefore, organizations considering the use of cloud-based services should pay special attention to the service provider's contract terms related to security and check if they explain how the security of the data is ensured through technical, physical, and organizational measures.

Analysis of the cloud providers' terms and conditions reveal different degrees of addressing security issues. Of the three selected cloud providers, Google is the only one that has a separate document entitled *Data Processing and Security Terms*, which is made available through a hyperlink buried deeply in section 15 of Google's terms of service. In this document, security terms are discussed at length, pertaining to both the physical infrastructure providing the services and customer content and account information (that is, personal data). The degree to which cloud providers will deliver security measures to customers appears to be reliant on the types of services being offered (for example, managed or non-managed) and whether or not the customer pays additional fees. Moreover, concerning controls on access and use of customer data, the selected cloud provider terms and conditions focus on assigning responsibility to the customer for managing access restrictions to their account and their content.

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

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

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

GreenQloud's end-user license agreement and terms of service include section 10 on other security and backup, in which the provider assigns responsibility for maintaining appropriate security protection of customer content to the customer. In section 2 on the customer's account and section 3 on acceptable conduct, it is mentioned that access to GreenQloud's services through a customer account is the responsibility of the customer, regardless of whether the activities are undertaken by the account holder or their employees. There is no mention of audit trails or access logs.

Data location and cross-border data flows

In cloud computing, the processing and storage services can be provided on-demand by using several the cloud provider's resources throughout the globe. As a result, legal concerns regarding cloud computing focus on the issue that the customer's data may be stored or processed in different locations and unknown jurisdictions (Bradshaw, Millard, and Walden 2011, 206). From a legal perspective, the main issue raised by the location of data is the storage of data outside the customer's jurisdiction. This can be a concern with regard not only to data protection laws but also to foreign laws that allow investigation agencies access to any data stored in a provider's jurisdiction. The most famous example is the US Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, also known as the Patriot Act.[7] Nevertheless, this major concern is often based on wrongful assumptions as to the application of such laws and needs to be examined in more detail.

First of all, contrary to a common misunderstanding, in Canada neither the Privacy Act nor PIPEDA prohibit the use of cloud-based services by public or private bodies, even if it implies a transfer of data outside the country. Provincial laws themselves do not restrain cross-border data flows, except for British Columbia, Nova Scotia, and Quebec (Klein 2008, 4 and 14; Vermeys, Gauthier, and Mizrahi 2014, 45, 112):

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

One common misunderstanding seems to be that only data stored in the United States are subject to the Patriot Act. In fact, according to this act, the US government has widespread powers to access data not only stored on servers located within the United States but also stored anywhere with a cloud-service provider that is registered in the United States or that conduct continuous and systematic business in the United States (Van Hoboken, Anrbak, and Van Eijk 2012, 36; Vermeys, Gauthier, and Mizrahi 2014, 49). In addition, as already mentioned, the US Patriot Act is certainly not a unique piece of legislation, as similar laws have been adopted by other governments, including Canada. Therefore, wherever the data are stored, whether or not in the cloud, organizations may be subject to similar types of orders to disclose information to governmental authorities (Office of the Privacy Commissioner of Canada 2005; Vermeys, Gauthier, and Mizrahi 2014, 49). One must also mention the fact that according to the Patriot Act, "a company subject to a section 215 order cannot reveal that the FBI has sought or obtained information from it" (Office of the Privacy Commissioner of Canada 2005). Nevertheless, an appropriate level of transparency can be reached if the service provider mentions in the contract that the data stored in the cloud may be subject to such disclosure orders. In addition, if an organization chooses to store personal data in the cloud of a service provider, it should inform individuals "that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction" (Office of the Privacy Commissioner of Canada 2009, 8 and 9).

