InterPARES Trust

Project Report

Title and code:		TR01: The Use of Cloud Services for Records Management Purposes in International Organizations
Document type:		Final Report
Status:		Final draft
Version:		5.0
Research domain:		TR-01 - Legal
Date submitted:		May 15, 2017
Last reviewed:		May 13, 2017
Author:		InterPARES Trust Project
Writer(s):		Eng Sengsavang, Elaine Goh
Research team:		Jens Boel, Elaine Goh, Eng Sengsavang, Luc Damer, Maggie Hunter, Emily Chicorli

Document Control

Version history			
Versions	Date	By	Version notes
1.0 – 2.0	April 9, 2017	Eng Sengsavang	Initial draft report
3.0 – 5.0	May 2017	Eng Sengsavang, Elaine Goh	Final draft for approval and comments at Transnational Team meeting: May 15, 2017 in Geneva

Table of Contents

Abstract

The study *The Use of Cloud Services for Records Management Purposes in International Organizations* was conducted under the auspices of the multi-national, interdisciplinary research project InterPARES Trust, from October 2013 to May 2017. The research investigates the perceived benefits and risks of cloud computing for recordkeeping purposes in international organizations, with a focus on the potential risks to inviolability and extraterritoriality when international organizations entrust their data and records to the cloud. To this end, an online survey conducted for the study captures a snapshot of cloud computing use in international organizations, identifying patterns in the drivers of, and barriers to, cloud computing adoption in international organizations. Interviews conducted for the study enrich the survey findings on the benefits and risks to cloud computing, including the potential impact on the jurisdictional immunities and inviolability of international organizations. The present Final Report for the study summarizes the background, research questions, aims, methodology, and findings of the research. The final products for the study include the Final Report, Interview Analysis, Survey Report, Literature Review and Annotated Bibliography, and a supplementary report on the topic of extraterritoriality.

Final Report: The Use of Cloud Services for Records Management Purposes in International Organizations

1. Research team

Lead Researcher:
Jens Boel, UNESCO

Project Researchers:
Elaine Goh, University of British Columbia
Eng Sengsavang, North Atlantic Treaty Organization

Contributors:
Darra Hofman, University of British Columbia
Elissa How, University of British Columbia

Graduate Research Assistants:
Emily Chicorli, University of British Columbia (August 2014 – August 2015)
Lucas Damer, University of British Columbia (November 2015–September 2016)
Maggie Hunter, University of British Columbia (February 2015 – June 2016)
Taryn Jones, University of British Columbia (October 2014 – December 2014)
Samuel Michelson, University of British Columbia (September – December 2015)

2. Background

The outsourcing of a great variety of services to external contractors, while not a new phenomenon, has become a salient feature of the machinery of contemporary organizations. Reports have indicated that the United Nations (UN) has increasingly outsourced security services, risk assessments and security training to private military and security companies (Jurriaans, 2012; Olson, 2013; Pingeot, 2012). However, concerns have been raised regarding the "great opacity" and lack of information about the contracts and companies hired by the UN (Pingeot, 2012). Clearly, the outsourcing of services and manpower raises issues of trust: whether the services of external operators can be trusted by organizations and their relevant stakeholders, and in turn, whether stakeholders can trust the organizations that depend on external providers for particular services.

In the realm of technology, a measure of the increasing ubiquity of outsourcing is exemplified by the popularization of cloud computing, a model for outsourcing various services associated with the management of data, records and various business functions to third-party services. The UN has actively encouraged both governments and businesses in middle- and low-income countries to leverage the benefits of cloud technology (United Nations, 2014). At the same time, a few UN agencies and other international organizations have either started or are considering deploying and using public cloud services. For example, the Office of Information Systems and Technology from the United Nations Development Programme (2014) report that they have moved 22,000 email accounts of staff containing 80 terabytes of information in the cloud. The UNDP has also launched a pilot project on the use of a file storage and file-sharing application.

Given the rise in the deployment of cloud services within all types of organizations, characterized by a geographically distributed and multi-layered outsourcing and service provider model, it is critical to begin considering the potential impact that such a model may have on the protection, integrity and security of organizational data and archives.

This is especially relevant given two principles linked to international organizations, inviolability and extraterritoriality, which are meant to protect their data, records and premises, among other assets and functions, from external access or interference. In the context of international organizations, both concepts derive from the system of privileges and immunities from which international organizations operate. This system consists of special rights and jurisdictional exemptions drawn up between international organizations and their member and host states (Jenks, 1961). Two types of privileges and immunities are jurisdictional immunities and the inviolability of premises and archives' (Abass, 2014, p. 191).

