InterPARES Trust Project Report

Title:		Interview Analysis: The Use of Cloud Services for Records Management Purposes in International Organizations
Status:		Final Draft
Version:		4.0
Date submitted:		May 15, 2017
Last reviewed:		May 11, 2017
Author:		InterPARES Trust Project
Writer(s):		Eng Sengsavang, University of British Columbia Elaine Goh, University of British Columbia
Research team:		Jens Boel, Elaine Goh, Eng Sengsavang, Luc Damer, Maggie Hunter, Emily Chicorli
Research domain:		Transnational Team 01 - Legal

Document Control

Version history			
Version	Date	By	Version notes
1.0	2016/09/22	E. Goh, E. Sengsavang	Draft Interview Analysis
2.0	2017/02/19	E. Goh, E. Sengsavang	Draft Interview Analysis
3.0	2017/05/08	E. Sengsavang, E. Goh	Draft Interview Analysis
4.0	2017/05/11	E. Sengsavang, E. Goh	Final Draft Interview Analysis for Presentation at Transnational Team Meeting, 15 May 2017, Geneva, Switzerland.

Table of Contents

1. Objective of Document

This document consists of an analysis of qualitative responses and perceptions of archival and records management and information technology (IT) professionals, gathered through interviews conducted for the InterPARES Trust research project, *The Use of Cloud Services for Records Management Purposes in International Organizations*. The project addresses the following research questions:

Research Question 1: What are the drivers for the deployment and use of cloud services by international organizations?

Research Question 2: What are the barriers for the deployment and use of cloud services by international organizations?

Research Question 3: What are the associated risks to extraterritoriality and inviolability of records and archives when international organizations delegate their records to the cloud?

Research Question 4: How can risks be mitigated and benefits enhanced when/if international organizations decide to entrust their records to the cloud?

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

2. Methodology

The interviews constitute part of a larger mixed-methods study. The main data sources collected for the study include survey statistics, qualitative interview data, an annotated bibliography, and a supplementary report on the topic of extraterritoriality. The interviews took place between March to December 2015, and complemented an online survey disseminated between September 2014 and December 2015, which resulted in statistical data.

The research team interviewed archives and records professionals and information technology (IT) professionals. The research team had originally planned to interview business users, auditors, and legal professionals, in addition to archival and records management and IT professionals. However, due to challenges in recruiting research participants for the study, archivists and records professionals emerged as the most readily-available participants, since this professional group shares a concern over the management and preservation of records in cloud computing.

In addition, we were able to leverage professional networks and contacts in the field, such as the International Council on Archives (ICA) and the InterPARES Trust networks, to recruit and contact potential participants. For example, since some of the intended

participants were attending the annual meeting of the Section of International Organizations (SIO) of the ICA in June 2015, arrangements were made for one of our team members to also attend. The meeting took place at the European Central Bank in Frankfurt, Germany, and enabled the research team to establish contacts with potential research participants. From this meeting, four interviews with archives and records practitioners were conducted *in-situ*, while a further two interviews were planned during the meeting and conducted in Brussels, Belgium, in the months following the meeting.

Customized interview guides were created for each professional category that the research team planned to interview, including for archives and records managers and information technology staff. The interview guides consider the following:

1. **Professional background of interviewees**, including job responsibilities, reporting structure and previous work experience in international organizations;
2. **Use of cloud services** in the interviewee's organization, including the interviewees' understanding of cloud computing; current and future adoption of cloud computing and records deployed by the organization; issues, concerns and policies related to cloud computing and the outsourcing of records to third parties;
3. The **extraterritoriality and inviolability** of international organizations, including how each principle is applied within the organization and how the principles influence decisions to adopt or not adopt cloud computing;
4. **Risks and benefits of cloud comp**uting, including discussion of the survey findings on top five drivers and barriers; and
5. **Service-level agreements** with cloud service providers, including discussion of the survey findings on the role of each profession in drafting agreements.

The interviews were conducted either in-person, via Skype or via telephone. All but two of the interviews were digitally recorded. The interviews that were not recorded were due to specific requests from the interviewees in question. However, handwritten notes were taken during the unrecorded interviews.

2.1 Data Analysis

This section discusses how the interview data was analyzed. The research team focused on analyzing the interview data in order to address the four study research questions: drivers and barriers of cloud computing adoption in international organizations (research questions 1-2); risks to extraterritoriality and inviolability when international organizations delegate their records to the cloud (research question 3); and how risks could be mitigated and benefits enhanced for international organizations that are considering

adopting cloud computing (research question 4). Research question 5 is best addressed by synthesizing an analysis of the annotated bibliography, survey, and the interviews, combined with an interpretation of archival theory. Therefore, the analysis of the interviews addresses only the first four research questions, while research question 5 will be addressed through an article proposal by two of the research team members for submission to an academic journal.

Graduate Research Assistants from InterPARES Trust assisted with transcribing the interviews following their completion. During the course of transcribing the interviews, the research team discussed some of the preliminary themes and categories that emerged from the data. We coded the interview data using a word processing document and spreadsheet, and performed content analyses of the interview transcripts based on each of the four research questions, starting from general themes, to more specific sub-categories and descriptions. Team members provided their comments and insights on the categories of description.

Some of the preliminary insights gleaned from the interview data were shared during the InterPARES plenary meeting in February 2016 held in Vancouver, Canada, and during the InterPARES Transnational Team meeting in September 2016 in Paris, France. Four of the research transcripts were jointly coded by two Graduate Research Assistants. The research team compared both similarities and discrepancies in the coding structure, and came to an agreement on the consistency of the interpretation.

Interviewees are assigned anonymous, unique codes. Archival and records management professionals have been given the code prefix "AR," followed by a sequential number (e.g. AR-1), while information technology staff have been assigned the prefix "IT," followed by a sequential number. Where applicable, the pronoun "her" or "she" will be used in the context of discussing the interviewees, but it does not in any way denote the gender of the specific interviewee. Below we present an analysis of the findings from the interviews for research questions 1-4.

2.2 Background of Interviewees

The research team interviewed a total of 15 individuals from two professional groups: archivists and records managers (12 interviewees) and IT professionals (three interviewees) who work in international organizations. The participants have worked in international organizations for durations of between three to more than 30 years. Nine interviewees have worked in international organizations for more than 15 years. Six work at the senior management level within their units, while five interviewees work at the management level, and three at the professional level. One interviewee works as a consultant.

2.3 Background of International Organizations

The interviewees work for 10 different international organizations, nine of which are based in Europe and one in the United States, with staff sizes ranging between 1,500 to upwards of 40,000 members. Of these, seven organizations employ fewer than 5,000 staff members (10 interviewees), one organization employs between 5,000 to 10,000 staff (one interviewee), one has over 10,000 staff (one interviewee), and two organizations employ over 30,000 staff members (3 interviewees). Thus, two-thirds of interviewees work for organizations employing fewer than 5,000 staff members, while one-third of interviewees work for organizations employing over 5,000 staff members. Although the number of interviewees for this study is small, their worldviews are useful because they are sharing the experiences of a relatively large sized organization. Moreover, some of these organizations have multiple field offices located in various organizations.

