InterPARES Trust Project Research Report

Title:		Literature Review for Transnational Team 01: Cloud Computing for Records Management Purposes in International Organizations
Status:		Draft (restricted)
Version:		2.0
Date submitted:		10 November 2016
Last reviewed:		15 October 2016
Author:		InterPARES Trust Project
Writer(s):		Eng Sengsavang, NATO Elaine Goh, University of British Columbia Darra Hofman, University of British Columbia Elissa How, University of British Columbia Samuel Michelson, University of British Columbia Maggie Hunter, University of British Columbia Lucas Damer, University of British Columbia With contributions from former GRAs: Emily Chicorli & Taryn Jones
Research domain:		Legal
URL:		

Document Control

Version history			
Version	Date	By	Version notes
1.0	6 May 2016	Darra Hofman, Elissa How	Draft literature review
2.0	15 Oct 2016	Eng Sengsavang	Finalized literature review

Contents

Introduction 2
LITERATURE REVIEW
Cloud Computing 4
Archives and Custody 8
International Organizations: Records Management and Archives 8
Risk Management 12
Legal Challenges in The Cloud 14
International Organizations: Legal Status, Privileges, and Immunities 14
Extraterritoriality: Inviolability and Extraterritorial Jurisdiction 18
Data Localization and Privacy Legislation 23
Cybercrime 28
Conclusion 30
References 31

Introduction

International organizations (IOs) must manage substantial amounts of sensitive, often confidential records in a frequently ill-defined, cross-border legal space, while contending with the resource challenges common to all organizations, including limited space, time, and money. Many organizations and institutions have addressed these issues by outsourcing records and information infrastructure to the cloud; indeed, the United

Nations (UN) has encouraged both governments and businesses in middle and low income countries to leverage the benefits of cloud technology (United Nations, 2014). This is not, however, as straightforward a choice as it may seem. Cloud computing, and particularly cloud-based records management, offers risks and benefits that differ from those associated with even digital records management on local servers. For example, issues of data protection and privacy, cybercrime, access, data ownership, and liability must be considered by any organization using the cloud for records management.

For international organizations, however, cloud computing is further complicated by their unique legal situation. International organizations' records and archives are typically extraterritorial, in both senses of the word.[1] However, there is little understanding of how, or even if, IO archives remain inviolable when hosted in the cloud, nor is there significant discussion of the risks and benefits of cloud computing for records management specific to international organizations. Despite the lack of considered examination of the risks and challenges, international organizations, and sometimes even business units within IOs, are nonetheless moving forward with storing their records in the cloud. A review of the literature highlights that the situation facing international organizations using the cloud is fraught, and that defining best practices will require sophisticated archival, technical, and legal research to understand the drivers, barriers, and consequences of international organizations entrusting their archives to the cloud.

[1] As discussed *infra*, "extraterritoriality" is a complicated legal term; with regards to the archives and records of International organizations, its two primary meaning are "inviolable" and "outside the control of a jurisdiction," and both meanings can apply to IO archives and records.

LITERATURE REVIEW

Cloud Computing

The first challenge of understanding cloud computing as a records management strategy for international organizations is to understand cloud computing. The National Institute of Standards and Technology defines “cloud computing” as:

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011, p. 2).

However, this definition is "not universally accepted any more than any other definition" (De Filippi & McCarthy, 2012, p.2). Duranti & Jansen define “cloud computing” in terms of its “essential characteristics,” which include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (2013, p. 161). Some articles usefully contain glossaries of terms and definitions related to cloud computing (Vaile et al, 2013; International Standards Organization and International Electrotechnical Commission (2014), *ISO/IEC 17788*; Millard, 2013) and overviews of cloud computing including categories, characteristics and related activities (ISO and IEC (2014), *ISO/IEC 17788*). One particularly detailed example, the Cloud Computing Reference Architecture (ISO and IEC (2014), *ISO/IEC 17788*; Liu, et al., 2011), seeks to “accurately communicate the components and offerings of cloud computing [through a] vendor-neutral architecture” (Liu et al., 2011, p.vi). Mackay, et al., envision an entirely new cloud computing platform that could serve as a trusted repository for sensitive data (2012). Ultimately, the very concept of cloud computing is dynamic.

Beyond the challenges of defining "cloud computing," the literature also grapples with the drivers of and barriers to its adoption. Indeed, Kronabeter and Fenz note that, Janus-like, many of the attributes that make cloud computing attractive also pose its greatest risks (Kronabeter, 2013). Dutta, et al., categorize the risks that organizations may encounter during cloud computing adoption, including organizational, operational, technical, and legal risks (Dutta et al., 2013). Terms and definitions are necessary to manage risk for the systematic and logical processes of cloud computing (ISO 31000, 2009).

The literature reviewed deals with legal and jurisdictional issues such as international legislation, data transiting and protection of privacy. For example, Adrian (2013) questions whether and how cloud computing infrastructure could support privacy legislation. The ongoing development of cloud computing contracts and common characteristics of such contracts is also an important component of cloud computing service models (Burden, 2014). Service level agreements (SLAs) are often the first and only level for customers to establish relationships with cloud providers; however, it is not necessarily clear who owns the data processed in the cloud, and the attendant metadata (Bushey, 2013). McClelland, et al., examine the records and information management (RIM) landscape in the context of cloud services, and provide a list of contract terms that should be addressed in cloud service provider contracts (2014). Other business models for cloud computing are also discussed (Millard, 2013).

Various jurisdictions approach cloud computing differently, and even within jurisdictions, the law is in flux. Several authors consider a diversity of issues that are impacted by cloud computing, including the territorial scope of the EU Privacy Directive and the EU Data Protection Regulation (Kronabeter, 2013; Millard, 2013), the impact of international legislation (Gray, 2013; Millard, 2013), the applicability of the European Data Privacy Directive (Kong, 2010),[2] harmonization between member states and data flow outside of the European Union (Gray, 2013; Kong, 2010), data sovereignty (Vaile et al., 2013), and the lack of international consensus about what laws would work for data flow (Kong, 2010). Gray considers the protection of privacy in various contexts (2013). Finally, DeFilippi & McCarthy highlight how easily national data protection laws, discussed in more detail *infra*, are circumvented (2012).

Among the many legal issues surrounding IO recordkeeping in the cloud, territoriality is a recurring and critical issue. Data "does not have any nationality but merely inherits the law of the territory in which it is located" (De Filippi & McCarthy, 2012, p. 8). Data, however, can flow into and through several territories with ease and the same data can thus be subject to multiple national laws at the same time. When data is held by a third party either within the same or in another territory as the creator or user, data sovereignty is limited (De Filippi & McCarthy, 2012). The EU features prominently in the research to date, but international organizations exist and work throughout the world, and thus issues of territoriality in cloud computing recordkeeping must be understood well beyond the EU.