The inviolability of both premises and archives is clearly established in the constitutional and multilateral treaties and host agreements of most international organizations (Jenks, 2014, p. 46-55), including in the 1946 General Convention[1] of the United Nations (Article II, Sections 3 & 4), the 1951 "Ottawa Agreement"[2] of the North Atlantic Treaty Organization (Articles VI & VII), and the 2015 Consolidated Versions of the Treaty on the European Union[3] (Articles 1 & 2), to name a few examples. The purpose of inviolability is to preserve the independence (Díaz-González, 1991, p. 95, 99) and the privacy of international organizations and their member states (Jenks, 1961, p. 47).

The inviolability principle applied to the Specialized Agencies of the UN, for instance, states, "The premises of the specialized agencies shall be inviolable. The property and assets of the specialized agencies, wherever located and by whomsoever held, shall be immune from search, requisition, confiscation, expropriation and any other

[1] Full name: 1946 Convention on the Privileges and Immunities of the United Nations.

[2] Full name: Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff signed in Ottawa, 1951.

[3] Full name: Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union and the Charter of Fundamental Rights of the European Union, 2015.

form of interference, whether by executive, administrative, judicial or legislative action" (UN, 1949, Article III, Section 5). For archives, it states, "The archives of the specialized agencies, and in general all documents belonging to them or held by them, shall be inviolable, wherever located" (UN, 1949, Article III, Section 6).

Although the inviolability of archives is extended regardless of where the archives are located, there is however always the element of risk of inadequate controls and protection of the archives, particularly when physical custody of the archives is delegated outside the premises of a UN building and hosted in the cloud. Consequently, archives that are located in a physical building of the UN agency have the highest degree of enforceable protection.

"Extraterritoriality," on the other hand, is a term that can refer to various legal conventions. However, in the context of international organizations, extraterritoriality most often refers to the jurisdictional immunities applicable to the organization and to its assets. Extraterritoriality in this sense refers to the protection and immunity from external jurisdictions established and agreed on by international organizations and their member and host states. This is often referred to as "immunity from legal process" in the legal instruments and agreements of international organizations. For example, Article 5 of the Ottawa Treaty of NATO states, "The Organization, its property and assets, wheresoever located and by whomsoever held, shall enjoy immunity from every form of legal process" (1951). Extraterritoriality therefore operates within the framework of the immunities of international organizations in the form of jurisdictional immunities. In this sense, the principle of extraterritoriality is closely related to inviolability, but inviolability may be understood as a specific type of jurisdictional immunity or as an extension of jurisdictional immunities.

In light of the increasing ubiquity of cloud computing, coupled with the distinct status of international organizations, this study addresses the intersection between cloud computing technology and the recordkeeping practices and related immunities of international organizations.

3. Research Questions

1) What are the drivers for the deployment and use of cloud services by international organizations?
2) What are the barriers for the deployment and use of cloud services by international organizations?
3) What are the associated risks to extraterritoriality and inviolability of records and archives when international organizations delegate their records to the cloud?
4) How can risks be mitigated and benefits enhanced when/if international organizations decide to entrust their records to the cloud?

5) How can the outsourcing of records of international organizations to the cloud best be reconciled with the principles of extraterritoriality and inviolability?

4. Study Objectives

This study focuses on both the challenges and the opportunities that cloud computing presents to international organizations, including in the context of their distinct legal status, privileges and immunities. To this end, the study considers the factors that both drive the adoption of cloud computing, and those that deter the deployment of cloud computing, largely from the point of view of archivists, records managers, and information technology professionals working within international organizations. To address this, the study identifies the perceived risks and benefits of cloud computing for international organizations, and measures the current adoption and usage patterns of cloud computing in international organizations.

In considering cloud computing risks and benefits, a corresponding topic is the impact that cloud technology may have on the extraterritoriality and inviolability of international organizations. Thus the research also asks whether and how cloud computing complicates the potential risks to the data and records of international organizations entrusted to the cloud. In what ways could cloud computing affect the potential for unauthorized access or interference by external actors, the very circumstances against which both principles are established to mitigate?

The data from the study contributes to documenting and understanding the relatively early stages in the adoption and uses of cloud computing for recordkeeping purposes in international organizations, as well as enhancing our understanding of the complex risks and opportunities that arise for international organizations with the introduction and growth of cloud computing technology.

The study focuses on intergovernmental organizations, since they constitute the largest study sample, but findings may be applicable to a wide range of international organizations that are considering using, or are already using, cloud computing technology, including non-governmental organizations. However, the study excludes private international organizations such as multi-national corporations. The research is also relevant to international organizations that have established privileges and immunities in the form of inviolability and/or jurisdictional immunities.