However, even if the law does not prohibit the transfer of personal data outside Canada, organizations should assess the risks of jeopardizing the integrity, security, and confidentiality of personal information entrusted to third-party service providers, wherever they are located (Office of the Privacy Commissioner of Canada 2009, 7 and 9). It has also been noted that certain countries, provinces, or regions restrict the possibilities to transfer certain data outside their jurisdiction. In Canada, British Columbia and Nova Scotia require public bodies to ensure that personal information in their custody or under their control is stored and accessed only in Canada, which would prohibit the use of cloud-computing servers based outside the country. Nevertheless, without entering into details, these restrictions provide for several exceptions and do not apply to private bodies (Klein 2008, 11; Vermeys, Gauthier, and Mizrahi 2014, 51). In Quebec, restrictions are imposed for the storage of personal data outside the province. In short, public and private bodies must ensure that the personal data will receive

an equivalent level of protection under local privacy laws than under Quebec privacy laws. While it has been recognized that such an equivalent protection is offered by other provincial privacy laws and by federal laws in Canada, as well as by European laws, some doubts might be raised for the storing of personal data in the United States (Vermeys, Gauthier, and Mizrahi 2014, 117; compare Klein 2008, 11). This issue can also lead to difficulties for a Canadian provider having servers located in the United States or for servers located in Quebec under the control of a foreign provider. However, considering the practical difficulties raised by such a restrictive approach, Nicolas Vermeys, Julie Gauthier, and Sarit Mizrahi (2014, 129) suggest that it could be possible to abide by the spirit of the act by using encryption technologies to protect data before storing them in the cloud, wherever the servers might be located (see also Canellos 2013).

Finally, it is well known that the European Union has also adopted a restrictive legal framework with regard to the transfer of personal data outside Europe, requiring that the privacy laws of the country of destination offers the same level of protection as the EC Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Date and on the Free Movement of Such Data.[8] In this context, the European Commission has officially considered Canada as providing an adequate level of protection for personal data transferred from the European Union to recipients subject to PIPEDA.[9] In the United States, companies may comply on a voluntary basis to the Safe Harbor international privacy principles, a program settled by the US Department of Commerce in consultation with the European Commission and officially recognized as offering an adequate level of protection.[10]

In addition to these issues, the location of data might also be a criterion (among others), according to the rules of conflict of law, in determining the law that applies in the case of litigation if the parties have not chosen the law governing the contract (Goh 2014, 59). However, most cloud providers include terms that state the choice of forum for settling disputes between the provider and customer. In general, cloud providers select a jurisdiction compatible with their own legal system (for example, Pathway Communications is based in Ontario, Canada).

Recordkeeping standards do not address jurisdiction and limit their discussion to location. The electronic records system should be able to track the location of records as they move throughout the system (ISO 2001, section 9.8.3). Google Cloud Platform's terms of service include section 1 on the provision of the services, in which the cloud provider asserts the right to transfer, process, and store "an application and customer data in the United States or any other country in which Google or its agents maintain facilities" (section 1.3 and section 8.1). Google also mentions the fact that it is, and will remain, enrolled in the Safe Harbor program and will adopt a solution that achieves compliance with the terms of EC Directive 95/46 (section 1.5). The terms of service expressly state that the customer has the obligation to protect the privacy and legal rights of its end users under all applicable laws, which includes the communication of

a privacy notice, the obtaining of any required consent and the obligation to inform end users that the data will be processed by Google (section 3.2). The terms also stipulate that notwithstanding any non-disclosure agreement, Google will disclose confidential information to the extent required by the applicable legal process and under certain conditions (section 7).

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

Pathway Communications CloudPath's terms of service include section 28 on governing law, in which the provider states that the agreement is governed by the laws of the province of Ontario and that all disputes arising from cloud-based services will be addressed in that specific jurisdiction (section 28.1). GreenQloud's end-user license agreement and terms of service include section 5 on the customer's responsibilities, in which compliance with Icelandic law is required.

End of service: contract termination

In the event that the relationship with a cloud provider ends, the organization needs assurance that it can gain access to its information and records and that any data it leaves behind in the third-party system will be deleted by the cloud provider (Bradshaw, Millard, and Walden 2011, 203). There are several reasons why the services may be terminated, some of which relate to actions taken by the cloud provider or the customer or simply to the scheduled end of the contract. It is important that organizations are aware of contract termination procedures before adopting cloud services. An additional consideration is whether the provider is offering a paid service or a free one (196). Contracts for paid services address the duration of the service and the necessary steps to terminate the contract, whereas free services do not have fixed durations and may reserve the right to close inactive accounts.