Particular research is needed into limitations on the cloud imposed by legislation within jurisdictions. Such limitations are poorly understood and can be problematic, such as EU prohibitions on external data flow that have led to the assertion that there is "an iron curtain on transfer of data" (Kong, 2013, p. 443). At the same time, transborder data transfers lack adequate supervision, and "due to uneven data protection levels in national

[2] To be superseded by the General Data Protection Regulation

sovereignties, data protection has become a major obstacle to free global data flow" (Kong, 2012, p. 442). The issues of data protection continue to be highly problematic, and while there is a discussion of the extant literature concerning these issues *infra*, there is a dearth of literature on this issue that is informed by an awareness of the specific case of international organizations.

In addition to the research considering specific legal issues regarding recordkeeping in the cloud, there is some literature which examines broader policy and regulatory approaches and implications. Policy and regulatory approaches undertaken by governments in developing countries to capitalize on the benefits of cloud computing are explored by the United Nations Conference on Trade and Development (2014). Policies and frameworks for determining liability are discussed in Kronabeter (2013). Lipinski (2013) considers the role of the court's discretion in interpreting the contracts and terms of service (TOS) governing cloud computing service agreements.

Ultimately, there is an urgent need for research into cloud computing and international organizations' recordkeeping. While the literature identifies and traces a number of issues, discussed *supra,* none of those issues are fully developed and understood. Identifying the types of terms and gaps that exist in contracts between providers and clients across multiple jurisdictions remains a pressing issue (InterPARES Trust Project). Furthermore, records and information management concerns specific to international organizations' use of cloud computing necessitate further research regarding specific challenges, opportunities, and best practices in that context.

Archives and Custody

In many ways, the challenges facing archivists and records managers in the cloud environment are eternal ones: how to ensure that records remain trustworthy, accessible yet at the same time secure and disclosed only to the right parties, and how archivists should view their roles and responsibilities, both at an organizational and societal level. Much of the literature addressing these issues in the digital, and particularly cloud, context, focuses on custody. This is logical, because digital records, particularly digital records consigned to the cloud, allow for fragmented custody in a way that was simply impossible with physical records. As Cook (2007) notes, “we are not producing, managing, and saving physical things or artifacts, but rather trying to understand and preserve the logical and virtual patterns that give electronic information its structure, content, and context, and thus its meaning as a ‘record’ or as evidence of acts and transactions (p.207). Indeed, the case of records management in the cloud is in some ways the case of the most fundamental archival questions, questions about the meaning and role of custody, about control of records, and about balancing ideal practices against realties of finite resources, writ large.

International Organizations: Records Management and Archives

The specific case of records management in cloud computing within international organizations receives fairly narrow treatment within the literature. Even within the small amount of existing literature, however, a breadth of issues is raised that require further research and understanding. Of the four texts reviewed which focus on records management and archives within international organizations, three address archives and records management in the United Nations (Biraud, 2013; Callejas & Terzi, 2012; United Nations Secretariat, 2007), while one examines the European Commission.

An expository bulletin issued by the United Nations General Secretariat in 2007 outlines the responsibilities of staff, work units, and the Archives and Records Management Section (ARMS) in the Secretariat for the creation, management, and disposition of records. The bulletin also outlines procedures for access to UN archives and non-current records. The mandate of ARMS is to establish relevant policies and guidelines for the management of records and archives, including electronic records. One of the responsibilities of ARMS is to develop procedures for the "appropriate identification, handling and management of sensitive records" (p. 4).

However, a critical report by Gérard Biraud for the United Nations Joint Inspection Unit in 2012 notes the lack of a unified approach to records and archives management across UN entities, leading to variations in regulatory frameworks within the UN. Moreover, Biraud finds that disparate policies are neither supported by provisions to carry out the work that is mandated, nor accompanied by practical guidelines and clarity regarding corporate roles and responsibilities.

Biraud's report further notes that RAM units fall within a variety of divisions or departments, including management, knowledge management, or information technology, indicating "the absence of any clear or common vision on where such functions belong" (p. 25; see also Annex IV). Additionally, there is a lack of integration amongst the above-mentioned information management functions (p. 29). Compounding the issue, records and archives management is perceived as having secondary importance, a status partially attributed to the recruitment of chiefs of archival units within middle management rather than senior management.

Biraud's report observes two emerging models for records and archives management in the UN. The first is a centralized approach consisting of a dedicated corporate unit staffed by professional archivists and records managers. The second model is a decentralized approach characterized by corporate stakeholders, such as administrative and information technology divisions, among others, that undertake RAM functions. The second, decentralized approach is the predominant model in UN funds and programmes. Fourteen records centres support recordkeeping for UN missions, yet these centres handle only paper records, while digital records are managed by information technology units.

Biraud's report is particularly relevant to the questions surrounding the role of cloud computing and extraterritoriality for international organizations. Biraud's finding that there is currently no cohesive digital recordkeeping and preservation strategy reflects the fragmentation and general uncertainty that digital records have brought to the fore; that fragmentation and uncertainty extends to the legal rights and obligations of international organizations' archives and records processed in the cloud. Biraud's conclusion that the use of remote and collaborative digital platforms underscores the need for an overarching policy framework to unify various RAM approaches and implementations across UN entities applies to many international organizations.

A report authored by Callejas and Terzi (2012) for the UN Joint Inspection Unit identifies similar issues surrounding the adoption of cloud computing. The purpose of the report is to outline recommendations on the adoption of ERP systems, noting that the transition to one system is not an information and communication technology (ICT) project, but rather a "major business transformation" (p. 8). On the topic of cloud computing, the report acknowledges that, "Cloud-based software implementation can be seen as problematic by some United Nations system organizations due to security and data confidentiality concerns" (p. 16). At the time of the report in 2012, UN-Habitat was negotiating to procure a cloud-based system for project management while waiting for Umoja, an enterprise resource planning (ERP) system, to be implemented. There is brief mention of other international organizations and their experiences with ERP systems, including cloud computing. In particular, the experiences of the IMF and World Bank are highlighted; their divergent approaches highlight the need for more research in this area to promote greater understanding of the potential issues at play. Paragraph 128 of the report states that, "while some organizations like the IMF consider public cloud solutions to be like any third party hosting solutions, others, such as the World Bank, have security and data confidentiality concerns regarding commercial clouds" (p. 30).

Turning from the United Nations, a 2010 Commission Communication to the European Parliament, as part of the Digital Initiative for Europe within the Europe 2020 Strategy, focuses on interoperability of communication software between Member States of the European Commission. The study provides some insight into why cloud computing is difficult to initiate within international organizations. Difficulties outlined in the Communication include: the different legal landscapes among Member States, lack of common infrastructures, multilingualism, and lack of agreement on the format of information. Overall, the aim of the document is to instill in Member States the benefits of developing interoperable communication technologies with their counterparts.

The diversity of issues and approaches found in the reviewed materials highlights the current lack of consensus regarding recordkeeping even within a single international organization, particularly where digital records and cloud computing are concerned. They also highlight the need for further research into these issues, to arrive at both a fuller understanding and a sense of potential best practices regarding the use of cloud computing for international organizations.