5. Methodology

5.1 Data Collection Design and Sources

The study spans the period between October 2013 and May 2017. The main data sources collected for the study include the survey results, anonymized qualitative interview data, unpublished policy documents relating to cloud computing from our interviewees, as well as selected constitutional and legal agreements from some international organizations, most of which are publicly accessible. The former includes policies on records management and bring-your-own-devices, while the latter includes sources such as the 1946 UN General Convention and the Food and Agriculture Organization Headquarters Agreement with Italy. Because of concerns about confidentiality, and based on request from the interviewees in this study, we have avoided quoting from the policy documents.

The research team designed a mixed-methods approach to address the study objectives, an approach that is informed by pragmatism as a worldview. Pragmatism operates from the premise that "truth is what works at the time," and that there are "many approaches to collecting and analyzing data rather than subscribing to only one way" (Creswell, 2007, p. 23). Such an approach means that researchers who adopt pragmatism will employ multiple methods in their data collection. Mixed-methods research uses "multiple methods to generate and analyze different kinds of data in the same study" (Schwandt, 2007, p. 198). The mixed methods approach offered research participants the option to either participate in the survey or the interviews or both, and was the most practical approach to addressing the research questions. Additionally, the mixed methods design enabled the research team to triangulate from various data sources, increased the flexibility of data collection, and afforded multiple opportunities and avenues for research participation.

5.1.1 Data Collection

The main phases of complementary[4] data collection occurred between September 2014 and December 2015:

1. An **online survey** disseminated between September 2014 and December 2015, which resulted in a report based on 42 completed responses from archivists, records managers, information technology, legal and communications professionals working in international organizations.

2. **Interviews** which occurred in the period spanning March to December 2015, with 15 archivists, records managers and information technology professionals working in international organizations. The outcome of the interviews is a report that identifies the major themes anchored on research questions 1-4.

[4] Complementary data design refers to the elaboration and enhancement of findings from one method by using the other (Onwuegbuezie and Johnson, 282).

The survey and interviews are complementary: while the survey focuses on research questions 1-2 on the uses, drivers and barriers of cloud computing adoption in international organizations, the interviews provide more context to the statistical results. Further, the interviews hone in on research questions 3-4 regarding the risks posed to the extraterritoriality and inviolability of international organizations by cloud computing, a subject that research team members deemed better suited for qualitative research.

5.1.2 Supporting Research Activities

Supporting research activities conducted on an ongoing basis during the study period, which informed both the design and analysis of the survey and interviews, include the following:

3. A **literature review and annotated bibliography** conducted from October 2013 to September 2016, resulting in 131 articles reviewed and annotated under three main thematic headings (Cloud Computing, Archives and Custody, and Legal Challenges in the Cloud) and six sub-headings (International Organizations: Records Management and Archives; Risk Management; International Organizations: Legal Status, Privileges and Immunities; Extraterritoriality: Inviolability and Extraterritorial Jurisdiction; Data Localization and Privacy Legislation; and Cybercrime).

4. A **supplementary report on the extraterritoriality of international organizations** completed in April 2016 by Elissa How (MAS graduate) and Darra Hofman (PhD Student) at the University of British Columbia, both lawyers, who were recruited to support the project by investigating the term 'extraterritoriality.'

5.1 Challenges and Limitations

A main challenge of the study was the difficulty in recruiting research participants for both the online survey and interviews. Therefore, a limitation of the study is the **small sample size** for each data collection activity (42 survey responses and 15 interviews). However, although the number of participants for this study is relatively small, the workings of relatively large-sized organizations are reflected through their experiences. Moreover, some of these organizations have multiple field offices located in various organizations, widening the geographic scope of the study.

Although the study uses anonymized data, due to the distinct set-up and security and privacy concerns of international organizations, some research participants were required to seek clearance from their senior management and/or security authorities before participating in the study, which caused delays and sometimes deterred participation. In addition, some potential research participants declined to take part in the study, either because they felt that their organization does not intend to use cloud computing, or the organization is not at a satisfactory stage of maturity in terms of records management.

Other potential participants expressed uncertainty about the criteria for participation, believing that their organization should be using cloud computing, or should be at an advanced stage in its records management/archival program, in order to take part in either the survey or the interviews or both. Some participants felt that they were not well informed on the subject matter. For example, one interviewee revealed that she was embarrassed by her lack of knowledge on cloud computing; this uncertainty or discomfort with the topic could be another reason why the research team had difficulties recruiting participants.

A related recruitment challenge consisted of the types of professionals working in international organizations who would agree to participate. For both the survey and interviews, the research team originally sought to recruit a range of professionals from various fields, including archivists, records managers, information technology, legal, audit, and general business users (administrative or management staff). However, this proved to be difficult due to a lack of responses from those outside the archives, records management, and information technology fields. Therefore, the study research participants are limited mostly to **archives, records management, and information technology professionals**. Within this pool, archives and records management practitioners represent the largest percentage of research participants.