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

Analysis of the selected cloud provider terms and conditions reveal two related, but different, activities: suspension of services and termination of services. Suspensions are typically in response to customer violations of the cloud service and require investigation by the cloud provider to determine restoration of the service and access to customer content or deletion of the account and customer content. Termination of services may be the final result of a suspension, the result of account inactivity, or the response to end of contract term.

Google Cloud Platform's terms of service include section 8 on term and termination, in which the cloud provider presents three types of termination: termination for breach (section 8.2), termination for inactivity (section 8.3), and termination for convenience (section 8.4). The effects of termination include terms that require the customer to delete the software, any application, instance, project, and customer data and that, upon request, each party will return or destroy confidential information of the other party (section 8.5). Google reserves the right to terminate services in the event of account inactivity exceeding 180 days (section 8.3).

Pathway Communications CloudPath's terms of service state in section 8 on client data that the customer will not have access to their data during a suspension or following termination (section 8.1). In addition, unless written modification is agreed upon, the cloud provider is free to delete client data from the system within seven days of termination of the account (section 8.4). Later in section 14 on service suspension or termination, the cloud provider includes several reasons for which the cloud provider can suspend or terminate services without liability, including unauthorized access by a third party (section 14.1.4) and overdue payment (section 14.1.6). The cloud provider will give "reasonable advance notice" of suspension of service. However, in the event of termination, the cloud provider is not obligated to refund payment and may prevent customers from accessing their data (section 14.2). In the case of a breach of contract, notice of account termination will be sent to the customer (section 16).

GreenQloud's end-user license agreement and terms of service include section 6 on suspension and termination, in which violations of the agreement will result in suspension or termination of the customer's account. During investigation of the suspected violation, all accounts are suspended. The cloud provider will not refund the customer for suspending or terminating accounts that are a result of violations of the agreement. GreenQloud states that it will try to notify the customer before suspension or termination. In the event of account suspension without cause, the cloud provider will provide fourteen days advanced notice. In section 7 on effect of termination, the customer is responsible for all fees and charges for in-process tasks that were completed by the cloud provider after the date of termination. Retrieval of customer data following termination is only available to clients that have paid for post-termination use of the provider's services.

Findings and discussion

Based on a thorough analysis of selected cloud providers' terms and agreements, the findings reveal that some boilerplate contracts, without additional fee-based services, are ineffective at meeting the recordkeeping needs of organizations and institutions operating within specific legal requirements. While some of the agreements do touch on the needs of records management and preservation, these sections of the agreements clearly aim, unsurprisingly, to protect the service provider rather than the client and its records needs. This is likely due to the reality that, because boilerplate agreements can be easily entered into by anyone, they have the potential to expose the service provider to a large amount of risk, which is further complicated by the fact that many of the companies offer similar terms, but the terms differ in their implementation. It is particularly true in the case of the uptime percentage terms of SLAs, which differ in how uptime is measured and how recompense is offered. It is also true with the terms on copyright and ownership, which may guarantee that the clients own their own data, but not the data created by the service provider in provisioning the service. This would likely mean that metadata assigned to records during their storage and use within the service would be unavailable, making proper audits and preservation extremely difficult.

Thus, records managers and archivists need to identify and establish the relevant regulatory and legal framework, in which the agency, organization, and/or institution operates within before adoption of cloud-based services. Areas such as public records requirements, freedom of information, and protection of privacy (POP) requirements, accountability requirements, security requirements, data location requirements or restrictions to cross-borders data flows, evidentiary requirements, and intellectual and copyright protection necessitate degrees of compliance and should be considered as part of the organization's recordkeeping strategy (Public Records Office Victoria 2013, 6). Private organizations, which do not handle public records are not subject to as rigorous a regulatory environment, except for POP; however, records managers and archivists still need to base their decisions on the availability of service required, the ability to execute records scheduling and disposition, the assurance of record reliability and authenticity, data privacy, long-term access, and system security. In any case, the provisions related to the end of the contract should be carefully examined to ensure a complete restitution of the data in a format that preserves their authenticity, with all of the associated metadata that ensure their traceability as well as the warranty that all of the customer's data are permanently and immediately destroyed after such a restitution.