Risk Management

In deciding for or against the use of cloud services, records managers and other information professionals in international organizations must make informed decisions based on the potential risks and benefits to their organizations. While a full understanding of those risks and benefits must be based on specialist knowledge, including archival and legal knowledge, it should also be informed by the relevant literature on risk management. While risk management as a whole is a broad field with rich technical knowledge of its own, applicable principles can be gleaned that help provide a framework for evaluating the drivers and barriers to cloud computing adoption. Risk itself is "the consequence of an organization setting and pursuing objectives against an uncertain environment" (Purdy, 2010, p. 882). Cloud computing has opened up a new world, in which the technology can both enable organizations to pursue their objectives while creating the uncertainty that must be managed:

> Information and communication technologies (ICT) have over several decades brought significant benefits to enterprises, individuals, and society as a whole. This is clearly evident when considering the wide and profound impact of the Internet in a great many parts of our daily lives. The Internet, and more broadly cyberspace, has become a cornerstone for a broad range of services and activities that today we take for granted. Due to cyberspace and its underlying infrastructure, people and organizations have access to more and better services than ever before. […] As a result, our daily lives, fundamental rights, economies,

> and social security depend on ICT working seamlessly. At the same time, cyberspace has introduced, and continues to introduce, numerous new threats and vulnerabilities (Refsdal, et al., 2015, p. v).

The literature addressing risk management of cloud computing for records management raises a multiplicity of issues, models, and approaches. Approaches addressed include Continuous Risk Management (Dorofee, et al., 1996) and information flow control (Bacon, et al., 2013). A significant amount of the literature considers the complexities and management of perceived risk, "the degree to which the consumer feels the uncertainty and consequences associated with their actions and play a critical role in consumer decision-making" (Chen, et al., 2010, p. 1608; Slovic, 2000; Slovic, et al., 1982; Stone & Gronhaug, 1993). In particular, the literature examines the factors behind perceived risk (Dowling & Staelin, 1994), the role of intangibility in perceived risk (Eggert, 2012), and the perceived risk at the organizational level (Mitchell, 1995; Munnukka, 2014). The differentiation between risk and perceived risk, and the impact upon organizational decision-making is a useful intellectual tool for understanding the factors at play in decisions to adopt cloud computing in international organizations.

Perhaps the most directly on-point risk management article is McKemmish's "Recordkeeping and archiving in the cloud. Is there a silver lining?" In this article, McKemmish examines the developments regarding records management in the cloud in the National Archives of Australia (NAA), the Public Record Office of Victoria, and the Cloud for Europe initiative. Particularly instructive is McKemmish's discussion of the NAA's model for risk assessment, including its *Check List,* risk categories, and checklists for Australian governmental organizations putting their records in the cloud. However, this article is primarily focused on the Australian public recordkeeping context, which is wedded to the continuum model, and requires further research to be generalized to the case of international organizations.

Legal Challenges in The Cloud

Equally important to understanding the adoption of cloud computing by international organizations for their archives and records management is the legal context in which these decisions are undertaken. While books can be and have been written about law and the cloud, several issues of particular importance to international organizations using cloud services for their records must be highlighted. Firstly, the unique legal status, privileges, and immunities of international organizations and their archives must be understood. International organizations exercise a legal independence afforded few other entities, embodied in the specific privileges and immunities of an IO and flowing from the legal instruments creating and empowering that IO. In particular, the archives of international organizations are often the subject of extraterritoriality, both in the sense of being inviolable, and in the sense of being outside the territory (and jurisdiction) of a particular entity.

International Organizations: Legal Status, Privileges, and Immunities

Several major themes emerge regarding the legal status, privileges and immunities of international organizations in the context of archives and records. The threshold issue is simply defining what is meant by an "international organization." A second issue is understanding the legal relationship between an international organization and its host country(ies), and defining the sources of international organizations' privileges and immunities. Finally, it is necessary to understand the specific privileges and immunities that surround international organizations' archives and records, and to define their boundaries, applications, and exceptions. This complex legal landscape means that a number of sources of law and legal instruments must be considered in determining the status, privileges, and immunities of any particular international organization.

The initial challenge is simply identifying what qualifies an organization as an "international organization." Muller (1995) defines an international organization according to three principles: it must be established by an international agreement; it must have its own, separate organs; and it must be established under international law (p. 4). Abass presents a table, "Typologies of international organizations," and asserts that the best definition of international organizations is articulated by the International Law Commission (ILC), which acknowledges that public IOs may be established by other instruments besides treaties, and may have non-State members (2014, p.159). Bekker (1994) notes that there is an indefinite variety of international organizations, which are extremely diverse in both nature and size, and that such "diversity has an impact upon both the legal status of intergovernmental organizations and the immunities they require" (p. 41-42). Diaz-Gonzalez (1985) begins his text by tying his understanding of what constitutes an "international organization" to the language of the United Nations, in which "'international organization' refers to intergovernmental, rather than non-governmental, organizations" (p. 106).

Once a definition for an "international organization" is arrived at, one must confront the substantive issues concerning the legal status of international organizations, including the legal personality, legal capacity, and privileges and immunities of IOs. Abass provides a detailed discussion of how legal personality is derived and how it operates. In the case of the latter, legal personality enables international organizations to function on their host states' territories and in domestic contexts (2014, p. 167). Related to legal personality is legal capacity, which allows international organizations to hold property, enter into contractual agreements, and exist as juridical entities before courts, among other activities (Abass, 2014, p.167-68). Diaz-Gonzalez states that although the first subjects of international law were States, international organizations are also now recognized under international law (1991). The possession of legal personality means that international organizations have an identity separate from their members, and leads to "two sets of consequences: the capacity to exercise certain powers; and the enjoyment of certain rights and privileges" (Diaz-Gonzalez, 1991, p. 174). In an older work, Diaz-Gonzalez explains that legal personality is important because it enables "the freedom of action essential to an international organization in order for it to carry out with complete independence the functions assigned to it" (1985, p. 136).

The "independence" assigned to international organizations is manifested in the form of privileges and immunities, which in turn derive from the principle of functional necessity (Miller, 2009). Jenks states that the law of international immunities has arisen out of a need to specify the "functional needs" of international organizations (1961, p. xxxviii). This functional necessity approach states that the immunities and privileges of an international organization are accorded to it on the basis of its functions and purposes (Bekker, 1994). Bekker clarifies that "it is not by consequence of an organization's personality but by consequence of the needs arising from its purposes and functions that an international organization enjoys or is entitled to enjoy certain privileges and immunities. This is the essence of the *functional* approach" (1994, p. 96-97).