Additionally, due to a gap in time between the data collection and data analysis and reporting activities of the study, the research on cloud computing adoption and use represents **data from the years 2014 to 2015**. This should be kept in mind considering the fast pace of technological change in the realm of cloud computing. Since the period of the data collection, international organizations are continuing to consider and adopt cloud computing for various functions, and developments in both the recordkeeping practices of international organizations and in cloud computing technology and services contribute to an ever-evolving landscape. The research team looks forward to further studies in this arena.

6. Study Findings

The combined study and interview findings offer a view into the state of cloud computing adoption and the factors that inform decision-making and organizational practices from the perspective of archivists, records managers, and information technology staff. The online survey statistics largely address questions on the deployment and uses, and evaluation and implementation of cloud services within international organizations. This includes data on the perceived drivers of, and barriers to, cloud computing adoption; the types of cloud services used, the types of records and functions deployed to the cloud; and the negotiation of contracts and service-level agreements with cloud providers, among other topics.

The interviews highlight and expand on the findings of the survey. Along with information about the use of cloud services in participants' organizations, the interviews explore: interviewees' understandings of cloud computing; issues, concerns and policies related to cloud computing and the outsourcing of records to third parties; the extraterritoriality and inviolability of international organizations, including how each principle is applied within organizations and how they influence decisions to adopt or not adopt cloud computing; risks and benefits of cloud computing, including discussion of the survey findings on top five drivers and barriers; and service-level agreements with cloud service providers, including discussion of the survey findings on the role of each profession in drafting agreements.

Where applicable, the pronoun "her" or "she" will be used in the context of discussing the participants, but this does not in any way denote the gender of the specific participant.

6.1 Study Sample

6.1.1 Background of Participants

The survey results are based on a sample of 42 respondents, while the interview data is based on 15 participants. Overall, the study measures the perceptions and views of archives and records professionals, who constitute over half of the survey respondents and 80% of interviewees. Information technology professionals represent about a quarter of study participants overall. Other professions nominally represented via the survey include legal (1 respondent) and communications/public relations staff (3 respondents).

The majority of study participants are professionals with management responsibilities or professionals with no management responsibilities. However, a significant majority of the interviewees are senior managers within their units (40%), while only 7% of survey participants fall within the same category.

6.1.2 Background of International Organizations

Due to the type of international organizations in which survey and interview participants are employed, the study provides an insight especially into the workings of medium- to large-sized intergovernmental organizations, based mostly in Europe, with a smaller number based in North America (19% of survey respondents and only one interview participant). One organization in the study, represented by a single survey respondent, is headquartered elsewhere, in Africa. However, a majority of the organizations have missions and bases worldwide.

The study collects data largely from staff of medium- to large-sized intergovernmental organizations (between 1,000 to upwards of 30,000 staff members). About 38% of survey respondents and 67% of interviewees work in organizations employing between 1,000-4,999 people. Just over a quarter of survey respondents work in large organizations staffed by more than 5,000 people, compared to one-third of interviewees in the same category. However, while one-third of survey respondents work in organizations with fewer than 1,000 employees, no interviewees work for organizations employing less than 1,000 staff. Additionally, three quarters of survey respondents and all of the interviewees work for intergovernmental organizations.

6.1.3 Policies and Practices Relating to the Management of Records and Data within Organizations

Most organizations have policies governing the retention and disposal of records (88%), policies on data protection or information privacy (83%), and policies on public access to records (88%). A strikingly lower percentage of organizations from the study have policies on the outsourcing, transfer and processing of data to third parties (40%). On the other hand, three-quarters of respondents affirm that their organizations conduct training and awareness programs related to the management and preservation of records, and over half of respondents claim that their organizations conduct audits of how data is held, processed and stored (57%). Less than a quarter of respondents report that their organizations do not conduct a risk assessment of records or information assets, while a majority are uncertain whether or not this is the case (63%).

6.2 Deployment and Uses of Cloud Computing in International Organizations

The survey results indicate that a majority of international organizations are using cloud computing services, albeit on a limited (55%) or exceptional (10%) basis. The findings project that the deployment of cloud computing within international organizations will continue to increase, based on 64% of respondents who indicate that their organizations will be using cloud services in the next one to three years. About 42% of respondents who work in larger organizations with 5,000 or more employees are exploring the option of using cloud services. This suggests that larger-sized organizations with 5,000 or more employees take a cautious approach to the adoption of cloud services.