However, it is possible that within the context of cloud services, some needs of records management may not be possible given the nature of the cloud. The purported benefits of cloud technology in sharing hardware to decrease costs, for example, cause extreme difficulties in ensuring that information has been irrecoverably destroyed when necessary. This is because the infrastructure that this information is stored on likely contains information from other clients or even information from the same client that is still needed, making degaussing

(that is, eliminating a magnetic field), physical destruction, or even wiping impossible. Another example of a difficulty that may emerge is the difference in where data may be stored permanently at rest, as Google refers to it (section 8.2). While the service provider may be able to guarantee that the client's data will be stored in a particular jurisdiction, it may be difficult to ensure that the data will not pass through jurisdictions that the client may be unaware of or that are unwanted by the client. It is conceivable that this data may be compromised or backed up during the transfer process, as the service providers do not specify what the transfer process to a state of permanent at rest may be or how long it may take.

Recommendations and further research

Any effort to aid records managers and archivists in entering into agreements with cloud-service providers should attempt to account for the needs of record-keeping systems as described by recordkeeping standards. In addition, it is important to recall that an organization that decides to opt for a cloud-based solution with a service provider must still fulfil its legal duties and remains accountable for the compliance with the requirements imposed by law. In this respect, specific issues that need to be addressed in cloud provider contracts are listed in the following checklist.

1. *Data ownership*
- Who owns the data stored, transmitted, or created in the cloud by the customer (that is, you)? Does the service provider have the right to use them and, if so, to what extent?
- Who owns the metadata generated by the system during procedures of upload, management, download, and migration? Do you have the right to access them for recordkeeping or legal purposes during the contractual relationship and at the end of the contract (see also section 7 on end of service)?

2. *Availability, retrieval, and use*
- Are SLA using precise indicators and providing clear information about the availability of the service?
- Does the degree of availability of the data fit with your business needs and allow you to comply with the freedom of information legislation (if you are a public body), the right of a person to access her own personal data, and the right of authorities to legally access your data for investigation, control, or judicial purposes?

3. *Data retention and disposition*
- Are your data (and all their copies) destroyed in compliance with your data retention and disposition schedules? If so, are they immediately and permanently destroyed in a manner that prevents their reconstruction, according to a secure destruction policy ensuring confidentiality of the data until their complete deletion?

- What is the nature and content of the associated metadata generated by the provider? Considering their nature and content, do they need to be destroyed at the same time and in the same manner as your data to comply with your internal or legal destruction policies? If yes, will the service provider proceed to such destruction?
- Does the system provide and give you access to audit trails of the destruction process? Will you receive an attestation, report, or statement of deletion from the provider, if requested by your internal or legal destruction policies?

4. *Data storage and preservation*
- Who is responsible for creating backups of customer data and recovering deleted or corrupted data?
- Are records migrated or emulated in a way that preserves their authenticity, reliability, integrity, and usability? Does the system provide and give you access to audit trails concerning the migration/emulation process?
- How will the service evolve? Will you be notified of any evolution of the service that could impede the authenticity of your data?

5. *Security, confidentiality, and privacy*
- Does the system prevent unauthorized access, use, alteration, or destruction of the data through technical, physical, and organizational measures? Does the system provide and give you access to audit trails, metadata, and/or access logs to demonstrate this?
- Will you be notified in the case of security breach or system malfunction?
- Does, or will, the service provider use the services of a subcontractor? Does the service provider provide information about the identity of the subcontractor and its tasks?
- What is the confidentiality policy of the service provider in regard to its employees, partners, and subcontractors?
- Is there a special confidentiality or security policy for sensitive, confidential, personal, or other special kinds of data?
- Is the service provider accredited and/or is he audited on a systematic, regular, and independent basis by a third-party to demonstrate that he complies with his security, confidentiality, and privacy policies? Is such a certification or audit process documented and do you have access to information such as the certifying or audit body and the expiration date of the certification?