3. Interview Findings

This section presents the various themes and findings from the analysis of the qualitative responses, which address research questions 1-4.

3.1 Themes Addressing Research Question 1

What are the drivers for the deployment and use of cloud services by international organizations?

The themes discerned from the data analysis illustrate that the factors that compel international organizations to adopt cloud services are also impediments for the adoption of cloud services. An interviewee admits that she is "conflicted" about the use of cloud services (AR-7). On one hand, she is aware that cloud computing brings an element of risk because there are doubts with regard to the extraterritoriality status of the records. On the other hand, she feels that "there's a lot of potential that can be unlocked through what the cloud offers," and that the organization "could really, really benefit from that" (AR-7). The interviewee is of the opinion that the IT infrastructure and service in her organization is "poor," and that it would be useful if her organization capitalises on cloud computing so as to integrate applications, to enable staff to have ready access to information from "everywhere," and also because the software as a service (SaaS) model is "extremely intuitive." AR-7 also claims that records management services offered in her organization can potentially reap the benefits from cloud computing in terms of the "improved aesthetic

and approach to IT systems and apps." The views expressed by AR-7 illustrate how factors that drive international organizations to adopt cloud services also constitute potential areas of risk.

One observation is that interviewees generally elaborate more on the risks to cloud computing, as compared to the specificities that drive their organization to adopt cloud computing services. This could be attributed to the fact that most of the research participants in the study are archivists and records professionals who are more attuned to the potential pitfalls in the use of cloud services. In addition, most of the IT professionals interviewed for the study are cognizant of the risks of cloud computing. Furthermore, the majority of interviewees had not received first-hand information from the departments within their organizations that had already proceeded to use cloud services. Consequently, they are unable to elaborate on the specific drivers for the deployment and use of cloud computing since they do not have sufficient background information.

3.1.1 Promoting ease of access to information, particularly for records created and generated from satellite field offices

Interviewees share that the easy and ready access to cloud services is an attractive selling point, particularly for large global organizations that have a wide network of satellite offices scattered across various continents (AR-1, AR-3, AR-12. IT-1). Both AR-1 and AR-3 point out that, because of the decentralized reporting structure and system of governance, field officers operate relatively independently and make their own informed decisions on the selection of cloud services. These cloud services are selected mainly because they provide ready access to records that can be shared outside of the organization, for the sake of "expediency" (AR-3) or simply based on convenience. Interviewees perceive cloud computing as a convenience tool primarily for two main reasons. Firstly, a number of participants have already used SaaS, such as Google Docs and Dropbox, in their private lives, are familiar with the interface of the technology, and thus feel that it could be extended for use in the office environment. Secondly, cloud computing services are perceived to provide more efficient services to business users because, "in theory, the services are available 24/7" (AR-1).

Cloud computing was also perceived 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. AR-9 claims that cloud computing provides a "very handy" tool to share information with third parties outside an organization. AR-12 concurs with AR-9's premise that cloud computing promotes access to information. AR-12 views cloud computing as providing the "backbone for ICT infrastructure of field offices" and supports the virtualization of office applications. She

further argues that "all information will be safe," because cloud computing will provide continuity of services even when there are "natural catastrophes" or when staff have to travel across different field offices on "short notice," and yet have to access shared IT infrastructures and information services to conduct their business activities. In the same vein, IT-1 envisages that cloud computing would help to integrate the IT infrastructure and "create a virtual team for colleagues from different bases," which would enable staff to "share information much more efficiently" and "work collaboratively."

Furthermore, cloud computing services promote ease of access to historical archives and to "non-sensitive" records (IT-2). In one organization, a pilot project had already commenced for the adoption of cloud services for historical archives. These archival records are already open to the public domain and as such, the organization deems that there is little risk involved in outsourcing the processing and storage of those records, because there are no copyright issues (AR-2). Furthermore, a number of leading archival institutions, such as the Parliamentary Archives in the UK, have already started using cloud services to store and provide access to open data. Consequently, there is a perception that cloud computing is no longer a novelty and that it is relatively safe for international organizations to follow the example of other leading archival institutions to store archival records that have already been declassified and are open to the public for consultation (AR-4).

3.1.2 Providing flexibility and scalability of services

Interviewees generally feel that the use of cloud computing services provide flexibility and scalability of services (AR-6, AR-7, AR-12). According to AR-12, cloud computing is a "necessity" in her organization because "internal resources are very limited and [we] cannot afford to develop [our] own computing centre." Both AR-6 and AR-7 point out that cloud computing presents "a flexible, easy solution," (AR-6) and that there is no need for staff to "worry about storage quotas" (AR-7). AR-6 argues that cloud computing negates the need for external storage devices, including the use of USBs, which are not "reliable" and also pose a problem for information security.

3.1.3 Cost savings

Interviewees cite cost savings as one of the main drivers for the deployment and use of cloud computing (AR-3, AR-4, AR-5, IT-1, IT-3). Cost cutting is perceived as the "ultimate driver" (AR-3), the "main driver" (AR-4), or the "top of the list" (IT-3) for the adoption of cloud services. In fact, AR-3 foresees that there will be an increase in the use of cloud services within her organization, provided that the information stored in the cloud

has "appropriate content." She asserts that the "external marketplace can provide decent services at good prices," and this is something that her organization can capitalise on, after taking into account all other considerations, including assessing the sensitivity of the information (AR-3). IT-1 states that cloud computing will result in cost savings in terms of manpower, because "you don't need so much IT staff." She argues that in order for an international organization to reap the benefits of cost savings, change management is necessary both on the part of IT staff and business users. IT staff have to think more strategically and reduce the costs of running IT operations through centralization of services. Business users also must adapt because IT staff will no longer be able to provide customized services, which may result in a perceived lowering of standards in service delivery.

Compared to IT-1, IT-2 states that in her organization, considerations for the deployment of cloud services are not made purely on the basis of cost cutting, but to take into account other risk factors, including the need to improve IT security.

3.2 Themes Addressing Research Question 2

What are the barriers for the deployment and use of cloud services by international organizations?

As noted under section 3.1, the main drivers for cloud computing also constitute potential areas of risks that can potentially become barriers for the deployment and use of cloud services. In answering this research question, the term "barriers" does not imply that international organizations in this study have not adopted or utilized cloud services. In some cases, specific departments within international organizations have proceeded to select cloud services, without consulting the IT department and/or the archives and records management units. Interviewees thus view the ad-hoc adoption of such services as problematic, and as a barrier due to the lack of consistency and standardization, and because other specific risks factors. The risk factors are elaborated in this section, while risks specifically related to the privileges and immunities of international organizations are elaborated in section 3.3.