The cloud deployment model most used by most international organizations is private clouds (48%), followed by public clouds (33%), while only 6% and 5% of respondents report using community and hybrid clouds, respectively. These findings invite a number of hypotheses. While international organizations prefer to use private clouds, public clouds are also employed to a significant degree, possibly due to a combination of the ease with which public clouds can be deployed, and the ubiquity of the deployment model. For example, one interviewee reveals that some staff in her organization have downloaded Dropbox and Google Drive into their office computers, which pose a risk to information security. Another possible reason for the adoption of public clouds as revealed during the interviews is that some of the records have already been opened to the public domain, including historical archives. As such, there is less of a concern to restrict access to the records. Section 6.3 will elaborate on this issue with regard to the drivers of cloud computing. The low use of community and hybrid clouds in international organizations may signal barriers to their deployment, such as a lack of awareness regarding their benefits, and challenges in partnering with other organizations in the case of community clouds.

According to the survey, the top five business services deployed to the cloud include web-conferencing (50%), websites and social media (48%), file sharing (33%), data storage and backup (21%), email (19%), and the use of office software (19%). 17% of respondents reported the use of other business services, including human resources recruitment tools and the management of library data.

On the matter of the type of records and data deployed to the cloud, almost half of respondents indicate websites and social media, while a quarter of responses are in the 'other' category. These include personnel recruitment data, travel records, contract management systems, library and online information resources, and logistics. Close behind 'other' are email records deployed to the cloud (19%), followed by data hosted from intranet sites (17%), personnel records (14%), and financial records (7%). 19% of survey respondents claim that the question is not applicable to them.

6.3 Drivers of Cloud Computing Adoption

The survey results illustrate that cloud computing appeals to organizations because of factors related to the ease and economy afforded by the technology, both in terms of scalability and resources. From the survey, the top five perceived **drivers** for cloud computing are:

1. Improved scalability of information infrastructure (76%);
2. Enhanced availability (69%);
3. Cost savings in hardware and software (69%);
4. Ease of deployment in setting up and implementing a system (55%); and
5. Increased flexibility (55%).

The interviews confirm the survey findings on flexibility and scalability of cloud services as key drivers, along with cost savings to the organization. Cloud computing is seen to provide a flexible and easy solution that dispenses with the need for cumbersome storage solutions, and could save costs on IT staff. Cloud computing is also perceived by some interviewees to provide ready access to information systems for individuals working in a distributed working environment across various field offices, where there are multiple stakeholders and third parties. This is a particularly attractive selling point for large global organizations that have a wide network of satellite offices scattered across various continents.

An additional observation from the interviews is that cloud services promote ease of access to historical archives and to publicly disclosed records. Some interviewees illustrate that the level of risk to an organization and its data when using cloud computing can depend on the type of records deployed. Since public records represent a lower risk to data privacy and security, some organizations have started to experiment with using cloud computing by first deploying documents that have already been opened to the public. Again, this reaffirms survey findings that cloud computing is used for external communications and information-sharing, since the top business functions deployed to the cloud are web-conferencing, websites and social media, and file sharing, while the most frequently cited type of records and data deployed to cloud computing include websites and social media.

6.3 Barriers to Cloud Computing Adoption

While cloud computing offers organizations a variety of choices in terms of deployment and service models, and a virtualized infrastructure “for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources” (National Institute of Standards and Technology), the very nature of the dynamic and open architecture poses risks. A key insight from the interviews is that the most appealing attributes of cloud computing also constitute its greatest risks. For example, while interviewees acknowledge that cloud computing can help to integrate and streamline the development and delivery of IT infrastructure and services in satellite offices across various countries, there are also concerns about the ability to implement cloud computing in field offices from developing countries, where internet connections can be patchy, and where they do not have a good IT system.

Generally, on the question of risks and barriers to the adoption of cloud computing within international organizations, the survey and interview findings converge significantly, particularly when participants consider risks to the jurisdictional immunities and the inviolability of international organizations. Central issues revolve around the security and privacy of data and of organizations, unauthorized access to data, ownership and custody, external jurisdictional control, and gaps in policy and governance frameworks to address these issues. At base, all of these issues are about the loss of control that an organization exercises over its own data, a concern that emerges at the forefront of discussions within security- and privacy-conscious international organizations.

From the survey, the top five barriers are:

1. Lack of protection of personal data/data breaches (93%);
2. Concerns over ownership and custody of records (88%);
3. Concerns over IT security (86%);
4. Compromise the inviolability of records (81%); and
5. Concerns over the applicability of domestic laws on data stored and processed outside international organizations (74%) / Concerns over protection of intellectual property (74%) (tied).