6. *Data location and cross-border data flows*
- Where is the location of the data (and their copies) while they are stored in cloud-based services? Do they comply with the location requirements that might be imposed on your organization's data by law, especially by applicable privacy law? If not, are you considering the use of encryption technologies before storing the data in the cloud?
- Will you be notified if the data location is moved outside your jurisdiction?

- Does the contract mention that the data stored in the cloud may be subject to disclosure orders by national or foreign security authorities? Will the provider inform you and ask for your consent before disclosure (if such information or consent is allowed by law)?
- What is the legal jurisdiction in which the agreement is enforced and how dispute settlement will be resolved?

7. *End of service: contract termination*
- What is the duration of the contract? In what circumstances and how can it be terminated? Will there be any prior notification before the termination of the contract?
- At the end of the contract, whatever the reason, do you have the warranty that your data will be restored in a usable and inter-operable format? What is the time, procedure, and cost of such a restitution? Does the provider provide assistance for the restitution?
- At the end of the contract, will you have the right to access the associated metadata generated by the system for recordkeeping and legal purposes, notably to demonstrate that the confidentiality, integrity, authenticity, and reliability of your data have not been altered during their storage in the cloud?
- At the end of the contract and after complete acknowledgement of the restitution of your data, will your data and associated metadata be immediately and permanently destroyed in a manner that prevents their reconstruction (see also section 3 on data retention and disposition)?

In this study, the authors analysed the available cloud providers' terms and agreements. In doing so, the authors did not enter into contract negotiations with individual cloud providers, which limits the findings of this study to what is available online, which typically include services deployed in public clouds. The recommendations provided in this article will assist records managers and archivists in assessing existing cloud provider contracts and identifying gaps, but they can also be used to customize a contract and supplement existing fee-based services.

At the same time, it should be acknowledged that adherence to a checklist may not completely ensure that the client of a cloud service is entering into an agreement that places them in full compliance with recordkeeping and legal needs, obligations, and requirements. As can be seen in the agreements looked at in section 3 of this article, service providers may offer terms related to a recordkeeping need but may differ in how that need is addressed and which party is protected most by the language used. As a result, clients will still need to actively engage in the agreement process since the need for recordkeeping is addressed to some degree by the agreement, but it may not mean that it is addressed as much as it should be for the security and well-being of the organization. Organizations that utilize a checklist in creating or choosing cloud agreements to enter into should use it as a guide for navigating recordkeeping needs in the cloud, but they should still conduct risk assessments for the terms of the

agreement to determine whether the terms offered are agreeable (Public Records Office Victoria 2012, 7).

Despite this precaution, the authors of this article still believe that a checklist is more useful to records managers and archivists than a model contract. While it is true that records managers and archivists generally strive to meet the same standards, differing legal frameworks and cultures, organizational contexts, capabilities, and risk appetites make model contract terms difficult to produce. Based on the research presented in this article, the authors have devised a checklist of issues that should be addressed in any cloud service contract. This list should be considered only as a draft, as additional research will be necessary to test the checklist and identify gaps or weaknesses that may exist within it.