According to Jenks, although the literature on the law of international immunities can be traced back to the nineteenth century, it remained largely undeveloped until the end of the Second World War (1961, p. 1). Post-World War II, which saw the proliferation of international organizations, scholars and lawmakers were required to distinguish between diplomatic immunities and international immunities. It became standard for the enabling instruments of international organizations to contain provisions conferring certain immunities on organizations themselves, as well as representatives of their member states and employees. These constitutions, adds Jenks, "are supplemented by headquarters and host agreements" with the states where IOs are located (1961, p. 3). Muller deals with this topic extensively in his text *International Organizations and their Host State*, whose "object is to define *how* and in *what context* the legal relationship between the two entities is regulated" (1995, p. 14).

According to Abass, international organizations possess four types of privileges and immunities: "jurisdictional immunity, inviolability of premises and archives, freedom of communication, and immunity relating to financial matters" (2014, p. 191). Hupkes provides a "diagram of categories of privileges and immunities" (2009, Figure 2, p. 24). The inviolability of premises and archives falls under the category of immunities of the organization itself, rather than that of persons under the organization (*Id.,* p. 24). The same author acknowledges that although they are often articulated in the same articles, "the inviolability of 'objects' like archives, property, funds and assets of an IO must be seen as separate privileges" from the inviolability of premises (*Id.,* p. 48). Similarly, Jenks provides a summary account of the inviolability of international organizations in three parts: inviolability of premises; inviolability of property and assets; and inviolability of archives (1961). Diaz-Gonzalez (1991) states that the purpose of inviolability is to enable "privacy and the preservation of secrecy," which is at the foundation of the independence of IOs, and is required for the fulfillment of their purposes (2014, p. 99).

Hupkes examines the development of diplomatic and organizational immunities, noting that there are both differences and similarities between the two situations. Notably, the privileges and immunities of international organizations evolved and draw from those of diplomatic missions. However, the law of international organization immunities is no longer predicated on the theory of diplomatic immunities but "has become a complex body of rules set forth in detail in conventions, agreements, statutes, and regulations" (Jenks, 1961, p. xxxv). Instead, it exists at the confluence of functional necessity and negotiated agreements with host countries, and is thus extraordinarily difficult to speak about in generalities.

Extraterritoriality: Inviolability and Extraterritorial Jurisdiction

Extraterritoriality is perhaps one of the best examples of the complexity of the legal status of international organizations, and of the changes over time and across contexts in legal understanding and application. Extraterritoriality is challenging because it is used to signify two separate concepts: diplomatic immunity and extraterritorial jurisdiction. Furthermore, the legal theory underpinning extraterritoriality (in the sense of diplomatic immunity) has changed over time, and there is significant confusion about the contexts and circumstances in which extraterritoriality applies. Because of both its complexity and its centrality to the inviolability of the archives, extraterritoriality must be understood if the larger questions of international organizations putting records and archives in the cloud is to be understood.

The Oxford Dictionary of Law defines "extraterritoriality" as "A theory in international law explaining diplomatic immunity on the basis that the premises of a foreign mission form a part of the territory of the sending state." Thus, as explained in further detail below, the concept of extraterritoriality is linked to the concept of diplomatic immunity and, indeed, is considered one of the justifications for diplomatic immunity. Such a definition is supported in non-legal definitions such as the Encyclopaedia Britannica, which explains that "extraterritoriality" is "…also called exterterritoriality, or diplomatic immunity", and represents, "in international law, the immunities enjoyed by foreign states or international organizations and the official representatives from the jurisdictions of the country in which they represent." This introductory definition is significant for two additional reasons. The first is that it is distinct in law from the more commonly discussed principle of extraterritoriality tied to the concept of extraterritorial jurisdiction; and, second, extraterritoriality is tied to the concept of diplomatic immunity with respect to states and not exclusively (or even specifically) to that of IOs. However, because both "extraterritoriality" and "extraterritorial jurisdiction" pose significant issues for IOs looking to use the cloud for their records and archives, the relevant literature for both meanings must be considered.

The meaning of "extraterritoriality" more directly relevant to international organizations' archives and records, that of diplomatic immunity and inviolability of the archives, is problematic. Extraterritoriality (also called exterritorality), one of the three traditional arguments for diplomatic immunity, has largely been rejected as a legal fiction in favor of “functional necessity” (discussed *supra*) (Ahluwalia, 1964). Secondly, there is a strong argument in the literature that “extraterritorality” per se does not apply to international organizations: “…the theory of exterritoriality is not applicable [to international organizations]: besides the fact that also in relation to diplomatic missions the theory is seen as obsolete, for IOs it lacks relevance simply because they don’t have territorial rights like states do” (Dikker Hupkes, 2009, §4.2). However, this does not mean that there are not important principles of immunity and inviolability that relate to IOs. There are significant issues to be understood regarding the inviolability of the archives of IOs in the context of the cloud; however, the literature is largely silent on these issues, and further research is urgently needed.

A majority of the literature on extraterritorial jurisdiction approaches the subject from the point of view of states (Ascensio, 2010; Currie & Scassa, 2011; Hildebrandt, 2013; Kuner, 2010; Suda, 2013). The extraterritoriality of data itself in cyberspace is addressed in some texts, while the extraterritoriality of international organizations (IOs) is often dealt with in the context of the legal status, privileges and immunities of IOs. Extraterritoriality is generally understood within the domain of international law as either a type of immunity or a type of jurisdictional reach beyond normal state powers. Suda, taking the latter understanding, defines extraterritoriality as "direct [state] authority over entities in foreign jurisdictions" (2013, p. 775).

Many authors examine the problematic nature of applying extraterritoriality laws in the sense of extraterritorial jurisdiction, citing the uncertainty for businesses in knowing to which laws they must adhere, the various meanings in different jurisdictions, expansive interpretations of legal instruments that lead to increased jurisdictional scope (Kuner, 2010), and the challenges of enforcing extraterritorial jurisdiction (Svantesson, 2015). Coughlan describes cases in Canadian law when it is unclear where jurisdiction lies, or where multiple jurisdictions may apply, while Kuner (2010) notes that “the term ‘extraterritorial jurisdiction’ appears to have different meanings in different legal systems” (Kuner 2010).

Several authors analyse extraterritoriality starting from the concepts of territoriality and jurisdiction (Berry & Reisman, 2012; Currie, Hildebrandt, 2013; Miller, 2009; Narayanan, 2012; Ryngaert & Zoetekouw, 2014; Svantesson, 2014;, Swanson, 2011). Some authors posit that jurisdiction can be independent from territory (Hildebrandt, 2013; Miller, 2009). Hildebrandt notes that the potential for jurisdiction to be independent from territory has implications for cyberspace, citing authors such as John Perry Barlow, David Johnson and David Post, who perceive that cyberspace is not a physical space. Hildebrandt argues that concepts of geographical borders and territorial jurisdiction are not applicable in cyberspace, since the "effects of any particular behaviour" "restricted by physical proximity [do] not hold" (2013, p. 202). This observation highlights the challenge cyberspace poses to the territorial nature of jurisdiction.