3.2.1 Technological barriers, particularly in developing countries

Section 3.1.1 discusses how cloud computing can help to integrate and streamline the development and delivery of IT infrastructure and services in satellite offices, located across various countries. However, IT-2 expresses concerns about the ability to implement cloud computing services in field offices from developing countries, where internet

connections can be patchy, and where they do not have a good IT system. IT-2 laments that availability of cloud computing services would be an issue if "getting into the cloud is a nightmare or it's too difficult or it's too slow, purely from the user and the customer point of view." Similarly, AR-8 states that it is difficult to embark and implement a central cloud service because the organization is dispersed across various countries, or because, as she describes it, because "we are all over the place." AR-8 also states that some field units do not even have adequate IT services because "…we have people in the desert with no electricity [who are] using personal computers."

3.2.2 Security considerations in protecting the organization's records, particularly those that contain sensitive and confidential information

As discussed under section 3.1.2, interviewees such as AR-6 feel that there is a greater security risk in keeping records through the use of external storage devices, as compared to storing and hosting records via a centralized cloud computing infrastructure. This is partly because individuals can potentially store and lose external storage devices. However, a number of interviewees express concerns that the adoption of cloud computing presents risks because of data breaches and/or unauthorized access (AR-3, AR-5, AR-6, and IT-2). This is particularly so for records containing confidential and classified information, including records containing personal information. According to AR-6, her organization has been the "object of cybercrime" from another country, and so it is critical for information to be kept "secure" so that "nobody from outside can come in." Because of concerns over cybercrime and hacking from external sources, the organization in question has decided that their information should be stored within the territorial boundaries of their country. Generally, the comments from the interviewees regarding security focus more on the locations where data can be stored, or what one interviewee referred to as the "location of the servers" (AR-10), rather than on transborder data flow. However, when discussing issues related to extraterritoriality and inviolability, several interviewees acknowledge that the transmission of information in cloud computing can be a concern. This is explored in more detail in Section 3.4c.1.

Furthermore, interviewees are concerned with external security threats that can emanate from other countries. As such, much of the security considerations focus on ensuring that "information needs to reside on the territory of one of the allies" (IT-1), on the use of technological solutions such as encryption "as a way to protect my data" (AR-8), and on strengthening security protocols when transporting data to and from an external service provider (AR-3). However, our findings show that interviewees generally do not pay much attention to internal security issues within the organization in relation to cloudcomputing (with the exception of IT-2). This is somewhat surprising given that some

of the security threats are caused by units or individuals who work internally within the organization. For example, some staff have proceeded to use SaaS to store and transmit sensitive records (AR-3, AR-8, AR-9). In other words, staff lack awareness on the need to protect information security and personal information within the organization. IT-2 notes that it is "very hard" to monitor internal security issues that can be partly caused by staff "doing something completely by mistake" without realizing it, or because of "determined insiders."

3.2.3 Decentralised approach with regard to the choice of technology

Interviewees shared that various units within international organizations operate independently from one another and at times, these departments may decide to deploy cloud services without necessarily consulting other departments or staff, such as archives and records professionals and legal personnel (AR-1, AR-2, AR-4, AR-7). AR-2 mentions the existence of "silos," where selection of technologies is not decided on an organization-wide basis. AR-1, AR-3, and AR-7 comment that decisions are made in a decentralized manner within their organizations, with some individual business units having their own IT and administrative units. In addition, some business units that are not satisfied with the level of service delivery from the IT department may decide to directly purchase their own software and IT systems from service providers. As such, it is difficult to establish controls in terms of IT governance, records management, and legal controls for the management and preservation of records in the cloud. As stated by AR-1, "once things become digital, there's less control over what is happening in practice".

Archives and records professionals reveal that often, they are only informed of plans to deploy cloud computing through informal discussions with business users. In another example, one of the archives and records professionals accidentally came across a record from the organization's recordkeeping system stating that the audit department intends to conduct an analysis on the impact of cloud computing with regard to security and energy savings, as well as the overall performance of the organization (AR-4). However, the initiative to deploy cloud computing was not made known to the archives and records professional.

3.2.4 Lack of policies governing the adoption and use of cloud computing

Interviewees lament that the current policy framework in their organizations are out-dated and do not address challenges in the management and preservation of records in the cloud. AR-5 recalls a few instances when business units had proceeded to select a cloud computing technology before steps were taken to develop a policy framework. Although

AR-5 admits that such a situation is "probably not ideal,' she proposes that it was unavoidable given the changes in technology and the need for business units to respond to an immediate issue regarding their business processes and activities. In another example, a business unit proceeded to store records in the cloud and was subsequently informed that the legal department had concerns with the department's decision. AR-5 claims that the policy work "seems to be in progress" and needs to address the issue on what records and data can be deployed to the cloud. AR-7 concurs with AR-5's observation that the policy framework lags behind the adoption and use of specific technologies. The organization for which AR-7 works is in the process of implementing an instant messaging system with video conferencing abilities. However, there is no existing policy that has addressed records management issues such as whether instant messages are records. In addition, the organization has not reflected on the use of the technology in terms of business value, and implications with regards to storage capacity (AR-7).

Due to the lack of policy frameworks in the management of records in the cloud, there is little consideration of records management issues in the selection and use of a cloud computing technology. Interviewees recognize the lack of records retention schedules for records deployed to cloud computing (AR-1, AR-6) and there is little consideration on archives preservation (AR-4, AR-7). A number of interviewees note difficulties in ascertaining the final and authoritative record, especially when it is easy to store and distribute multiple copies in the cloud (AR-6, AR-11, IT-1). In one organization, users are told to store records for "long-term storage" in the records management system, whereas the cloud-based system is mainly used for sharing files. However, the interviewee admits that despite the instructions given to users, they have not instituted proper controls and checks (AR-6).

3.2.5 Varied understandings of cloud computing and the risks involved in outsourcing

The data reveals that interviewees understand cloud computing in various ways. Some interviewees associate cloud computing with the storage of data (AR-2, AR-3, AR-4), while others view cloud computing both in terms of hosting hardware and software (AR-7, AR-11). Some interviewees also view cloud computing as a method of managing "IT capabilities" (IT-3). One interviewee acknowledges that cloud computing is "one of these buzz words that everybody uses, but possibly not everybody understands it to the full extent" (AR-4). These varied understandings of cloud computing imply that there are times where a choice is made about a technology without taking into consideration the legal and records management implications. In one organization, a SaaS was selected strictly on the basis of price. The interviewee claims that the individuals involved in selecting the cloud

service viewed it as "web-based service" because the concept of the "cloud hadn't taken off at that time" (AR-7). AR-7's observation illustrates that the organization selected a cloud computing service without adequate understanding of the technology and the accompanying risks involved. Some archives and records professionals reflect that they lack "IT capabilities and skills" (AR-3) and that they do not possess sufficient technical knowledge to fully comprehend and assess the impact of the technology on records management (AR-12).

3.3 Themes Addressing Research Question 3

What are the associated risks to extraterritoriality and inviolability of records and archives when international organizations delegate their records to the cloud?