More than half of the interview participants highlight a concern over the lack of protection of personal data or data breaches. Unauthorized access to data by third parties raises security concerns over the protection of organizational records, particularly those that contain sensitive and confidential information. The risk from third parties could emanate from governments, from cloud service providers, or from hostile agents such as hackers, whether state or non-state. Another security threat stems from internal units or individuals within the organization, as some staff may practice risky storage or management of records either without realizing it, or in some cases, deliberately. Because of the political nature of intergovernmental organizations, many organizational policies focus on ensuring that “information needs to reside on the territory of one of the allies,” as one interviewee describes it. However, in a cloud computing environment, many staff question the enforceability of such policies.

Some interviewees note threats to data protection and data privacy regulations particularly in the European Union, and concerns regarding the extraterritorial reach of the United States in particular. Although international organizations and their data are protected by inviolability and jurisdictional immunities, the jurisdictions of the locations in which data are stored or pass through, or the nationality of the cloud service provider itself, are perceived to pose risks to the privacy and autonomy of international organizations.

The issue of the ownership and custody of records in the cloud is a closely related concern. Some participants believe that records are not safe unless they are in the custody of the organization, whether in the form of physical records or digital records on a server. The issue is also raised in the context of discussions on the transfer of data across multiple data servers in a cloud computing architecture. Interviewees diverge on the question of whether hosting data off-site means that the organization is no longer protected by inviolability and jurisdictional immunities; some hold this view, while others believe that even if records are not physically in the custody of the organization, inviolability and extraterritoriality still apply. Participants assert, in particularly strong terms, the need to establish the organization's ownership over its own data.

The lack of policies governing the adoption and use of cloud computing also emerges as a significant barrier to cloud adoption, as current policy frameworks in organizations are outdated and do not address challenges in the management and preservation of records in the cloud. As a consequence, there is little consideration of records management issues in the selection and use of a cloud computing technology. Another reason for this may be that varied understandings of cloud computing from the interviews imply that there are times when a choice is made about a technology without taking into consideration the legal and records management implications.

6.2.2 Implementation of Cloud Computing and Negotiation of Contracts and Service Level Agreements

Both the survey and interview findings suggest that archivists and records managers face considerable challenges when it comes to being involved and informed, and gaining a seat at the table in the evaluation and decision-making processes for the adoption of cloud computing within organizations. The use and implementation of cloud computing is led largely by information technology units (76%), while only 10% of archives and records professionals claim to be leading the adoption of cloud computing. By contrast, a significant percentage of archives and records management professionals (29%) report that they are *not* involved in evaluating and implementing cloud services, while all respondents in the information technology field report being at least largely or partly involved in evaluating and implementing cloud services.

Meanwhile, interviewees underscore the decentralised approach in the choice of technology within organizations, where various units operate independently from one another and at times, may decide to deploy cloud services without necessarily consulting other departments or staff, such as archives and records professionals and legal personnel. Some business units, dissatisfied with the IT service within their organizations, may also decide to directly purchase their own software and IT systems from service providers.

The situation appears to be similar when organizations draft service-level agreements, as IT staff are significantly more involved than their archival and records management counterparts. A quarter of respondents indicate that their organization negotiates a service level agreement for cloud services, while an equal percentage of respondents claim that they do not know whether their organization negotiates a service-level agreement (29%), or that the question is not applicable to them, since their organization has not implemented cloud computing (29%). Nevertheless, a significantly higher percentage of information technology professionals are involved in drafting a service level agreement for their organization, as compared to records and archives professionals. 36% of information technology professionals claim to be largely involved in drafting a service level agreement, while only 4% of records and archives professionals claim to be largely involved. Almost half of IT professionals also report being partly involved in drafting a service level agreement, while only 13% of archives and records professionals claim to be partly involved.

7. Recommendations

The study findings act as signposts both for the gaps that need to be filled and the possible steps that could be taken in order to address the legal, organizational, security, privacy, human, and technological issues that arise along with the technology. Below we outline recommendations based on the study findings, some taken directly from study participants and others synthesized by research team members based on the research findings.

7.1 Address organizational service and protection requirements through comprehensive contracts with cloud providers, in consultation with legal, archives and records, and IT staff

Organizations should address cloud computing service requirements and organizational security and privacy conditions through detailed and comprehensive contracts with cloud providers. A practical tool that organizations can use is the InterPARES Trust document "Contract Terms with Cloud Service Providers" (McClelland and Hurley, 2016). The authors provide a matrix of specific categories of contract terms that should be addressed with the cloud provider. Contract terms should be developed in consultation with the organization's legal, archives and records management, and IT professionals. Important contract terms to include are outlined below.