How to resolve the issues of territoriality and the cloud remains an open question. Several authors assert that cloud computing models are also “location independent” (Berry & Reisman, 2012). For example, Ryngaert & Zoetekouw assert that an entirely territorial model for extraterritoriality would have difficulty addressing crimes that occur solely online (2014). Examining the historical background to “jurisdictional alternatives to territory” and the challenges that virtual communities pose to territoriality, they conclude that the Internet presents unique issues that may “necessitate a paradigmatic shift in how we conceptualize spatiality…and the exercise of jurisdiction.” (*Id.,* 2014, p. 18). Andrews and Newman argue along the same lines as Ryngaert & Zoetekouw, finding that the cloud has revolutionized territorial law and that “from a legal perspective, the cloud embodies a new template for interactions” (2013, p. 327) Narayanan goes so far as to endorse a data protection framework structured similarly to the international laws of the sea, wherein data involved in transborder flows would be considered to be under no jurisdiction (2012).

Not all scholars agree, however, that cyberspace is beyond territory. Julie Cohen rejects the distinction between physical space and cyberspace, viewing humans as embodied beings who comprehend even the virtual through embodied experience, perceiving a "rich variety of entanglements between virtual and physical spaces that are real to the extent that they generate real consequences" (2007, p. 203). Currie & Scassa (2011) explore how the principles of territoriality continue to be applicable to the Internet; they ultimately envision supranational governance of the Internet. Several authors attempt to offer solutions to issues of extraterritorial jurisdiction in cloud computing or on the Internet (Andrews & Newman, 2013; Currie, 2006; Hildebrandt, 2013; Narayanan, 2006; Rynaert & Zoetekouw, 2014). Cross-border data transfers have led to a renewed consideration of extraterritorial rights (Couglan, et al., 2006). Clearly, cloud computing poses significant legal problems with regards to jurisdiction, but the law has yet to catch up with technology (Andrews & Newman, 2013).

Extraterritoriality is also addressed from the point of view of data protection and privacy issues, especially by Kuner (2009, 2014). Kuner finds EU data privacy law (under the old Data Privacy Directive) to be particularly problematic: it is “cumbersome, expensive, slow,” and “sends the wrong message to third countries” (2009, p. 263). Kuner finds that extraterritorial claims are unreasonable, as businesses and individuals cannot be expected to modify their online behaviour simply to comply with all data privacy laws in all jurisdictions (Kuner, 2014). Svantesson (2014) makes a comparable observation when describing a ‘conundrum’ of extraterritoriality in data privacy law: while it is ‘reasonable’ for states to protect data from foreign interference, it is ‘unreasonable’ to expect Internet users to comply with every state law worldwide. Yet jurisdictional grounds for EU data protection laws exist, as do extraterritorial claims in several data privacy laws worldwide (Svantesson, 2014).

Data Localization and Privacy Legislation

Data localization (also referred to in various sources as data sovereignty, data nationalism, or data protectionism) requires data to remain within the physical boundaries of the country where it originated. As of 2012, 89 states worldwide had enacted data localization legislation (Greenleaf, 2012, p. 68). Many states recognize that the right to control one’s data “is a value that lies deep in the desires of the human person and affects the dignity and integrity of that person” and, in fact, privacy was recognized by the United Nations General Assembly in 1948 as a human right in article 12 of their Universal Declaration of Human Rights (Kirby, 2011, p. 12). Furthermore, the need to protect privacy clearly is linked to data protectionism, since “the main reason for the enactment of transborder (or cross-border) data flow regulation has been to ensure data protection rights and protect privacy" (Kuner, 2013, p. 138; Poullet, 2007, p. 142).

The need to balance privacy and transborder data flows has become especially complicated in today's increasingly cloud-based digital world. Technological benefits are not without benefits, certainly, and we need to recognize that the uses of the data collected – especially Big Data – can lead to unexpected analytical breakthroughs from which "…individuals, businesses, and societies benefit enormously" (Cate, Cullen, & Schonberger, 2013, p. 8). Nonetheless, despite this benefit, Hon. Micheal Kirby, the chair of the expert group that created the influential OECD Guidelines on Privacy in 1978-1980, reminds us that "…uncritical technological euphoria is not a proper response to the challenges to privacy presented by new technology and the shifting public use of it" (Kirby, 2011, p. 13). As a result, as noted by Wiebe, the need to balance the human right of privacy against ease of communication on the internet (Hague Convention on Private International Law, 2010, p. 7) crosses different areas of the law and the distinction between private and public law has becomes less clear as a result (Wiebe, 2014, p. 64).

It is also clear that different jurisdictions approach privacy differently, a further confusing factor when organizations, and especially international organizations, consider moving to the cloud. For example, Bajaj notes a pattern of sorts for privacy regulation development – from self-regulation that result in codes of practice to privacy standards and through to privacy laws (Bajaj, 2012, p. 132). Today, there remains very different data protection approaches in different states that is due, at least in part, to different cultural, historical, and legal attitudes (Kuner, 2014, p. 59). Busch, a Professor in Germany, argues that since the terrorist attacks of September 11, 2001 in the United

States, a shift occurred worldwide when considering cross-border data traffic. Up to that point, there had been a focus on commercial interest, but after 9/11, the focus shifted to security. This shift has further resulted in regulatory differences between the United States and the European Union (Busch, 2013, p. 314). Moreover, Busch concludes that we need to keep into mind the different viewpoints of actors involved with cross-border data issues (economic, security, and civil rights interests), as well as deeply-rooted and varied perceptions on the state's role in regulating personal data. As a result, we collectively remain "…still far from achieving a unitary level of protection" (Busch, 2013, pgs. 328-329).

As a multinational team of researchers point out in their article titled "Data Protection Principles for the 21st Century," an article that considers ways to update the OECD information privacy guidelines from 1980, the issue of data crossing borders and the inconsistency of laws is not new, but the magnitude of data increases across borders has substantially expanded (Cate, Cullen & Schonberger, 2013, p. 5). Because there have been such changes in technology, and because data crosses borders so frequently, legislation has become much more international in nature - requiring legal instruments such as treaties. This is directly related to the fact that, with the advance of the spread of global technologies, "have come new problems that cross borders and are sometimes insusceptible to effective local solutions" (Kirby, 2011, p. 8). In other words, states are forced to try and have their laws extend extraterritorially to address some of these issues, and the resulting confusion of what laws might apply to what data adds to the overall confusion of privacy rights in the cloud.

Additionally, we see cases like the famous Google Spain "Right to Be Forgotten" case (Google Spain v. AEPD and Mario Costeja Gonzalez) from 2014, which supports an extraterritorial application of EU data protection law (Kuner, 2014, p. 63). Indeed, the European Union, the focus of many of the articles reviewed here, has been seen as "becoming the de facto world regulator on data protection" (Kuner, 2014, p. 57) and the EU Data Protection Directive 95/46 does have binding legal effect (Kuner, 2014, p. 58). Moreover, since 2012, the EU has undergone a process to update the Directive with the result that in Spring 2016, the EU bodies published the General Data Protection Regulation to replace the current Directive and come into force from May 2018 (European Commission, 10 Oct 2016). The General Data Protection Regulation expands on the extraterritorial scope of its predecessor by including explicit rules requiring EU data protection laws to apply to goods and services consumed by EU citizens wherever they are located (European Commission, 2016). Nonetheless, the extraterritorial effects of this new legislation remain to be seen. In the meantime, expansive differences between states exist, with the EU standard being precise and specific and the American one based more on self-regulating the free market, as well as being segmented and sector-based (Marchinkowski, 2013, 1183-1184).

In addition to recognizing the different approaches to privacy worldwide, any organization considering accessing or storing information in the cloud needs to appreciate the inherent tension in cross-border data flows, which sees data frequently crossing borders, against the ongoing reality that legal systems tend to be based on territory. Thus, one of the challenges that arises is that data protection regulations take traditional approaches to legal rights based on physical location, so that today, data "carries a burden that ‘runs with it’ and binds third parties through remedies that have developed through a grounding in “property rules” (Victor, 2013, p. 515). Busch notes that there is a crucial tension in the very nature of the Internet given that, while it might have been set up with “utopian ideas about the new medium” to improve world liberty, there remains an undeniable “tension between a communication structure designed and implemented to be global, and the largely territorially-based rules of nation states and international organisations” (Busch, 2013, p. 316). Unfortunately, there remains little harmonization of legislation across borders, and this leads to challenges for individuals, companies, and data controllers alike (Kuner, 2014, p. 55).

As noted, such problems are magnified when using the cloud. Some have even argued that this notion of location has become irrelevant in cloud computing and that “…what matters most in not where information is stored, but who can read it, i.e. who is able to obtain access to it in intelligible form”(Hon & Millard, 2012, p. 53). As a result of the disconnect between the way we currently use data and our traditional approaches to data protectionism, what has happened is that “…the current European approaches towards transborder data flows are not working effectively” (Kierkegarrd, 2011, p. 233). Put another way, this European regulatory approach can be seen as “…cumbersome, expensive, slow” (Kuner, 2009, 263). Similar views are expressed by Koops (2014), who argues that European laws often are not assisted by the myriad of laws around them, at least in part because there is no single data protection framework but instead, a multiplicity of regulatory frameworks (p. 14). Still other legal commentators suggest that this very issue makes it difficult in a practical sense for some businesses to operate across borders (Svantesson, 2013, p. 278), and leads to the reality that many small- and mediumsized enterprises “likely ignore the restrictions on cross-border data transfers either altogether or to a large extent” (Parker, 2012, p. 7).

Cybercrime

Finally, keeping records in the cloud also has implications for the investigation and enforcement of crimes, including those committed by or against international organizations. The literature highlights two primary issues associated with cybercrime and the cloud: enforcement (Cybercrime Convention Committee, 2012) and jurisdiction (Spoenle, 2010). Territoriality (Spoenle, 2010; Cybercrime Convention Committee, 2012), specifically the inability to determine the jurisdiction of data and the need to establish jurisdiction in order not to violate “territorial sovereignty” (Spoenle, 2010), raises a number of questions for international organizations whose data might be targeted by criminal enterprises. Legislative issues relating to data in the cloud include the inadequacies of existing legislation to address cybercrime (Spoenle, 2010), the lack of implementation of existing legislative schemes (Cybercrime Convention Committee, 2013), the need for legislative clarification (NIST), conflicting international laws (Cybercrime Convention Committee, 2012), and the lack of clear territoriality which interferes with procedural actions (Spoenle, 2010; Cybercrime Convention Committee, 2012).

Cloud computing has engendered challenges in the fight against cybercrime, such as increased difficulty in the acquisition of evidence (Spoenle, 2010) and other forensic challenges (NIST). The important role of power of disposal is defined as a "person having the power to alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever" (CCC 2012). Creating categories and terminology (NIST) and establishing an instrument of regulation for transborder data flow (CCC 2013) are identified as important actions to be taken. Ongoing technological changes are also noted (CCC 2013).

Conclusion

There exists a breadth of literature addressing a diversity of subtopics pertinent to the questions surrounding the adoption of cloud computing for records management by international organizations. However, there exists no literature directly addressing the drivers, benefits, risks, and barriers of IO cloud computing adoption. Archival, technical, and legal research must be undertaken to enable international organizations to navigate this space. Questions of inviolability and extraterritoriality, and how and if they apply to records in the cloud, are largely unanswered legally. Best archival practices to maintain accessible, trustworthy records in a cloud environment are still developing. And the technology underpinning all of these questions evolves at a breathtaking pace, requiring us to constantly update our practices to align principles with new means of records creation, use, access, disposition, and preservation. The breadth and depth of the applicable literature shows the complexity that records managers face in this realm; without tools to better manage the complexity, international organizations risk everything about their records, including the records themselves.

References

Adrian, A. (2013). “How much privacy do clouds provide? An Australian perspective.” *Computer Law and Security Review,* 29(1), 48-57.

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

Ahluwalia, K. (1964). *The Legal Status, Privileges and Immunities of the Specialized Agencies of the United Nations and Certain Other International Organizations and their Headquarters* (pp. 48-104). Springer Netherlands.

Al-Bakri, S.H., Shanmugam, B., Samy, G.N., Idris, N.B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. *Security and Communications Networks, 7* (21), 2114-2124.

Ascensio, H. (2010). Extraterritoriality as an instrument*. Contribution to the work of the UN Secretary-General's Special Representative on human rights and transnational corporations and other businesses.* http://www.diplomatie.gouv.fr/en/IMG/pdf/Extraterritoriality_as_a_tool.pdf

Bacon, J., Eyers, D., Pasquier, T. F. J.-M., Singh, J., Papagiannis, I., & Pietzuch, P. (2013). Information Flow Control for Secure Cloud Computing. *IEEE Transactions on Network and Service Management,* 11(1), 76 – 89.

Bajaj, K. (2012). Promoting data protection standards through contracts: The case of the data security council of India. *Review of Policy Research, 29* (1), 131-139.

Bekker, P. H. F. (1994). *The legal position of intergovernmental organizations: A functional necessity analysis of their legal status and immunities.* Martinus Nijhoff Publishers.

Berry, R., & Reisman, M. (2012). Policy challenges of cross-border cloud computing. *Journal of International Commerce and Economics, 4* (2), 1-38.

Biraud, G. (2013). *Records and archives management in the united nations* No. JIU/REP/2013/2). Geneva: Joint Inspection Unit, United Nations. https://www.unjiu.org/en/reports-notes/JIU%20Products/JIU_REP_2013_2_English.pdf

Bohaker, Heidi, Lisa Austin, Andrew Clement & Stephanie Perrin, *Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digitally Interconnected World*. [Report] (ecommunications outsourcing project, iSchool, University of Toronto), 2. September 15, 2015, accessed April 2, 2016. http://ecommoutsourcing.ischool.utoronto.ca/

Burden, K. (2014). "'Cloud bursts': Emerging trends in contracting for cloud services." *Computer Law & Security Review*, 30(2), 196-198.

Busch, A. (2013). The regulation of transborder data traffic: Disputes across the Atlantic. *Security and Human Rights, 23*(4), 313-330.

Bushey, J. (2013). Trustworthy Digital Images and the Cloud: Early Findings of the Records in the Cloud Project. In J. N. Gathegi, Y. Tonta, S. Kurbanoglu, U. Al, & Z. Taskin (Eds.), *Challenges of information management beyond the cloud: 4th international symposium on information management in a changing world, IMCW 2013, Limerick, Ireland, September 4-6, 2013. revised selected papers* (pp. 43-53). Berlin: Springer.

Callejas, J. F., & Terzi, C. (2012). *Review of enterprise resource planning (ERP) systems in united nations organizations* (No. JIU/REP/2012/8). Geneva: Joint Inspection Unit, United Nations.

Cate, F. H., Cullen, P., & Mayer-Schönberger, V. (2014). *Data protection principles for the 21st century: Revising the 1980 OECD guidelines.* Oxford Internet Institute. www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf

Choi, W. *(2006). Diplomatic and consular law in the internet age*. Singapore Year Book of International Law*, 10, 117-132.*

Clopton, Z. D. (2013). Extraterritoriality and extranationality: A comparative study. *Duke Journal of Comparative & International Law, 23*(2), 217-265.

Cohen, J. E. (2007). Cyberspace as/and Space. *Columbia Law Review*, *107*(1), 210-256.

Colket, M. *(1945)*. The inviolability of diplomatic archives. *The American Archivist, 8(1), 26-49.*

Colonna, L. (2014). Article 4 of the EU data protection directive and the irrelevance of the EU-US safe harbor program? *International Data Privacy Law, 4* (3), 203-221.

Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions: Towards interoperability for European public services (2010). (Final Report No. COM(2010) 744). Brussels: European Commission.

Coughlan, S. G., Currie, R. J., Kindred, H. M., & Scassa, T. (2006). *Global reach, local grasp: Constructing extraterritorial jurisdiction in the age of globalization (Dalhousie Law School)*. Canada: Law Commission of Canada.

Currie, R. J., & Scassa, T. (2011). New first principles? Assessing the internet's challenges to jurisdiction. *Georgetown Journal of International Law, 42*(4), 1017-1082.

Cybercrime Convention Committee (T-CY): Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data. (2012). *Transborder access and jurisdiction: What are the options?* No. T-CY (2012(3)). Strasbourg: Council of Europe. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

De Filippi, P., & Mccarthy, S. (2012). Cloud Computing : Centralization and Data Sovereignty. *European Journal of Law and Technology*, 3(2), 1–18.

Díaz-González, L. (1991). *(Consolidated) fifth report of the special rapporteur 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 1991, vol.II(1) No. A/CN.4/438 and Corr.1).* Geneva: United Nations. http://legal.un.org/ilc/documentation/english/a_cn4_438.pdf#

Díaz-González, L. (1985). *Second 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 1985, vol.II(1) No. A/CN.4/391 and Add.1). Geneva: United Nations. http://legal.un.org/ilc/documentation/english/a_cn4_391.pdf

Dikker Hupkes, S. D. (2009). Protection and Effective Functioning of International Organizations. Final Report International Institutional Law; Secure Haven project.

Dikker Hupkes, S. D. (2009). *Protection and effective functioning of international organizations (Final Report No. WP 1110).* Den Haag: Universiteit Leiden. https://openaccess.leidenuniv.nl/bitstream/handle/1887/14119/SH-Report+Protection+and+Effective+Functioning+of+International+Organizations.pdf;jsessionid=6A8A1BB0611486FDB5BFBF3A44A18A27?sequence=1

Dover, R., & Frosini, J. (2012). *The extraterritorial effects of legislation and policies in the EU and US.* Brussels, Belgium: European Parliament. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/433701/EXPO-AFET_ET%282012%29433701_EN.pdf

Duranti, L. (2007). Archives as a place. *Archives and Manuscripts, 24* (2).

Duranti, L., & Jansen, A. (2013). Records in the cloud: Authenticity and jurisdiction. *Digital Heritage International Congress, 2.* pp. 161-164.

Dutta, A., Peng, G.C.A., & Choudhary, A. (2013). Risks in Enterprise Cloud Computing: The Perspective of IT Experts. *The Journal of Computer Information Systems*, 53(4), 39-48.

Esayas, S. Y. (2012). A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data. *Computer Law & Security Review, 28* (6), 662-678.

European Commission (10 October 2016). "Reform of EU data protection rules." Retrieved 1 November 2016: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

European Commission (2016). "How will the EU's data protection reform make international cooperation easier?" Retrieved 1 November 2016: http://ec.europa.eu/justice/data-protection/files/5_reform_en.pdf

Gray, A. (2013). Conflict of laws and the cloud. *Computer Law & Security Review* 29(1), 58-65.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of convention 108. *International Data Privacy Law, 2* (2), 68-92.

Haeberlen, T., & Dupré, L. (2012). *Cloud Computing: Benefits, Risks, and Recommendations for Information Security.* European Network and Information Security Agency (ENISA).

Hague Conference on Private International Law. (2010) "Cross-border data flows and protection of privacy." Preliminary Document No. 13 of March 2010 for the attention of the Council of April 2010 on General Affairs and Policy of the Conference. https://assets.hcch.net/upload/wop/genaff2010pd13e.pdf.

Henkoglu, T. & Kulcu, O. (2013). Evaluations of conditions regarding cloud computing applications in turkey, EU and the USA. In J. N. Gathegi, Y. Tonta, S. Kurbanoglu, U. Al, & Z. Taskin (Eds.), *Challenges of information management beyond the cloud: 4th international symposium on information management in a changing world, IMCW 2013, Limerick, Ireland, September 4-6, 2013. revised selected papers* (pp. 36-42) Springer: Berlin.

Hildebrandt, M. (2013). Extraterritorial jurisdiction to enforce in cyberspace? Bodin, schmitt, grotius in cyberspace. *University of Toronto Law Journal, 63*(2), 196-224.

Hon, W. K., Kosta, E., Millard, C., & Stefanatou, D. (2014). *Cloud accountability: The likely impact of the proposed EU data protection regulation* (Research Paper No. 172/2014). London: Queen Mary School of Law Legal Studies.

Hon, W. K., Millard, C., & Walden, I. (2011). The problem of 'personal data' in cloud computing - what information is regulated? The cloud of unknowing, part 1. [Queen Mary School of Law Legal Studies Research Paper No. 75/2011] *International Data Privacy Law, 1* (4), 211-228. http://ssrn.com/abstract=1783577 or http://dx.doi.org/10.2139/ssrn.1783577.

Hon, W. K., Millard, C., & Walden, I. (2012). Who is responsible for 'personal data' in cloud computing? The cloud of unknowing part 2. [Queen Mary School of Law Legal Studies Research Paper No. 77/2011] *International Data Privacy Law, 2* (1), 3-18. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130

Hon, W. K., & Millard, C. (2012). Data protection jurisdiction and cloud computing - when are cloud users and providers subject to EU data protection law? The cloud of unknowing, part 3. [Queen Mary School of Law Legal Studies Research Paper No. 84/2011] *International Review of Law, Computers & Technology, 26* (2-3)

Hon, W. K., & Millard, C. (2012). Data export in cloud computing - how can personal data be transferred outside the EEA? The cloud of unknowing, part 4. *SCRIPTed, 9* (1), 25-63. http://script-ed.org/?p=324

International Standards Organization and International Electrotechnical Commission. (2014). *ISO/IEC 17788: Information technology - cloud computing - overview and vocabulary*. Geneva, Switzerland: International Standards Organization and International Electrotechnical Commission.

International Standards Organization and International Electrotechnical Commission. (2014). *ISO/IEC 17789: Information technology - cloud computing - reference architecture*. Geneva, Switzerland: International Standards Organization and International Electrotechnical Commission.

International Standards Organization. (2009). *ISO 31000: Risk management - principles and guidelines*. Geneva, Switzerland: International Standards Organization.

Jenks, W. C. (1961). *International immunities*. London: Stevens & Sons Limited.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I., & Saxby, S. (2011). 30 years on - the review of the council of Europe data protection convention 108. *Computer Law & Security Review, 27* (3), 223-231.

Kong, L. (2010). Data Protection and Transborder Data Flow in the European and Global Context. *European Journal of International Law*, *21*(2), 441-456.

Kronabeter, A., & Fenz, S. (2013). Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation. *Cloud Computing: third international conference,* *cloudcomp 2012, Vienna, Austria, September 24-26, 2012, revised selected papers* (pp. 114-123). Springer International Publishing.

Kuner, C. (2014). The court of justice of the EU judgment on data protection and internet search engines: Current issues and future challenges. In B. Hess, & C. M. Mariottini (Eds.), *Protecting privacy in private international procedural law and by data protection* [LSE Legal Studies Working Paper No. 3/2015] (pp. 19-55). London: London School of Economics and Political Science. http://ssrn.com/abstract=2496060 or http://dx.doi.org/10.2139/ssrn.2496060

Kuner, C. (2010). Data protection law and international jurisdiction on the internet (part 1). *International Journal of Law and Information Technology, 18*(2), 176-193. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496847

Kuner, C. (2010). Data protection and international jurisdiction on the internet (part 2). International Journal of Law and Information Technology, *18*(3), 227-247. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689495

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2013). The extraterritoriality of data privacy laws—an explosive issue yet to detonate. *International Data Privacy Law*, *3*(3), 147-148.

Law, J., & Martin, E. (2014). Extraterritoriality. *Oxford Reference: A Dictionary of Law, 7th ed*. Oxford: Oxford University Press. Online at http://www.oxfordreference.com.ezproxy.library.ubc.ca/view/10.1093/acref/9780199551248.001.0001/acref-9780199551248-e-1508?rskey=Bp77cF&result=1.

Lipinski, T. A. (2013). Click here to cloud: End users issues in cloud computing terms of service agreements. In J. N. Gathegi, Y. Tonta & S. Kurbanoglu (Eds.), *Challenges of information management beyond the cloud 4th international symposium on information management in a changing world* (pp. 92-111). Berlin: Springer.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, *500*(2011), 292.

Mackay, M., Baker, T., & Al-Yasiri, A. (2012). Security-oriented cloud computing platform for critical infrastructures. *Computer Law & Security Review, 28*(6), 679-686.

McLelland, R., Hurley, G., Collins, D., & Hackett, Y. (2014). *10 contract terms with cloud service providers.* InterPARES Trust Project.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology.

Millard, C. J. (Ed.) (2013). *Cloud computing law*. Oxford, United Kingdom: Oxford University Press.

Miller, A.J. (2009). “The Privileges and Immunities of the United Nations.” *International Organizations Law Review*, 7(1), 7-115.

Miller, S. (2010). Revisiting extraterritorial jurisdiction: A territorial justification for extraterritorial jurisdiction under the European convention. *The European Journal of International Law, 20*(4), 1223-1246.

Muller, A. S. (1995). *International organizations and their host states: Aspects of their legal relationship*. The Hague: Kluwer Law International.

Nedbal, D., Steininger, M., Erskine, A. M., Wagner, G., & Wetzlinger, W. (2014). The adoption of cloud services in the context of organizations: An examination of drivers and barriers. *Adoption and Diffusion of Information Technology (SIGADIT): Twentieth Americas Conference on Information Systems,* Savannah, Georgia.

NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory. (2014). *NIST cloud computing forensic challenges* No. Draft NISTIR 8006. USA: National Institute of Standard and Technology.

Purdy, G. (2010). ISO 31000:2009--setting a new standard for risk management. *Risk Analysis, 30*(6), 881. doi:10.1111/j.1539-6924.2010.01442.x

Record-keeping and the management of United Nations archives (2007). (Secretary-General's bulletin No. St/SGB/2007/5). Geneva: United Nations Secretariat. https://archives.un.org/sites/archives.un.org/files/ST_SGB_2007_5_eng.pdf

Refsdal, A., Solhaug, B., Stølen, K., & SpringerLINK ebooks - Computer Science. (2015). *Cyber-risk management* (1st 2015.;1st 2015; ed.). DE: Springer International Publishing. doi:10.1007/978-3-319-23570-7

Ryan, P. & Falvey, S. (2012). Trust in the clouds. *Computer Law & Security Review, 28*(5), 513-521.

Ryngaert, C., & Zoetekouw, M. (2014). The end of territory? The re-emergence of community as a principle of jurisdictional order in the internet era. *The Future of the Past – the Nation State, the Notion of Sovereignty, Territory, Diversity and Pluralism and Map-Making and its Geopolitical Significance,* pp. 1-19.

Scott, J. (2014). Extraterritoriality and territorial extension in EU law. *American Journal of Comparative Law, 62*(1), 87-126.

Spoenle, J. (2010). *Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?* Strasbourg: Council of Europe.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

Svantesson, D. J. B. (2014). The extraterritoriality of EU data privacy law - its theoretical justification and its practical effect on US businesses. *Stanford Journal of International Law, 50*(1), 53-102.

Suda, Y. (2013). Transatlantic politics of data transfer: Extraterritoriality, counter-extraterritoriality and counter-terrorism. *Journal of Common Market Studies, 51*(4), 772-788.

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.

Upward, F., & McKemmish, S. (1994). Somewhere beyond custody: literature review. *Archives and Manuscripts*, *22*(1), 136.

Vaile, D., Kalinich, K.P., Fair, P.V., & Lawrence, A. (2013). Data sovereignty and the cloud: A board and executive officer's guide. *UNSW Law Research Paper,* 2013-84.