Research question 3 addresses the concepts of extraterritoriality and inviolability in relation to international organizations, and asks how they may be impacted when international organizations adopt cloud computing. In designing the interview script to address this research question, the research team chose not to establish definitions for extraterritoriality and inviolability, since we anticipated that definitions for and perceptions of the terms may vary amongst interview participants. We aimed instead to gauge how participants themselves understand and apply the two principles, rather than prescribing our own definitions for the terms. The interpretations of interviewees could in turn help to explain whether and how organizational decisions or practices related to cloud computing are impacted by considerations of extraterritoriality and inviolability.

3.3a Interviewees' Perceptions of Extraterritoriality

Responses indicate that extraterritoriality is understood and applied in various ways within international organizations. However, a majority of interviewees link extraterritoriality to the system of privileges and immunities of international organizations, and to the concept of inviolability. This suggests that in the context of international organizations, extraterritoriality most often refers to the jurisdictional immunities of the organization from interference or unauthorized access by state or other parties. Some interviewees seem uncertain, or express doubt in their own understandings of extraterritoriality and how it is relevant for international organizations.

Four of the fifteen interviewees admit to a lack of understanding and/or awareness of extraterritoriality within their organizations or at a personal level (AR-1, AR-3, IT-1, IT-2). On the question of how and whether considerations of extraterritoriality figure in

organizational decision-making and practices, AR-1 notes, "I don't think there has been active engagement [with extraterritoriality] at the recordkeeping level." In the same organization, there have also been no discussions between legal staff and staff involved in creating information technology policies on the implications of deploying digital records off-site, as opposed to keeping data on-site (AR-1). IT-2 notes that decision-makers within international organizations, such as information technology staff, who are leading the implementation of cloud adoption within organizations, are not necessarily aware of the concept of extraterritoriality and how it may be relevant to the management of records in cloud computing systems.

Several interviewees believe that extraterritoriality in connection with international organizations is related to the principle of inviolability and/or immunities (AR-1, AR-3, AR-6, AR-7, AR-8, AR-9, AR12). AR-8 asserts, "I think that [extraterritoriality and inviolability] go together. I don't see how you can take…one separate from the other. One is based on the other." AR-1 states that extraterritoriality is "applied more like inviolability," while AR-3 describes extraterritoriality as "protection from wherever the organization is located." AR-9 extends this type of immunity to the assets of the organization: "…even if some of the assets of the organization, like archives for example, would leave the organization's premises, they are still inviolable, extraterritorial, even if they are not at the organization." Another interviewee states, "we are extraterritorial because we are an international organization. So we have our own rules and regulations. And, external rules and regulations do not really apply" (AR-6).

The significance of the space or premises that an international organization occupies emerges as a notable theme addressed by interviewees. Some participants articulate the view that extraterritoriality means that international organizations are considered to be separate from the territory of the nations that host them (AR-3, AR-9, AR-11). As one participant remarks:

> *All [of the organization's] premises, and certainly conceptually it would apply to the cloud…are not considered [host-nation] territory. So any repository of the [organization's] records, for example our facility over in [host country], even though it's outside off the main headquarters, the agreement with the landlord of that building includes language to the effect that that space that we have is considered premises of the [organization]* (AR-3).

The premises of the organization are legally and physically separate from the territory of the host nation, and this principle extends beyond the headquarters of the organization to the premises of its missions and bases. "Conceptually," the notion of a separate space applies 'to the cloud' (AR-3). In this view, "extraterritorial" means that the space occupied by international organizations, including any of its repositories, are by agreement

considered to be *outside of* host nation territory: extra-territorial to the host nation.

The comment distinguishes between 'premises' versus 'territory': while states have territories, organizations occupy premises or space. International organizations do not have territory, and their physical bases and missions are not extensions of a territory, as is often thought in the case of diplomatic missions.[1] Rather, international organizations occupy a kind of negative space that is *not part of* state territory, instead of possessing a positive, distinct territory.

The question of whether the location of data determines the immunity of an organization or its data looms large for several interviewees (AR-1, AR-2, AR-3, AR-4, AR-6, AR-9, IT-2). For some interviewees, the physical location of data—where data is stored, processed, and where it passes through, can be a determining factor. Referring to discussions with colleagues, one interviewee describes extraterritoriality as meaning: "we can only keep all of our records that are in archival custody inside the building" (AR-1). This statement highlights the notion that both extraterritoriality and inviolability apply only when records are held on the premises of the organization. The position is echoed by IT-3, who states, "we don't do any extraterritoriality. The majority of resources are on premises, and when we do share things it's with other work institutions, so it's like the same family. There's no real extraterritoriality." Both interviewees suggest that the protection of data can be guaranteed only within the premises of an international organization.

Concepts of ownership and control over an organization's own data emerge as another important issue (AR-7, AR-8, AR-9, AR-12). One interviewee perceives extraterritoriality to mean that the organization has ultimate control, ownership and authority over its own records: "We are completely free to decide what we do with [the organizations' records], so it's up to us to say what we want to keep [and] what we want to destroy…we are very conscious that we are opening the whole archives as a privilege, not as an obligation" (AR-8). The interviewee emphasizes the complete control that the organization exercises over the fate of its own records, and over access to its records.

AR-7 asserts: "the records of the organization do not belong to any one country, any one member of the organization, but are the organization's records, and they're again immune from search and seizure." Here, AR-7 draws a direct relationship between extraterritoriality, immunity and ownership: the records of an international organization belong strictly to the organization itself, not even to its members, and are therefore immune from external access.

---

[1] This conception, in any case, has been declared to be a legal fiction by Dikker-Hupkes: "…the extraterritoriality theory…refers to the legal fiction that the premises of diplomatic missions are considered to be official territory of the sending state. This fiction has been discarded as a theory for a long time, although it is still subject to widespread popular belief" (26).

3.3b Interviewees' Perceptions of Inviolability

The inviolability of archives and premises is clearly established in the constitutional treaties and multilateral and host-seat agreements of most international organizations. This may explain why, in comparison with perceptions of extraterritoriality, interviewees discuss the term "inviolability" with more confidence, and with a more consistent understanding of its meaning. In general, interviewees understand inviolability to mean a type of immunity that protects international organizations from any interference, physical or legal, from their host or other states.

Some interviewees cite the specific agreements or treaties of their organizations that establish inviolability (AR-10, AR-11). One participant referenced, during the interview, the inviolability clause in both the founding treaty and the treaty on the status of representatives and staff of her organization, stating that not only the premises, but the "property and assets" of the organization are inviolable "…wheresoever located and whomsoever held, [and] shall be immune from search, requisition, confiscation, expropriation, or any form of interference." The clause also states: "The archives of the organization and all documents belonging to it, or held by it, shall be held inviolable." The headquarters agreement of the same organization with the host nation contains a similar article, asserting the inviolability of the organization's archives and documents, and the article can also be found in the organization's records policy. Another interviewee states that inviolability is "absolute," and cites specific articles in the founding treaty and in another agreement of her organization establishing the inviolability of the archives.