Notes

1. Google Cloud Platform: Data Processing and Security Terms, https://developers.google.com/cloud/terms; Pathway Communications CloudPath, http://cloudpath.pathcom.com; GreenQloud, https://www.greenqloud.com.
2. See *Oxford v Moss*, [1979] 68 Cr App R 183.
3. Digital Millennium Copyright Act, Pub L 105-304.
5. Privacy Act, RSC 1985, c P-21; Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
5. Access to Information Act, RSC 1985, c A-1.
6. Sarbanes-Oxley Act, Pub L 107-204, 116 Stat 745; Basel I (1988), Basel II (2004), and Basel III (2010) accords are a set of international recommendations for banking regulations issued by the Basel Committee on Banking Supervision.
7. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub L 107-56, 115 Stat 272.
8. EC Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Date and on the Free Movement of Such Data, [1995] OJ L281.
9. EC Decision 2002/2 pursuant to Directive 95/46/EC on the Adequate Protection of Personal Data Provided by the Canadian Personal Information Protection and Electronic Documents Act, [2002] OJ L002, 13.
10. EC Decision pursuant to Directive 95/46/EC on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, [2000] OJ L215, 7.

References

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

Baset, Salman. 2012. "Cloud SLAs." *Operating Systems Review* 46 (2): 57–66. http://dx.doi.org/10.1145/2331576.2331586.

Bradshaw, Simon, Christopher Millard, and Ian Walden. 2011. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." *International Journal of Law and Information Technology* 19 (3): 187–223. http://dx.doi.org/10.1093/ijlit/ear005.

Canellos, David. 2013. *Adopting the Cloud While Adhering to Domestic and Foreign Government Regulations*. http://www.safegov.org/2013/10/2/adopting-the-cloud-while-adhering-to-domestic-foreign-government-regulations.

European Commission. 2009. Model Requirements for the Management of Electronic Records. Brussels, Belgium.
——. 2014. Cloud Service Level Agreement Standardisation Guidelines. Brussels, Belgium.
Ferguson-Boucher, Kirsten, and Nicole Convery. 2011. ''Storing Information in the Cloud: A Research Project.'' *Journal of the Society of Archivists* 32 (2): 221–39. http://dx.doi.org/10.1080/00379816.2011.619693.
Goh, Elaine. 2014. ''Clear skies or cloudy forecast? Legal Challenges in the Management and Acquisition of Audiovisual Materials in the Cloud.'' *Records Management Journal* 24 (1): 56–73. http://dx.doi.org/10.1108/RMJ-01-2014-0001.
InterPARES 2 Project. 2015. *InterPARES 2 Dictionary*. http://interpares.org/ip2/display_file.cfm?doc=ip2_dictionary.pdf.
International Organization for Standardization (ISO). 2001. *ISO 15489-1*. http://www.wgarm.net/ccarm/docs-repository/doc/doc402817.PDF.
——. 2012. *ISO 14721*. http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284.
——. 2013. *ISO/IEC NP 19086*. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902.
Klein, Kris. 2008. *Applying Canadian Privacy Law to Transborder Flows of Personal Information from Canada to the United States: A Clarification*. Industry Canada. https://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00508.html.
Office of the Privacy Commissioner of Canada. 2005. *Bank's Notification to Customers Triggers PATRIOT Act Concerns*. PIPEDA Case Summary no. 2005–313. https://www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp.
——. 2009. *Processing Personal Data across Borders. Guidelines*. https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf.
Public Records Office Victoria. 2012. *Cloud Computing: Implications for Records Management, V.1.0*. State of Victoria, Australia. http://prov.vic.gov.au/wp-content/uploads/2012/04/Issues-Paper-Cloud-Computing.pdf.
——. 2013. *Cloud Computing Decision Making, V. 1.0*. State of Victoria, Australia. http://www.unimelb.edu.au/unisec/privacy/pdf/PROVCloud_Computing_Guideline_1.pdf.
Reed, Chris. 2010. ''Information 'Ownership' in the Cloud.'' Legal Studies Research Paper no 45. School of Law, Queen Mary University of London. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.
Van Hoboken, Joris, Axel Anrbak, and Nico Van Eijk. 2012. *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534.
Vermeys, Nicolas, Julie M. Gauthier, and Sarit Mizrahi. 2014. ''Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le Gouvernement du Québec.'' Working paper. Laboratoire de cyberjustice, Université de Montréal. http://www.cyberjustice.ca/wordpress/wp-content/uploads/2014/08/%C3%89tude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-Qu%C3%A9bec.pdf.