- Specify that ownership and copyright of data remain with the organization.
- Specify the territory or territories where data can be stored, processed and transmitted.
- Specify whether the data in the custody of a particular cloud provider may be subject to any domestic regulations, including whether the data could be subject to access or control by domestic governments (that is, by the government that regulates the data service provider).
- Specify domestic or regional data protection and privacy regulations and standards that apply to the data belonging to the organization.
- International organizations should include a clause protecting the inviolability and jurisdictional immunities already applicable to the organization.

- Guarantee that the organization will have long-term, continuous access to information throughout the lifecycle of records, and also in relation to retention and disposition schedules.
- Broadly specify technical and organizational measures governing the processing of data.
- Specify that there must be adequate security and organizational controls against loss and unauthorized access to records and data.
- Ensure full data deletion (including copies).
- Ensure that records cannot be reconstituted or reconstructed when a request is made to destroy records in accordance with the retention and disposition schedule.
- Ensure that the organization has access to the audit logs of its own data.
- Since cloud service providers also outsource part of their services to third parties, it is recommended that contracts contain provisions for providers to inform organizations of any changes in their third-party services, and that organizations have the right the terminate the contract if there is a change in their service chain.
- There should be adequate provisions for an exit clause, specifying the circumstances when organizations can terminate the contract, such as if cloud providers fail to provide continuous delivery of services within a standard period of time. The exit clause should also include steps that enable organizations to retrieve and migrate their data within a specified time frame.

7.2 Take a proactive and multidisciplinary approach to implementing cloud computing and developing cloud contracts

As demonstrated by the study findings, it is becoming increasingly critical for organizations to mobilize an interdisciplinary approach to the management of a technology that, by its design, operates on the boundaries between technological, legal, security, and records management concerns. Therefore, organizations should develop greater collaboration and knowledge-sharing between various types of professionals, including archives and records, IT, legal, security and senior management staff. International organizations should thus consider developing cross-disciplinary joint working groups to decide on the choice of technology and to develop and review information and records management policies. This could help to discourage silos, and to foster a more coherent, broader approach to evaluation and decision-making, taking into account different types of professional expertise to leverage the benefits and mitigate the risks of cloud computing throughout the entire life of records.

7.3 Develop organizational policies addressing security and privacy in cloud computing systems and records management concerns, and ensure policy requirements are met through audit and inspection controls

Organizations should review and update their policies to take into account security and privacy issues in cloud computing systems, as well as to address issues relating to the outsourcing, processing and transfer of data and records to third parties. Organizational policies should consider prevailing standards on records management and information security (for example, *ISO 15489-1:2016 Information and documentation – Records Management*), as well as international cloud computing standards and tools. This should include the suite of cloud computing standards including *ISO/IEC 19086-1:2016 Cloud computing - Service level agreement (SLA) framework -- Part 1* and *ISO/IEC 17789:2014 Cloud computing -- Reference architecture*. Organizational stakeholders can follow and consider a number of other ISO/IEC standards on cloud computing that are currently under development.[5] The policy framework should address both records management and legal issues on maintaining custody and control of records in the cloud.

7.4 Develop a risk register to analyze the risks involved in outsourcing records to the cloud

It may be useful for international organizations to develop a risk register that documents information management risks identified in their organizations, including the perceived levels of risk, the impact, and how such risks could be managed and mitigated. Multiple stakeholders should be involved in the development of the risk register. A proactive approach to the establishment of controls with regard to the outsourcing, processing, and storage of data and records would enable international organizations to improve their policy frameworks and business practices, and could better inform the decision-making process. External factors, manifested by technological changes and how they may influence the records creation process, combined with internal factors such as internal operations, organizational culture and the evolving business practices of international organizations, combine to create various risk events that would be helpful to identify whenever a new technology is selected. The identification of risk events with regard to the outsourcing of records to cloud service providers would enable organizations to assess how such risks could help organizations to meet or prevent the fulfillment of their missions and functions. International organizations should recognize that the outsourcing of records and data does not denote the transfer of risks to an external party, because ultimately, international organizations are accountable to their stakeholders and to their mandates, as specified in their constitutional and multilateral agreements.

[5] See the ISO Standards Catalogue on "Cloud Computing and Distributed Platforms": https://www.iso.org/committee/601355/x/catalogue/

7.5 Explore the option for international organizations to establish a community cloud consortium

International organizations could consider forming a community cloud consortium as a possible model for their information management and systems strategy. As revealed by the interview data and survey results, international organizations share similar concerns with regard to extraterritoriality issues, the inviolability of records, and the ownership, custody and control of records. As such, a community cloud could help to achieve greater economies of scale, address specific concerns with regard to the protection and custody of records founded upon a system of privileges and immunities, and harmonize specific provisions in the development of service-level agreements with cloud providers.