Similar to interpretations of extraterritoriality, some interviewees link inviolability with ownership and/or control over data (AR-7, AR-8, AR-12). One interviewee describes inviolability as meaning: "nobody can take [the archives of the organization] away [unless] the organization gives specific consent, or agreement that those can be used, but otherwise…they cannot just be taken away" (AR-10). The same interviewee connects inviolability to the idea of "integrity" (AR-10). In the context of inviolability, the notion of 'integrity' can have multiple meanings, such as that a repository remains safe from unauthorized access, or that records are whole.

3.3c Interviewees' Perceptions of Risks to Extraterritoriality and Inviolability in Cloud Computing

The team identified six risks to extraterritoriality and inviolability when international organizations adopt cloud computing for recordkeeping purposes: 1) the risk of external control over organizational data; 2) the risk of unauthorized access, which encompasses risks to data protection, data privacy, and security; 3) the risk that

organizational standards or policies are not enforceable in the cloud; 4) the risk of loss of ownership of data; 5) risks related to the loss of custody of data; and 6) risks to data integrity. A narrative analysis of each risk is provided in the following section.

3.3c.1 Risk of External Control Over Data

The most commonly cited risk to the jurisdictional immunities of international organizations is that posed by domestic, even "hostile" (AR-3) jurisdictions or governments (AR-1, AR 2, AR-3, AR-4, AR-6, AR-8, AR-9, AR-10, AR-11, AR-12, IT-2, IT-3). Although international organizations and their data are protected by inviolability and extraterritoriality, in the sense of having immunity from state laws (AR-2, IT-2), the jurisdictions of the locations in which data is stored or passes through, or the nationality of the cloud service provider itself, are perceived to pose risks to the control that an organization is able to exercise over its own data.

The transmission of data in the cloud in particular raises questions as to how data may be vulnerable to the laws of jurisdiction(s) that data passes through while being processed in the cloud. As AR-3 remarks, "It's a tough enough challenge if you're thinking about [data] being in a cloud environment…certainly when you're potentially in hostile territory, but most importantly [extraterritoriality] relates to the transmission of information." Participants describe the characteristics of cloud computing models that contribute to a lack of clarity over how and where data is stored, transmitted, and processed. They cite as especially problematic the "dispersal of data" (AR-7) or continual transmission of data in several different servers located in multiple countries (AR-3, AR-11); or, as AR-10 puts it, a system in which "nothing is fixed" (AR-10). If the location of data is unknown, or constantly moving, or if data is replicated in more than one location at one time, then there is an increased risk of the loss of control over one's data.

AR-11 explains the complexity of transferring physical records in airspace, stating that 'extraterritoriality constraints make it difficult.' For both physical and digital records, 'there are rules on the transport of the organization's information through non-organizational territory; and in a cloud computing environment, transfer is even more complicated' (AR-11), presumably due to the difficulty of determining the location of data as it passes through globally distributed data servers. According to legal staff, the organization would 'violate its own inviolability' if it were to host data off-site, due to 'the fear that [state] laws would apply to the organization' (AR-11). In other words, hosting data off-site would mean that the data would no longer be protected by the inviolability principle; the organization would, in this case, waive its own immunity.

By contrast, AR-9 states that, "even if some of the assets of the organization, like archives for example, would leave the organization's premises, they are still inviolable,

extraterritorial, even if they are not at the organization. So that's the legal department who would take care of integrating that correctly in the agreements." Since archives and records are considered to be part of the assets of an organization, the inviolability principle would apply to data whether or not it is on the premises of the organization. According to this view, an international organization could deploy records to the cloud without waiving its immunity; the inviolability principle would hold even in the cloud, and would be reinforced through legal agreements.

Although AR-11 and AR-9 hold differing positions on how inviolability would be applied to data in the cloud, they share a concern, along with virtually all other interviewees, over the location and jurisdiction of data. This concern is perhaps exacerbated by the distinct—and possibly more tenuous—legal status of international organizations as compared to that of states. AR-6 notes that international organizations "have no jurisdiction," and that there is a "legal background" that is "missing for us." This concern underscores the need to consider and clarify issues related to data location and data jurisdiction before deploying records to the cloud.

Other interviewees express concerns related to the jurisdiction and nationality of the cloud service provider. One interviewee notes that the United States "has a legal framework that allows U.S. officials to impose on IBM or other multinationals access to data that the [U.S. government] normally would not have access to" (AR-12). Another interviewee states:

> *I just learned that even if [the cloud service provider is] in a European country having a higher level of protection...in fact if the company is American...they have to follow [American] rules, so there's no protection. There's zero protection...you are putting your data at risk...And you're putting it in a corporate company who will have to follow the rules of the [U.S.] government. You are putting yourself in a very weird position, I think* (AR-8).

The reference to a 'hostile territory' by AR-3 additionally suggests a recognition that diplomatic or political relations could affect the safety or control of data in the cloud. One interviewee notes that one of the risks of entrusting data to cloud service providers relates to the vagaries of "high-level political situations" (AR-2). Foreshadowing the 'BREXIT' vote that took place in the United Kingdom in 2016, AR-2 remarks that the extraterritoriality of data could be impacted by whether or not the UK decides to leave the EU. In such a case, if the organization has cloud service contracts with UK providers, "what happens to our records?" (AR-2).

These comments are illustrative of the common perception amongst participants that external jurisdiction(s) to which data may be subjected pose a serious risk to

organizations that entrust their records to the cloud. This may help to explain why interviewees express the need to know where data and data servers are located (AR-2, AR-6, AR-11), in order to control the physical location of data (AR-11) and to ensure that the jurisdiction to which data may be subjected is clear (AR-4, AR-6).

3.3c.2 Risk of Unauthorized Access: Data Protection, Data Privacy, and Security

A consequence of the loss of control over an organization's data is the risk of unauthorized access to data by external parties (AR-4, AR-8, AR-9, AR-10, AR-11, AR-12, IT-3). Some interviewees acknowledge 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 (AR-10, AR-11, IT-3).

One interviewee expresses the belief that there is no privacy protection in cloud computing models, and that it is difficult to define privacy concerns (AR-11). Another interviewee asserts, "essentially the key question" is "to be sure that the provider will respect EU laws on data protection" (IT-3). AR-11 asks, "who is administering the data centre and who could look at the data?" suggesting apprehension over unauthorized access to data. When explaining why the international organization in question has not yet adopted cloud computing, AR-11 states that organizations lose control when they put their data in the cloud, and that governments are declining to use the public cloud for the same reason, because they cannot control the access to their data in the cloud.

A basic understanding of inviolability is that it signifies protection against any form of unauthorized access by parties external to an international organization. It is logical, then, that participants cite unauthorized access in a cloud environment as a risk to the inviolability of archives (AR-4, AR-9). One interviewee opines that "one of the main problems is of course the risk of external access, the security of the information" (AR-9); another replied, in answer to the question regarding risks to inviolability in the cloud, "basically access, unauthorized access, the fact that documents might be available, might be hacked" (AR-4).

A third interviewee describes the nature of the records held by their organization as being particularly vulnerable, since it contains personal data of a highly sensitive nature; for this reason, the inviolability principle is "a rule that is taken very seriously": "There are standards for request for instance…there is a unit that deals with this. So they examine and they only share information [if there is] a very strong reason to do it, and only a small part we want to share." (AR-8). She continues, "if we are thinking about using [cloud computing], it would be for data…that's already public. And there's not an issue about this data. But even if this data [is public,] we're wondering if this is the solution [that] would fit" on the cloud (AR-8). As the interviewee explains, even if data deployed to the cloud

consists of publicly disclosed records, there is still uncertainty over whether cloud computing is an appropriate solution.

The comment echoes a conclusion made by AR-2, who describes a pilot project by an international organization testing a cloud computing environment. In the pilot project, the organization used public records: "It was just a pilot of historical records that…were already public and publishable…so it's a minor risk attached to it" (AR-2). Both interviewees signal that the level of risk to an organization and its data when using cloud computing can depend on the type of records deployed.

One consequence of unauthorized access to data is the impact that this would have on the security of an organization or on its interests. One interviewee notes that if their organization were to adopt cloud computing, the staff of the cloud service provider would need a security clearance (AR-11). Another interviewee questions whether data would be secure enough in the cloud (AR-12). Security risks stem from the lack of guarantees in cloud computing mentioned by other interviewees, since without such guarantees, security concerns become a prohibitive factor in the adoption of cloud computing.

3.3c.3 Risk to the Enforcement of Organizational Standards or Policies in the Cloud

Many interviewees refer to organizational policies prohibiting data, and therefore data servers, from being stored outside the territories of the member states of an international organization (AR-6, AR-9, AR-10, AR-11, IT-1). Doubts are raised regarding the enforceability of such policies in a cloud computing environment. One interviewee notes that it is uncertain whether it is even possible for a cloud provider to guarantee that data stays exclusively within member state territories (IT-1). Another states that while an organization could stipulate a specific contractual requirement for the "data to be hosted only in Europe…the difficulty is that [contractors] really do it" (AR-12). Having a legal agreement may not be enough to guarantee that data in the cloud would stay within the bounds of national borders specified within a contract. One participant asks, "this information is in theory in control of somebody else, and from a security point of view what guarantees have we got that they are protecting our information according to our standards?" (IT-2).Another interviewee states, "the biggest problem is trying to enforce the same policy with the cloud provider…with private companies that operate on a multinational level like IBM, to be sure they are doing what they are really doing…it is more difficult" (AR-12).

A related issue is the unpredictability and lack of certainty over the consequences of deploying organizational records to the cloud. Some interviewees explain that the implications of storing data outside a member territory are uncertain (AR-1, AR-6). As one interviewee states, "I'm not sure when we store our information in something which is no

longer our own international territory, what would be the impact on it" (AR-6). The statement draws attention to the fact that, despite the increasing integration of cloud computing models, the full impact of the technology is as yet unknown. As one interviewee remarks, "I think we need to make sure we're doing it correctly, that we have a policy, that we protect ourselves contractually, and I'm not really convinced that…we can contractually protect ourselves or contractually protect our extraterritoriality at this time...the cloud is a very much untested territory" (AR-7). This perceived lack of guarantee or inability to enforce policies in the cloud seems to act as a significant barrier to the adoption of cloud technology within international organizations, as exemplified by an unequivocal statement by AR-10: "I think that it's just not…a question. [Extraterritoriality] just needs to be guaranteed. If it cannot be guaranteed, then it is simply not done."

3.3c.4 Risks to Data Ownership

Four interviewees express a concern over the ownership of data (AR-2, AR-9, AR-10, IT-2) deployed to the cloud. One interviewee states: "Our major worry or concern was really, this data still belonged to the UN, so we needed to know where this data was really placed…this data should never appear as being [the] property…of someone else or…another body" (AR-2). The interviewee explains that the issue of ownership has less to do with copyright issues than with concerns over the use of information and intellectual property, and in particular, with the "reputational risk of the misuse of this information" (AR-2).

In the context of cloud computing, AR-10 asserts, "ownership of the [organization's] information…can never change [to] whoever is the service provider." She reiterates, "there can be no transfer of ownership" (AR-10). Ownership must always remain within the organization, and in a cloud contract, ownership of data deployed to the cloud "needs to be crystal clear," so "you would have to define" it (AR-10). IT-1 similarly suggests, "there would definitely have to be some sort of agreement as to whose information this was, the whole legal aspect of it," another call to establish clear ownership of data deployed to the cloud.

A discussion with one of the interviewees turns to concerns over the potential for third-party service providers to abuse intellectual property rights: "Some of those free services, they say, if you put something on our site it's free, but then it becomes our property, which is not possible in the organization, and people often probably don't even know that…and then there are problems" (AR-9). AR-10 affirms, "I think also ownership…is linked to inviolability...[the data] should be the property of the organization" (AR-10).

3.3c.5 Risk of Loss of Custody

Several participants highlight custody of records in cloud computing as an issue (AR-1, AR-7, AR-8, AR-9, AR-10). Some interviewees express the belief 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. One interviewee states, in regards to an organization's records, "…there can be a transfer of custodianship, but that always has to be to an organizational entity, not to an external service provider" (AR-10). Another interviewee states, "based on the interpretation by the legal people, extraterritoriality means that we can only keep all of our records that are in archival custody inside the building" (AR-1). When legal staff were asked, "Can we then put the material somewhere else? The response we got is, 'No you cannot, because we only have that extraterritoriality principle in place in the building'" (AR-1). According to this view, custody is a prohibitive factor in the decision to adopt cloud computing, since it is an outsourcing model wherein physical custody of records is not possible. Instead, digital records are processed, transmitted and stored off-site, through remote and opaque processes that are difficult to monitor. The virtualized nature of cloud computing services and the distance and scale that characterizes the technological infrastructure, both in terms of geographic distribution and end hardware (data centres, etc.), complicates the question of the meaning of archival custody.

However, one interviewee states that in cloud computing, "The records are maybe not for the time being, then, in the organization, but they're still in the organization...Even if they're in another place" (AR-9). The statement suggests that even if records are not directly in the custody of the organization, and outsourced instead to third-party services, they are still considered conceptually and intellectually to be "in the organization."

3.3c.6 Risks to Data Integrity

Participants express concerns over the integrity of data deployed to the cloud. Integrity is discussed by participants in various ways, meaning whole, un-tampered with, unaltered, and auditable, or having a verifiable trace (AR-4, AR-7, AR-11, IT-3). AR-7 states, "to the best of my knowledge…we're not using a private isolated cloud, nor what some might call an internal cloud…It depends on how you would define private cloud. I mean are the records…isolated on their own servers [with] no records of any other body…on those servers as well?…I doubt there was any contractual obligation to separate or to delineate between our records and records from other entities." The question alludes to an issue inherent in various cloud computing service models, wherein the data belonging to one organization could be mixed with that of other organizations. Again, this becomes a problem particularly when organizations manage classified or sensitive information, a

reality for most international organizations.

Another interviewee speaks of the need to "...guarantee...that the records cannot be tampered with, altered in any way," and stresses the importance of ensuring that records are traceable and that their integrity remains intact, meaning "...that the records that we put [in the cloud] are the same that we will retrieve" (AR-4). Similarly, IT-3 notes challenges related to "ensuring that the information is really correct, that it has not been hampered by any third parties or individual or organization." AR-11 questions how one could prove that records have not been tampered with, and concludes that she cannot see how organizations could entrust their records to the cloud.

3.4 Themes Addressing Research Question 4

How can risks be mitigated and benefits enhanced when/if international organizations decide to entrust their records to the cloud?

While participants express mixed levels of confidence in the appropriateness or potential of cloud computing to be adopted by their organizations, citing various factors, many also offer suggestions and mechanisms to safeguard records in the cloud. Many of the mechanisms relate to contractual or legal means to ensure that records delegated to the cloud are properly managed, but other measures, such as technological and physical protection measures or the development of policy, offer complementary means to mitigate the risks of deploying records to the cloud.

3.4.1 Develop detailed service agreements

Participants acknowledge that one way to mitigate the risks of cloud computing is to draw clearly defined and detailed contracts with cloud service providers (AR-3, AR-4). AR-4 asserts, "you should clearly define what are the requisites and spell out everything that is expected…it's very important to think about all the eventualities, define them clearly in the contract." AR-3 describes an example of "a dataset maintained off-site…by a third party," for which "there were very elaborate MoUs wrapped around the contract. And there were also very stringent measures taken to transport the data to and from the vendor." AR-10 maintains that a particular detail that would need to be contractually defined is ownership of data.

3.4.2 Include contract provisions to protect inviolability and jurisdictional immunities

Three interviewees believe that inviolability and jurisdictional immunities need to be respected in cloud computing contracts, or point to standard clauses in external service agreements of their organizations that protect the immunities and privileges of the organization (AR-3, AR-9, AR-10). For example, AR-3 remarks, "there is language in our MoU with [a cloud service provider], even though that's public information, there is language around inviolability, that's absolutely standard in any cloud [contract]." Even if only public records of the organization are deployed to the cloud, the agreement with the service provider would stipulate a standard inviolability clause. AR-3 clarifies that, "in fact all [of the organization's] contracts with external vendors do make provisions regarding the protection of privileges and immunities and inviolability."

AR-9 confirms, "We've used external companies, for example, for digitizing archives. There's always a contract. The contract contains all the clauses for confidentiality and inviolability." For AR-9, "a contract that respects all the laws and the conventions of the organization" would need to be implemented in a cloud computing service contract; for emphasis, she cites a constitutional treaty of the international organization in which privileges, immunities and inviolability are stipulated. Another interviewee, in describing a potential cloud service contract, states, "Inviolability would definitely be there, [as well as] extraterritoriality and immunities" (AR-10).

3.4.3 Include contract provisions specifying which laws would apply to records

Some participants suggest establishing a contractual clause to specify which laws would apply to the records deployed to cloud computing. AR-4 stresses, "specify very clearly…which is the legislation that applies, so for example these are our records, it follows that the regulations of the EU institution of the [international organization] would apply to [our records in the cloud], but clearly spell it out and if there's any dispute, define also how it would be settled" (AR-4). AR-12 states that a specific contractual requirement would be for "the data to be hosted only in Europe."

3.4.4 Ensure organizational standards are met, for example through audit and inspection controls

After contract clauses, participants express with almost as much frequency the need to ensure that third-party service providers meet the standards of the organization (AR-11, IT-3), for example through audit and inspection controls (AR-10, AR-11). As one

participant notes generally, "We're not yet there, but I would say that one of the most important [measures] would be engagement by the service provider to comply with the policies and regulations [of the client organization]" (IT-3). Another interviewee emphasizes compliance with the standards of the organization: 'Obviously [there] would have to be a guarantee that the service provider would provide the services according to the standards set by the particular agency [within the organization]…we all have standards of what we would want'; this would include 'minimum standards for security…that the provider would have to agree to or guarantee [could] be met' (IT-2).

Two interviewees mention audits and inspections by their organization as a way to ensure that external providers comply with standards (AR-10, AR-11). AR-10 notes that it is not enough to embed a clause within a contract; the organization:

> *…also has to monitor and control it…This is also part of the accreditation process, where someone in…security would actually go out, inspect these sites…this accreditation process is something we see in basically the underlying part for all sorts of services. You have to have that in place before anything will actually be considered…for us, it's the only way to make that work.*

Another participant underlines the fact that 'for records, there are legal requirements that the provider has to meet organizational standards, and the organization needs to certify that it has been done' (AR-11). However, she questions how to prove that records have not been tampered with, and surmises that 'unless an audit control is in place, and can be provided to the organization,' the organization cannot trust records to the cloud (AR-11). AR-11 also notes that 'third parties must accept our security guidance'; a few years ago, the organization cancelled a contract unrelated to cloud computing because the contractors were not compliant with organizational standards.

3.4.5 Develop or revise policies and/or a governance framework to address cloud computing and involve the archival/records management profession in cloud computing decisions

Some interviewees call for international organizations to form or revise policies and governance frameworks that address cloud computing. One participant states, "Legal needs to come up with some kind of a recommendation or absolute policy" for addressing cloud computing (AR-5). Another participant opines that there needs to be "a governance group" to devise a cloud computing policy (IT-3). A third interviewee foresees the possibility that cloud computing technology will become an inevitability, to which organizations may be bound to adapt: "we may be forced because it is said that the forces for cloud computing are quite strong in the business and also in [the organization]. So,

where technology is going, it may force us to review our security policies" (IT-1).

Two participants stress the need for archivists and records managers to play a more active role in decision-making and policy development related to cloud computing technology within organizations. As AR-4 states:

> *…we need to be proactive, I'm saying this for my institution, I was surprised to see [that my] apparently very conservative institution…are taking the preliminary steps [to consider adopting cloud computing] and…nobody's waiting for us in this discussion, so we should be proactive and move and appear and say…we records professionals have something important to say about this, and when you define these records, these cloud policies, we should be moved.*

AR-4 elaborates that the information management unit in their organization is "trying to become a player in these issues, try[ing] to have an active role, because until now for many decisions, records and archives management has been not considered. It's an afterthought at best. But in this case obviously it has important implications and we should be present…and contact these people and tell them look, when you launch this cloud policy take us into account. At least think of us as possible stakeholders and give us an opportunity to say our point."

In the same vein, AR-6 states: "we [archivists/records managers] can always insist that we should be involved. This is how it always happens." The latter statement suggests that archivists and records managers do not become participants in decision-making processes unless they are proactive.

3.4.6 Manage the type of records deployed to the cloud

Many interviewees perceive that one way to mitigate the risks of deploying records to cloud services is to limit or manage the types of records that organizations entrust to third-party providers. Two interviewees cite pilot projects within their organizations that test cloud computing services using public records, which pose a low risk to the privacy and security of data and organizations (AR-2, AR-4). Interviewees also perceive the need to define the type of records that are deployed to the cloud:

> *We need to think also [about] the kind of records that would go into the cloud, because I don't think that for this organization all records would go…once the kind of records are clearly defined, for example, these are public, then what are the requisites. If some records are not public or have some more stringent requisites for security, then we need to specify something different (AR-4).*

Another interviewee asserts, "we need to determine what kinds of things are being put on the cloud and what kinds of things people plan to put on the cloud" (AR-5). One interviewee holds the viewpoint that their organization should "decide…what will be cloudified, what will be de-cloudified. There should be some governance decisions. That's how the policy should look" (IT-3). The interviewee imagines a cloud computing policy that would outline the kinds of records that should and should not be managed using cloud services. Finally, AR-9 predicts that cloud computing "will probably be for things that are published to share in the context of a project [or] to share information with a third party [and] with the external community...[but] confidential records, I can't see them move to the cloud" (AR-9).

3.4.7 Introduce technological and physical protection measures

Apart from legal, contractual or policy measures, other measures for addressing the risks of cloud computing include technological and physical protection measures focusing on data security. One interviewee suggests cryptographic measures for ensuring the security of records in the cloud (IT-1). Customers who "come with their own cryptographic devices, which the users control…add on top of the security offered by Microsoft. It gives [the client] an additional level of security and potentially it could meet a company's or somebody's inviolability requirement" (IT-1).

Another interviewee suggests the preservation format PDF/A as a measure to ensure that inviolability is not circumvented: "So far, what I know is that it's really a technical thing, but PDF/A for ensuring the security facet, ensuring that the information is really correct, that it has not been hampered by any third parties or individual or organization...even on-premises, inviolability is addressed via these technical solutions, provided by Adobe, PDF/A...It's a special format for archiving information to ensure that it will be inviolable, in theory" (IT-3).

Two participants suggest technological checks for ensuring the integrity of records in the cloud and as a guarantee that they have not been tampered with. AR-11 states that third-party providers 'must be willing to accept the [organization's] vulnerability checks and implement remedial measures required by' the technology oversight agency of the organization. Similarly, AR-4 opines that "we need to establish protocols to control…procedures of transfer [in cloud computing]…to ensure this integrity, for example, whenever we push something to the cloud and then it's retrieved and passed through…hashtags, algorithms, to make sure that the records are the same that we send."

One participant suggests that data server centres must be physically protected "in a similar way [from] what we asked for external physical storage" for paper records: "I would go back to…all that we have written about when we…outsource our storage areas…When

it was for physical [records], all the things we have thought about…that it has to be safe, that there's no unauthorized access" (AR-6).

3.4.8 Request specific service measures: continuation of service, continual access

Some interviewees assert the need to ensure that specific service measures are in place to mitigate the risks of deploying records to the cloud. One interviewee mentions that it would be important to ensure availability of services, especially during peak times (IT-3). Another interviewee cites the need to guarantee "access over time to the information" in relation to retention and disposition schedules (AR-10), suggesting a concern with access to data and services over a longer term and throughout the lifecycle of records. The same interviewee expresses a concern with maintaining the integrity of information, by stating that the second most important measure when adopting cloud services "would be defining the exit strategy to ensure that we would get the information back in the correct form" (IT-3). Another interviewee suggests "not putting all your eggs in the same basket, have a system of several providers, at least two providers in order to guarantee continual service" (AR-4).

3.4.9 Use a private cloud

One interviewee explains that their organization has adopted cloud computing services, but uses a private cloud: "The fact that they selected a private cloud was of course [so] they can have their own rules for it" (AR-6). The implication is that in a private cloud, as opposed to a public, community or hybrid cloud, an organization has more control over the management of their records in the cloud.

3.4.10 Address concerns of member states

The politics of multilateral relationships figure as a consideration for one interviewee, who notes the importance of members states' concerns in the decision to adopt cloud computing services by their organization:

> *…we also need to…think about how we would address concerns about the cloud if they were expressed by our member states, because our member states…pay attention to all sorts of things, and it is potentially something that they could say, well you know I hear you're putting records in the cloud and that's not safe, what are you thinking? We would need to have clearly thought about the issues…because it's certainly something that could…be questioned…by member states…and they have strong feelings about some other countries…so I think that*

would definitely be a concern (AR-5).

This echoes the comments of other interviewees who, in discussions on extraterritoriality, voice the need to ensure that data in the cloud stays within the territories of member nations (AR-6, AR-9, AR-10, AR-11, IT-1). Political borders and international relations thus play a role in the deployment of cloud computing. In the example provided by AR-5, the member states of international organizations could, for political and/or security-related motivations, challenge initiatives to adopt cloud computing. Moreover, as discussed in the previous section, the locations of data storage and transmission in a cloud computing model could, in both perceived and real ways, pose a jurisdictional threat to an organization's data, and therefore to international organizations.

4. Conclusion

The interviews offer an insight into the experiences and perceptions of archivists, records managers, and information technology staff on the adoption and employment of cloud computing in international organizations. A picture emerges revealing that factors which render cloud computing attractive for international organizations are the same features perceived to pose significant risks. These can act as barriers to the adoption of the technology within typically security- and privacy-conscious international organizations. The findings also highlight organizational issues that suggest the lack of a coordinated approach to the adoption of cloud computing, especially between various units and between different types of professional experts within organizations. In particular, archivists and records managers are often left out of the process of cloud computing implementation, and there is also a lack of governance frameworks and policies that address the fundamental shift in the service model for managing, processing and storing records and for carrying out various business functions.

As a consequence, the attendant legal, organizational, security, privacy, human, and technological issues that arise along with the technology need to be addressed. These include the risks to inviolability and the jurisdictional immunities of international organizations, both principles which, while constituting an essential aspect of the distinct character and status of international organizations, are often not well-enough considered, understood, or addressed in relation to the outsourcing of records to third parties. Many of the concerns raised regarding the immunities of international organizations revolve around the jurisdictional and legal uncertainties posed by the distributed and virtualized nature of cloud computing. Legal issues intersect with matters of ownership, custody, integrity of records and information, and trust in third-party services. In response to these complex challenges, which clearly require a multi-disciplinary approach, archivists, records

managers and information technology professionals have much to offer and to gain, both from working together and with other staff, and from pro-actively offering their concerns and expertise as part of the adaptation process, as evidenced by interviewees' recommendations, experience, and sensitivity to the issues at stake.

References

Dikker-Hupkes, S.D. (2009). “Protection and Effective Functioning of International Organizations.” Universiteit Leiden.