8. Conclusions

The study findings depict some of the key challenges and potential gains specific to international organizations in relation to cloud computing, stemming from their distinct legal status and composition. Issues related to the applicability of extraterritoriality and inviolability to the archives and premises of international organizations, and their unique organizational cultures, often characterized by complex bureaucratic structures featuring multiple field offices across the globe, come into play. The study findings reveal the importance of sustained engagement between records and archives, IT, legal and security staff within international organizations on the implementation and use of cloud computing systems. It is clear from the complementary and contrasting knowledge and perceptions of staff in each profession that different types of experts have much to learn from one another, and international organizations stand to gain even more from greater collaboration between staffs.

More research could be undertaken in the form of specific case studies investigating the various and multiple issues that international organizations encounter in the process of evaluating and implementing cloud services. Issues such as information security, privacy, and the management and preservation of records could be examined within specific legislative and organizational contexts.

9. Products

- **Literature Review and Annotated Bibliography**
- **Survey Report**
- **Interview Analysis**
- **Supplementary Report: Extraterritoriality, IGO's and the Cloud**

References

Abass, A. (2014). International organizations. *Complete international law: Text, cases and materials* (Second ed., chapter 6). Oxford: Oxford University Press.

Creswell, J. W. (2007). *Qualitative inquiry & research design: Choosing among five approaches* (2nd ed.). Thousand Oaks: SAGE Publications.

Díaz-González, L. (1991). *(Consolidated) Fifth Report on Relations Between States and International organizations (second part of the topic): Status, Privileges and Immunities of International Organizations, their Officials, Experts, etc*, Extract from the Yearbook of the International Law Commission II(1). Accessed December 16, 2014: http://legal.un.org/ilc/documentation/english/a_cn4_438.pdf

Food and Agriculture Organization of the United Nations. (1991). *Agreement between the United Nations and the Food and Agriculture Organization of the United Nations on the One Part and the Government of the Italian Republic on the Other Part Regarding the Headquarters for the World Food Programme*. http://documents.wfp.org/stellent/groups/public/documents/communications/wfp219968.pdf

Jenks, C. Wilfred. (1961). *International Immunities*. London: Stevens & Sons Limited.

Jurriaans, K.-J. (2012, July 12). U . N . Increasingly Reliant on Private Security Contractors. *Inter Press Service News Agency*. Retrieved from http://www.ipsnews.net/2012/07/u-n-increasingly-reliant-on-private-security-contractors/

McClelland, R. and Grant Hurley. (2016). “Contract Terms with Cloud Service Providers.” InterPARES Trust. Accessed May 13, 2017. https://interparestrust.org/docs/file/NA10_20160130_ContractTerms_InternationalPlenary3_FinalReport_Final.pdf

National Institute of Standards and Technology. (2010). “Cloud computing.” Accessed May 13, 2017: https://www.nist.gov/programs-projects/cloud-computing

North Atlantic Treaty Organization. (1951). Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff signed in Ottawa, 1951. Accessed April 30, 2017: http://www.nato.int/cps/en/natohq/official_texts_17248.htm

Olson, A. (2013, August 8). Correction: UN-outsourcing security story. *Associated Press*. Retrieved from http://bigstory.ap.org/article/panel-un-reliance-private-security-firms-grows

Onwuegbuzie, Anthony J. and R. Burke Johnson. (2008). "The Validity Issue in Mixed Research." In *The Mixed Methods Reader*. Edited by Vicki L. Plano Clark and John W. Creswell. 273-298. Thousand Oaks, CA: SAGE Publications, 2008.

Pingeot, L. (2012). *Dangerous Partnership - Private Military & Security Companies and the UN*. New York. Retrieved from http://psm.du.edu/media/documents/reports_and_stats/ngo_reports/global_policy_forumddangerous_partnership.pdf

Schwandt, T. A. (2007). *The SAGE dictionary of qualitative inquiry* (3rd ed.). Los Angeles, Calif: SAGE Publications.

United Nations. (1946). *Convention on the Privileges and Immunities of the United Nations*. Accessed April 30, 2017: http://www.un.org/en/ethics/pdf/convention.pdf

United Nations. (1947). *Convention on the Privileges and Immunities of the Specialized Agencies*. Accessed May 12, 2017: http://portal.unesco.org/en/ev.php-URL_ID=48887&URL_DO=DO_TOPIC&URL_SECTION=201.html

United Nations Conference on Trade and Development. (2014). *Information economy report, 2013: The cloud economy and developing countries.* 2014 IIS 4050-S33; UNCTAD/IER/2013; ISBN 978-92-1-112869-7 (paper); ISBN 978-92-1-054154-1 (internet). Retrieved from: http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf.