InterPARES Trust Project
Research Report

Title:		Annotated Bibliography for Transnational Team
Status:		Final
Version:		3.0
Date submitted:		10 November 2016
Last reviewed:		10 November 2016
Author:		InterPARES Trust Project
Writer(s):		Eng Sengsavang, NATO Elaine Goh, University of British Columbia Lucas Damer, University of British Columbia Elissa How, University of British Columbia Darra Hofman, University of British Columbia Samuel Michelson, University of British Columbia Maggie Hunter, University of British Columbia With contribution from former GRAs: Emily Chicorli & Taryn Jones
Research domain:		Legal
URL:		

Document Control

Version history			
Version	Date	By	Version notes
1	13 Feb 2016	Lucas Damer, Eng Sengsavang, Elaine Goh, Samuel Michelson, Maggie Hunter, With contribution from former GRAs: Emily Chicorli & Taryn Jones	Draft annotated bibliography prepared for the IPTrust Plenary meeting 16-18 February 2016
2	May 2016	Lucas Damer, Eng Sengsavang, Elaine Goh, Darra Hofman, Elissa How Samuel Michelson, Maggie Hunter, With contribution from former GRAs: Emily Chicorli & Taryn Jones	Draft annotated bibliography and Literature Review prepared for the Transnational IPTrust Plenary meeting June 2016
3	November 2016	Eng Sengsavang	Finalized annotated bibliography and Literature Review following the Transnational IP Trust Plenary meeting, September 2016

TOPICS

ANNOTATED BIBLIOGRAPHY

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), 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 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.

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

This article aims to determine whether or not cloud computing infrastructures can support privacy regulations but still remain practical. The majority of the article defines and explains the concepts of privacy and personal information, covering different approaches to privacy, and specifically discussing Australia's response to privacy and privacy breaches. Overall, Adrian argues that cloud computing is posing significant challenges to legal adaptations of current technologies.

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

The author argues that there is a shift occurring in cloud service contracts due to the increased flexibility of cloud service providers when negotiating terms of contract. Burden provides an overview of why cloud contracts developed and why they developed the way they did (i.e. with stringent terms), and outlines six provisions common to a cloud service contract. These are: the ability of the supplier to change terms, some without any notification; the right of the supplier to terminate or suspend services; the fact that warranties regarding the content and quality of service are limited (if they even exist); the reality that there is little, if any, coverage for potential infringement claims; the low limits of liability for loss of data; and limited service offerings. Burden explains that the premise behind many cloud service contracts essentially requires customers to take terms of services as they are. Several factors have affected the shift towards increased flexibility of cloud service providers when negotiating contracts: increased customer knowledge, increased customer identity, increased deal size/complexity; and competition with other providers.

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.**

Bushey provides an overview of the benefits and risks of adopting cloud-based systems, arguing that in order to ensure that records are reliable, accurate and authentic, such systems should be informed by archivists using criteria from archival diplomatics. Bushey details the results from a survey that questions respondents on their motivations and concerns regarding cloud service adoption, and the issues encountered when using cloud computing. A total of 34 questions were asked, with 353 responses collected, a response rate of 50 percent. Over half of the respondents worked in organizations that use cloud computing. The survey found that 38% of organizations that do not currently use cloud computing are considering it, while 39 % of respondents did not know if their organizations use cloud computing. The top reasons to use cloud computing include increased collaboration, reduction in costs, increased performance, increased storage, keeping pace with industry, and improvements in security. The top reasons for choosing not to use cloud computing include security risks, legal implications, loss of control of data, privacy risks, cost, technological complexity and lack of knowledge of cloud computing. Bushey explains that although service level agreements (SLAs) remain the only avenue for cloud customers to establish parameters for controlling access, to comply with data protection regulations, and to determine legal custody of the records, survey findings nonetheless show that a minority of organizations negotiate SLAs that prioritize ownership of data and metadata.

De Filippi, P., & McCarthy, S. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology*, *3*(2), 1–18.

The authors acknowledge the definition of cloud computing given by the National Institute of Standards and Technology (NIST), but consider the definition as "not universally accepted any more than any other definition" (p. 2). Instead, the authors define cloud computing as "the sharing or storage by users of their infrastructure or content on remote servers that are accessible online" (p. 2). De Filippi and McCarthy highlight a number of risks related to the deployment and use of cloud computing. First, there may be potential breaches of privacy regarding personal and governmental information. Second, the data stored in the cloud may be subjected to multiple domestic laws, depending on where the data is stored, processed, or transmitted. Moreover, cloud service providers can potentially store data in different servers and data centres so as to circumvent national laws on data protection. The authors note that data by itself "does not have any nationality but merely inherits the law of the territory in which it is located" (p. 8). Since data can be easily transmitted from one jurisdiction to another, the same bits of information can be subjected to several national laws within a specific moment in time. The third issue is that of data sovereignty. Even within a jurisdiction, the ability of the owner to exert control is limited when data is held by a third party.

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.

This study explores the potential risks that organizations may encounter during cloud computing adoption, and outlines processes to assess and prioritize these risks from the perspective of information technology practitioners and consultants. To this end, the researchers disseminated a questionnaire and define cloud computing risk as: “The occurrence of an event, which is associated with the adoption and use of cloud computing, and can have undesirable consequences or impacts on user companies” (p. 40). Prior to publishing the questionnaire, the researchers conducted an intensive literature review, which led to the development of an ontology of cloud computing risks (p. 41).

Cloud risks are organized into four main categories and twelve sub-categories. The four main categories are: organizational, operational, technical, and legal risks. Organizational risks include the significant impact of cloud computing on diverse organizational aspects, such as IT governance, compliance with industrial regulations, in-house IT experts, and IT planning. Operational risks refer to those affecting daily business and IT operations. Technical risks may arise from the complicated cloud infrastructure and inherent IT deficiencies existent within the company. Lastly, the nature and inherent features of cloud computing can lead to a range of legal risks related to data privacy, intellectual property, and contracts. The most critical top ten risks perceived by IT experts were found to be caused by the current legal and technical complexities and deficiencies associated with cloud computing, as well as by a lack of preparation and planning by user companies.

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

In this short, but extremely dense and informative article, Anthony Gray reviews the possible set of legal principles that could be applied in determining the rights of parties in a cloud agreement when a breach of privacy occurs. Gray looks at these approaches from EU, Australian and US perspectives. He reviews various regulations, articles and laws that could be used by these countries and the ways in which the legislation could be disputed in the cloud computing environment. For example, if the U.S. applies "second restatement," which basically states that jurisdiction can be determined "where the injury occurred," how would the rule apply if the injury occurs in multiple states or countries due to cloud computing infrastructures and the Internet? It is not always very clear in national laws where the rule is applicable. Gray also mentions the EU General Data Protection Regulation of January 2012. Under this reform proposal, there would be common privacy legislation across the EU, rather than a patchwork of different national laws. In addition, Gray briefly touches upon data transiting through servers in different countries. Gray suggests the creation of an international treaty that clarifies the question of legal regulation, privacy and security matters relating to cloud computing services, to be agreed upon by as many countries as possible. The footnotes in Gray's article are full of possible relevant articles and legal cases.

Haeberlen, T., & Dupré, L. (2012). *Cloud computing: Benefits, risks, and recommendations for information security*. European Network and Information Security Agency (ENISA).

This report is the first round of a project to revise and update the 2009 Cloud Risk Assessment study published by the European Network and Information Security Agency (ENISA). Both the 2009 Assessment and the current report consider benefits and risks of cloud computing from the point of view of information security. The "top security benefits" cited by the current review are: security and the benefits of scale; security as a market differentiator; more timely, effective and efficient updates and defaults; rapid, smart scaling of resources; and the benefits of resource concentration. The "top security risks," according to the report, are: loss of governance; lock-in; isolation failure; management interface compromise; data protection; insecure or incomplete data deletion; malicious insiders; customers' security expectations; and the availability chain.

The report defines "risk" as the interaction of a threat and vulnerability impacting an asset. In considering the risks of cloud computing, the report provides a table for each risk with scores for probability, impact, level of risk, and a comparison between "classic IT" and cloud computing scenarios. The authors recommend a number of points to consider when assessing cloud computing risks, including the recommendation to weigh risks along with business opportunities, which may compensate for risks. Cloud computing risks should also be measured against the pitfalls of staying with traditional desktop-based models. The threats of cloud computing vary considerably depending on the type of cloud model used. Additionally, some, but not all, risks may be transferred to the cloud provider: those that cannot be transferred include risks that may lead to the failure of an enterprise, and legal and reputational risks.

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.

In their article, Henkoglu and Kulcu discuss the fact that many people perceive cloud computing as a non-secured technology. They observe that the United States, unlike Europe, lacks a comprehensive law protecting the privacy of personal information and limiting data transfers to other countries; however, "sensitive" data is addressed in U.S. federal law that addresses privacy. A compelling point made by the authors is that U.S. federal regulations require companies to abide by a minimum set of rules regarding the protection of data. In doing so, the government incentivizes organizations to protect data, rather than requiring compliance to the practice by law. For example, healthcare institutions are obliged to ensure the security of personal healthcare information, yet are not required to store the data in an encrypted state. However, if healthcare institutions store data through encryption at an adequate level, they do not have to declare any breach of data, enabling them to avoid additional expenditures, customer dissatisfaction or loss of reputation. Therefore, many healthcare institutions are incentivized to use data encryption so that they do not have to declare data breaches. The authors explain that if U.S. health care organizations transfer patient information to cloud systems located in different countries, organizations would be obliged to declare breaches and would be held liable if information security is breached within their systems. The cloud service provider, however, would not be held liable under U.S. law, since providers are liable only within the framework of agreements between provider and user.

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.**
ISO/IEC 17788 provides an overview of cloud computing technology, along with a set of terms and definitions. Cloud computing is defined as an evolving paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand (p. 2). The cloud computing paradigm is composed of key characteristics, cloud computing roles and activities, cloud capability types/service categories, cloud deployment models and cloud computing cross cutting aspects (p. 4). The key characteristics of cloud computing are identified as: broad network access: physical and virtual resources are available over a network and accessed through standard mechanisms that promote heterogeneous client platforms and offer an increased level of convenience; measured service: usage of cloud services can be monitored, reported, and billed, which optimizes and validates the delivered cloud service; multi-tenancy: multiple tenants and their data are isolated from and inaccessible to one another; on-demand self service: the cloud service customer can provision computing capabilities automatically or with minimal interaction with the cloud service provider; rapid elasticity and scalability: physical or virtual resources can be quickly and elastically adjusted to increase or decrease resources, so that customers need not worry about limited resources and capacity planning; and resource pooling: physical or virtual resources can be aggregated in order to serve one or more cloud service customer, and cloud service providers can support multi-tenancy while also using abstraction to mask the complexity of the process from the customer (p. 5).

All cloud computing-related activities can be categorized into three main groups: activities that use services, activities that provide services and activities that support services. A single party could play more than one role at any given point and could engage in a specific subset of activities of a role. The major roles of cloud computing are: the cloud service customer, the cloud service partner, and the cloud service provider (pp. 5-6).

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.**
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60545

ISO/IEC 17789 is a “Recommendation | International Standard” that introduces the Cloud Computing Reference Architecture (CCRA) “for cloud computing standardization and…[to] provide an overall framework for the basic concepts and principles of a cloud computing system” (p. 7). The CCRA conceives of four “views” through which cloud computing systems can be understood: the user view, the functional view, the implementation view, and the deployment view (p. 4). The user view encompasses the ‘parties, roles, sub-roles, and cloud computing activities’ within the system, while the functional view describes the “functions necessary for the support of cloud computing activities” (p. 4). These two views are addressed by ISO/IEC 17789. The implementation and deployment views are outside the scope of the recommendation/standard.

The user view includes the elements ‘cloud computing activities; roles and sub-roles; parties (stakeholders); cloud services (based on cloud capability types described in ISO 17788: IaaS, PaaS, SaaS, NaaS); cloud deployment models (public, private, community, hybrid), and cross-cutting aspects (p. 5). Cloud computing roles include the cloud service customer (CSC), cloud service provider (CSP), and cloud service partner (CSN). Each role has specific sub-roles that are sub-types of the cloud computing activities of a given role (p. 9). For example, CSC sub-roles include cloud service user, cloud service administrator, cloud service business manager, and cloud service integrator (p. 10). In turn, each sub-role has various cloud computing activities such as “monitor service” for the cloud service administrator. Each of the three roles is described and broken down by its sub-roles and their cloud computing activities in clause 8.

The functional view of cloud computing “is a technology-neutral view of the functions necessary to form a cloud computing system” (p. 7) and includes the following parts: functional components, functional layers, and multi-layer functions. The functional components are groups of functions that are needed to enact the cloud computing activities outlined in clause 8 (p. 29). For example, the “user function” is a functional component that is needed to perform the “user service” activity (p. 31). The functional components are in turn classed into four functional layers: user layer, access layer, service layer or resource layer; or into the multi-layer functions that span all layers. These are described in more detail in clause 9 of the standard.

Cross-cutting aspects “are shared issues across...roles, activities and functional components” (p. 23). An example of a cross-cutting aspect is security, because it impacts multiple elements such as infrastructure, services, and the cloud service customer, cloud service provider, and cloud service partner (the last three are all “roles”) (p. 23). Cross-cutting aspects identify key cloud computing issues, including: auditability, availability, governance, interoperability, maintenance and versioning, performance, portability, protection of personally identifiable information, regulatory, resiliency, reversibility, security, service levels and service level agreements (p. 24). Each issue is described and sometimes, but not in every case, recommendations or standards for addressing the issue are provided in Section 8.5.

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

This document provides a systematic and logical process to manage risk. It also recommends that organizations develop, implement and continuously improve a framework to integrate the process. One of the featured components of the process is to establish the context, which is described as an activity at the beginning of a risk management process to capture the objectives of the organizations. The whole process involves establishing the context, risk identification, risk analysis, risk evaluation and risk treatment.

Terms and definitions related to risk and risk management are outlined in section 2. Section 3 outlines the 11 principles that need to be complied with in order to ensure risk management is effective. This includes such principles as recognizing that risk management creates and protects values, risk management is part of decision-making, and that risk management is structured, systematic and timely. Section 4 provides a framework to help manage risk, which includes: design of a framework for managing risk (4.3 - 4.3.7), implementing risk management (4.4 - 4.4.2), monitoring and review of the framework (4.5), and continual improvement of the framework (4.6). Section 5 outlines the process described above in greater detail. Of importance to us is the portion that defines risk criteria in section 5.3.5, as it discusses how criteria can be identified for risk that reflects the organization's values, objectives and resources.

Kong, L. (2010). Data protection and transborder data flow in the European and global context. *European Journal of International Law*, *21*(2), 441-456.

In this article, Kong asserts that transborder data transfers generally lack adequate supervision and that this has been one of the many challenges faced by the European Data Privacy Directive. Kong provides a brief background on technological innovations that spurred an increase in transborder data flows, and notes that "due to uneven data protection levels in national sovereignties, data protection has become a major obstacle to free global data flow" (p. 442). Kong examines contractual and corporate law models, and analyses the scope of standard clauses and the safeguards they provide.

Kong examines the European law's stance on cross-border data transfer, and notes that one of the Directive's core criteria is the 'equivalence' principle. While the Directive attempts to facilitate harmonization between Member States, data flow outside of the

European Union is prohibited unless specific conditions are met, and this has led to the assertion that there is “an iron curtain on transfer of data.” (p. 443) The author discusses the adequacy of the assessment system for third party states and the shortcomings of the system as a whole.

The author addresses liability regimes and notes that in the European Union, standard contractual clauses assign a degree of liability to the data transferor, so it is in that party’s best interest to ensure data security. Data subjects have third-party beneficiary rights. Kong turns to the Corporate Law Model and assesses the effectiveness of Binding Corporate Rules. A global model for international, legally-binding data protection regulations would be optimal. However, when discussing the advantages and disadvantages of such a model, Kong notes that there is a lack of consensus within the international community.

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.

The authors observe that many of the benefits that make cloud computing attractive also increase risks to security and privacy. The article provides a framework to assist service providers in complying with the new EU regulations, as well as a brief overview of the issues of security and privacy in the context of cloud computing. The authors note that it is increasingly difficult for legal instruments to be up-to-date, as the technological environment changes so rapidly.

The article provides a discussion on the definitions of terms such as “controller,” “representative,” “processor,” “main establishment,” and “processing.” The proposed changes to the EU Privacy Directive would increase harmonization across the EU and provide a clearer idea of when EU law could be applied extraterritorially. The territorial scope of the EU Privacy Directive, concerns the processing of personal data within the EU, the processing of personal data of subjects resident in the EU by controllers who are outside of the EU, and the monitoring of EU citizens’ behaviour.

The authors provide a framework for determining the reliability of a cloud service provider based on National Institute of Standards and Technology (NIST) guidelines, and discuss legal and organizational requirements necessitated by the proposed EU Data Protection Regulation. The authors address data security and protection, and list what organizations should know about their cloud service provider. The requirements of Articles 30, 31, 40, 41, and 42 of the Regulation regarding transborder transfer and data loss or data breach are addressed. The authors conclude that security and privacy are significant challenges that both service providers and clients must deal with.

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.

In this article, Lipinski explains how cloud computing service agreements are governed by contract law. He describes licenses, agreements and Terms of Service (ToS) as legal forms of permissions, and explains how they apply in cloud computing environments. Lipinski also discusses in great detail how ToS provide and limit features to users, and describes the lack of transparency in cloud ToS using the examples of Apple iCloud, OpenDrive and Dropbox to examine how different companies handle ToS, and how users can unknowingly consent to changes in ToS (i.e. simply by continued use of the service). To highlight the disparities in the changes to ToS, Lipinski discusses the Douglas vs. Talk America case, in which the latter revised its site contract but never informed users such as Douglas of the changes. The ruling on the case determined that in this instance, once a contract is formed any changes to it represent an offer for additional terms, which in theory requires separate, distinct assent. Cloud service providers have various provisions within the ToS that limit their liability, such as broad discretion to terminate users and/or suspend access to services, indemnification clauses (requiring users to compensate the provider for loss or damage sustained due to the conduct of the user), and altering copyright rules. Lipinski discusses unconscionability, i.e. how TOS issues are a matter of law for courts to decide case by case. For example, courts can void an entire agreement or strike particular clause(s).

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

This technical article looks at how cloud computing platforms can become more secure through critical infrastructures. The article begins by identifying the core technical issues that are preventing cloud computing from becoming a “truly ubiquitous” service: data lock-in due to proprietary protocols; confidentiality concerns over shared resources; networking bottlenecks in and around core data centers at peak times; and loss of governance over mission-critical data. Though the authors admit that while wide standardization for cloud computing is developing, “The inescapable fact is that until a sufficient level of trust can be associated with moving services to the cloud, customers with high security requirements will shun these services in favour of a more controlled environment” (p. 679). The article presents a concept for an innovative new platform to ensure the integrity of cloud services and identify the core requirements, components and features of the infrastructure. The article also provides an analysis of the current approaches to security in clouds, while discussing "trusted computing" (TC) and "critical infrastructures" (CIs).

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

This study by the InterPARES Trust Project was designed to identify the types of terms and gaps that exist in contracts between cloud service providers and their clients across multiple jurisdictions, and Records Information Management concerns that specifically reflect the needs of records managers attempting to work in the cloud. The report provides an overview of the cloud, including its various implementations and cloud services, and the types of contracts (i.e. Terms of Conditions, Terms of Service, and Service Level Agreements). Important recordkeeping principles from ARMA and the International Standards Organization that relate to cloud computing services are outlined, such as that a recordkeeping system should have the ability to retain and properly dispose of records at any time. The report provides summaries of seven American legal cases that identify recordkeeping concerns that could apply in the cloud environment.

The authors discuss different initiatives, both governmental and public, within Canada, the U.S. and the European Union that use or plan to use cloud services, such as federal governments, Shared Services Canada and FedRAMP. The report examines universities within Canada and the U.S. that implement services in the cloud and collaborate with third-party industry members, alongside a consideration of freedom of information and privacy legislation in various provinces and states. In section 8, the report analyzes cloud service contracts from thirteen companies.

Lastly, the authors identify fifteen contract term categories that should be addressed in cloud service provider contracts: General destruction guarantee, specific destruction method, destruction on contract termination, service continuity, outages, disaster recovery plan, general security provisions, physical security specifications, technological security specifications, tiered security provisions, territory of storage, copyright/ownership, general privacy, privacy policy, and privacy legislation (pp. 26-30).

The report includes appendices that further explain the legal cases, an annotated bibliography, and summaries of contract and service terms offered by cloud service providers in the U.S., Canada and the European Union.

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

This book provides a comprehensive investigation into legal issues one may encounter when acquiring, implementing, and maintaining cloud computing systems. The majority of the book focuses on the use of cloud computing by EU citizens. However, there is information relevant to international organizations' (IOs) use of cloud computing, most notably the tensions surrounding EU and American laws with regards to cloud use and implementation. The book is divided into four parts. Part I (chapters 1-2) provides background on cloud computing infrastructure and services. Part II (chapters 3-6) outlines the different transactions that take place between service provider(s) and user(s). Part III (chapters 7-10) deals with personal data in the context of EU laws. Finally, Part IV (chapters 11-14) discusses regulation and governance within the cloud computing environment.

Chapter 1 details what cloud computing is. This includes a discussion on some of the possible combinations (and resulting complications) of cloud computing architectures, such as an SaaS based on a PaaS model that is itself based on an IaaS model. Without knowing it, the end user may be dependent on several providers and sub-providers rather than just the SaaS provider alone. This is an important consideration for IOs, especially in regards to jurisdictional claims over data and awareness of who may have access to data. Chapter 2 outlines control, security, and risk factors in the cloud computing environment. Data security issues (confidentiality, integrity, and availability) and collocation risks (being located with the data of another party) are highlighted. There are conflicting viewpoints on the methods employed to ensure confidentiality and integrity. Some providers argue that storing cloud data physically in multiple sets of equipment or multiple data centres is the best course of action, while others argue that the multiplicity of locations increases the risk of accessibility by third parties. The author suggests that SLAs can cover minimum service requirements, but given that standards for measuring service levels have not been established, these can be ambiguous and contentious.

The chapter outlines some of the key differences between traditional outsourcing and cloud computing: active agency versus passive resources for self-service usage, "direction of travel" and sequence of events, the standardized shared infrastructure and environments, knowledge, and degrees of control. It is worth noting how lawyers approach cloud computing. A lack of awareness of how cloud arrangements work has resulted in some lawyers treating cloud contracts as though they were software licences, or technology product sales, rather than contracts for services. This is consequential since different aspects of the technology are considered in licences than are considered in contracts.

Chapter 3 outlines the methodology employed in the 2009 Cloud Legal Project, based in Queen Mary University of London, Centre for Commercial Law Studies initiated with significant financial support from Microsoft Corporation. The aim of the project is to address the uncertainty in legal and regulatory aspects of cloud computing. The chapter discusses the classification of cloud services and terms of service (ToS) documents, categorization and analysis of terms, contractual forms and applicable law, data handling (including data integrity, preservation, disclosure, location/transfer, monitoring, and rights over content), liabilities and responsibilities, and practical findings. Studies have found that cloud service providers will generally, but not invariably, use their principal place of business as the basis for the legal system and litigation governing their ToS. The ToS should be the primary document consulted in terms of data protection and privacy issues.

Chapter 4 continues with the Cloud Legal Project, but focuses on negotiated rather than standard form contracts. The project found that users consider providers' standard contract terms insufficient to accommodate customer needs. The top issue cited was the exclusion or limitation of liability and remedies, followed by service level availability, security and privacy, termination rights, providers' ability to change service features unilaterally, and intellectual property rights. The research was limited to contracts between cloud users and providers of SaaS, PaaS, or IaaS services, not including end-user software licences. However, there is a discussion on click-through agreements, which present users with the providers' standard terms without an opportunity to negotiate. A 2010 survey which found that 50% of IT and IT security specialists were unaware of at least some cloud computing resources deployed in their organizations, while lawyers expressed that their involvement had not been sought early enough in the ToS and SLA process. The terminology in contracts was seen to change according to size and/or prestige of the user in addition to the type of service model being discussed. While smaller, less prestigious users generally agreed to the terms of contract, larger, more powerful users, notably governments, occasionally required providers to use language from their own standard IT services or outsourcing terms.

Issues of jurisdiction come up in section 5.3.1 of Chapter 4. Users are more concerned about data centre location than collocation within a third party's data centre. For example, one UK-based global user, although it does not process personal data in the cloud, nonetheless ensures that its provider processes data exclusively in EU data centres or, if data is transferred to the U.S., that the data be certified under the Safe Harbour principles. There is also the issue of "follow the sun" services and support staff. Although the data may be kept within a certain territory, the cloud service provider may opt to have remote access to metadata granted to those working elsewhere in the world. This provides a further complication in terms of access and data security. The chapter proposes one possible compromise between the security concerns of providers and users in the form of independent certifications of cloud providers. Certifications are starting to become more prominent with groups such as the Cloud Security Alliance (CSA) and the Open Data Centre Alliance.

Chapter 5 outlines the process undertaken by the UK government in order to procure cloud services. Chapter 6 deals with ownership of information in clouds. This includes not only the information generated, stored, and disseminated by the user, but also the information generated, stored, and disseminated by the provider and third parties. The question of who owns the information that is generated in the cloud, however, is slightly more difficult to determine. There is discussion on the role of copyright, especially how it changes depending on legal tradition, the locale of the creator of cloud-generated information, and the collaborative nature of cloud-generated material. The author mentions the concept of Content as a Service (CaaS), but does not explain in detail what this model entails.

Chapters 7 through 10 deal with the protection of personal data. The difference between anonymyzing data (such as deleting identifiers, substituting codes, aggregating information, and/or introducing statistical noise) and pseudonymizing data (disguising identities which can be either reversible or irreversible) is discussed. Encryption, monitoring of client use, and an accountability-based approach to address privacy concerns targeted by the 'personal data' concept are also examined, as is the question of who is the controller and who is the processor in a cloud-based environment. "Controller" and "processor" are terms adopted from the EU Data Protection Directive (DPD). Introduced in the 1990s, portions of the directive do not fit well into the cloud computing environment. For instance, the definition of a controller can be confused with the definition for a processor, given that cloud computing blurs the lines between controller and processor.

Chapter 9 begins by establishing the location-based nature of data protection laws in the EU. In particular, DPD Articles 4 and 17(3) deal with applicable law and jurisdictional reach. There are three grounds on which European data protection becomes applicable: establishment, public international law, and use of equipment within the jurisdiction. Practically speaking, this leads to much confusion, for example, when the data protection laws of two nations apply to the same act of processing. In addition, there are concerns around the controller saving cookies or other data of its EEA-based users, or uncertainty over a data centre located in a non-EEA Member State that provides cloud services. Chapter 10 deals with data export restrictions, data transfers, and data export exceptions. One of the possible solutions proposed to combat conflicts between these concepts is the initialization of "regional clouds," which may be of use for certain international organizations.

Chapter 11 explores law enforcement's access to data in the cloud. Much of this chapter examines the territorial jurisdictional reach of certain authorities, otherwise referred to as Law Enforcement Authorities (LEAs). The majority of the focus is on American LEAs attempting to investigate European-based clouds. The forensic challenges presented by the cloud environment are discussed, including contractual relationships between the service provider and the subscriber, infrastructure provider, and communication service provider. Cloud computing structures provide obstacles for forensic examination, and jurisdictions vary significantly in granting LEAs access to similar data types under different authorization procedures. The Council of Europe Cybercrime Convention aims to impose a unified response to cybercrime investigations across Europe. Terminology used in the Convention is analyzed, including 'control,' which can be viewed in three different ways: managerial, technical, and legal.

Chapter 12 focuses on the business side of cloud computing, most importantly competition legislation. Chapter 13 deals with consumer protection in cloud environments. 12 issues for the consumer in ToS agreements are outlined: applicable law and jurisdiction, arbitration, acceptable use, variation of contract terms, data integrity, data preservation, data location/transfer, rights in customer content, warranty, exclusion and limitation of liability, and indemnification. The final chapter summarizes portions of the previous 13 chapters in the context of cloud computing governance. Governance denotes a system of rule-creation and enforcement that does not depend solely on state command and control. Cloud governance encompasses two main areas: internal (the provider's technical workings) and external governance. In conclusion, the author reiterates that national laws lack legitimacy and more needs to be done to tailor laws to the cloud computing environment.

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.

This paper examines the barriers and drivers for organizations to adopt cloud computing. It begins with a literature review of empirical work done on the topic of cloud adoption in organizations. A table outlines the scope and adopting unit (noting if the cloud adoption takes place on the organizational level, among organizations, or among individuals), the method used, and the main outcomes of the studies. Some of the featured papers focus on cloud computing in general, while others look at specific applications like Google Apps. The authors consider factors involved in organizational adoption of cloud computing such as size, location, infrastructure, and political stability.

The authors then introduce their proposed theoretical research model. They highlight three innovation factors that are key to innovation adoption: compatibility, relative advantage, and complexity (as outlined by Tornatzky and Klein, and detailed in this paper in relation to cloud computing). Other innovation factors include image, security and trust. There is a discussion about innovation characteristics research that focuses on planned adoption and implementation of cloud computing. In the conclusion, the authors reiterate that their project is a "research-in-progress" and that their focus will be on public cloud implementation in an organizational setting. They also discuss next steps and future research possibilities.

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

The authors argue that current approaches to data protection are based on an old paradigm of computer use from the 1980s and 1990s that assumes data is located physically on premises, in contrast to today's usage of computers on the Internet/cloud computing. In discussing the development of cloud computing, the authors observe that cloud computing has been around a lot longer than many of us think. According to theories from the early use of computers, the technology can be traced back to web-based email in the early 1990s. The article looks at the development of government clouds in France and Germany in the 1970s onward. The authors explain how "data sharding" and "data obfuscation" work and explain why they help to secure data, even though both processes involve the geographical separation of data (a core design philosophy of cloud computing). These techniques create conflicts between those countries that require data to be stored entirely within their borders ("localization" or "data location requirements") and those that do not, since data sharding and data obfuscation secure data by spreading it across multiple data centers. The result is that no single data center possesses all of the information required to read any document. The authors argue that laws mandating all data be stored in one jurisdiction provide assurance that the government has control over data within that jurisdiction. However, the tradeoff is that data becomes technically less secure.

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). Switzerland: United Nations. http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf

The objective of this report by the United Nations is to examine the "economic potential of cloud computing for low and middle income countries" (p. iii). The report seems to endorse the adoption of cloud services and recommends the development of a national cloud strategy. Governments and businesses in middle- and low-income countries are encouraged to assess the potential of cloud computing within their own context.

The report attempts to address three main research questions. The first question is the current status of the cloud economy in developing countries. The second question is the impact of the cloud economy for different groups of stakeholders. Finally, the report examines policy and regulatory approaches undertaken by governments in developing countries to capitalise on the benefits of cloud computing.

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.**

This guide provides a concise, comprehensive examination of issues concerning the sovereignty of data stored in cloud computing systems. The guide is designed for a broad audience and includes a glossary of technical and legal terms that may prove useful. The authors note that with an increase in cloud storage comes a similar increase in questions of data sovereignty and corresponding security measures. The guide includes a series of self-reflective questions that can be used in order to ascertain whether businesses afford their digital assets sufficient protection. The authors also highlight that cloud service providers may include a clause in contracts excluding them from liability over matters that are within their control. A brief overview of the types of cloud services, including IaaS, PaaS, and SaaS, is provided. Chapter Three focuses on risk management and corporate governance issues, noting that the economy of scale that often makes cloud computing so attractive also increases the level of risk. The authors urge information officers to ensure that they know where the data is stored for jurisdictional purposes. Several examples from Australian, European, American, and Canadian perspectives are provided. The authors offer an outline of how to select a cloud provider, and address jurisdictional obligations. Chapter Five offers a discussion on third-party data access. Clients increasingly question whether cloud storage necessitates cross-border data flows. The authors look at legal instruments related to obtaining third-party access to data stored in the cloud, with a focus on American legislation. Information managers must be aware of the regulatory environment in which the organization operates, and to this end Chapter Six analyzes security concerns and addresses jurisdictional policies. The implementation, integration, auditing and evaluation of jurisdictional policies forms part of the discussion.

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.

Bearman, D. (1991). An indefensible bastion: Archives as a repository in the electronic age. In D. Bearman (Ed.), *Archives and museum informatics technical report: Archival management of electronic records* (pp. 14-24).

Written in 1991, this article addresses the issue of custodianship over early electronic records. The introduction gives a brief background of Gerald Ham's idea of post-custodial archives and Bearman's experience with electronic records custodianship. Bearman's experience includes identifying strategies for the National Archives and Records Service, the establishment of an Information Resources Management office within the Smithsonian Institution, and a role in the United Nations Advisory Committee for Coordination of Information Systems (UN/ACCIS). Bearman notes that, in these positions, there were few advantages and considerable disadvantages to practicing archival custody of electronic records. Two of the disadvantages are the migration costs and the fact that the transfer of records to the archives assumes that there would be records present in the office of origin after they cease being active.

The article is divided into two major sections and a conclusion. The first section argues against archivists as custodians of electronic records. This argument is based on four concerns in the archival profession. First, organizational concerns stem from the low-status position of archives and records management within organizations, and archives are not allocated the same amount of responsibility as other assets such as money, personnel, and space. Second, the custodial role that archivists have defined for themselves is not professional. Bearman argues that this definition usually omits aspects such as accountability, the ability to audit information, and appreciation of the cultural and technical character of communication. Third, economic concerns stem from inadequate funding for professional archival tasks, including records systems analysis and appraisal, and the cost of migrating and maintaining electronic data. Finally, there is the cultural change away from physical loci of information.

The second section introduces several tactics to deal with these issues. Such tactics include: regulating information management (including the ideas of accountability of offices rather than occupants, control over behaviour towards records, and information as a corporate asset); auditing information management practices; training of information creators by archivists, and informing the users about the decentralization of custody. Bearman concludes that electronic records pose a special challenge to the concept of the custodial repository for a number of reasons. These reasons include the fact that because electronic records are organizationally beyond the control of custodial archivists, they are professionally outside the experience of archivists. Additionally, Bearman notes that economics undermines traditional repositories and the culture of electronic records creation makes them more vulnerable to destruction by their creators, thus increasing the requirement that creators assume responsibility for their care.

Bearman, D., & Hedstrom, M. (1993). Reinventing archives for electronic records: Alternative service delivery options. In *Electronic records management program strategies* (81-98). Pittsburgh: Archives and Museum Informatics.

The article examines traditional archival practices and observes that they are not always appropriate for the management of electronic records. As the authors state, the inspiration for this article stems from both the realization of information technology's impact on recordkeeping and David Osborne and Ted Gaebler's book *Reinventing Government*. In *Reinventing Government*, there is an emphasis on rethinking service delivery options and focusing on outcomes rather than outputs.

The article discusses why current methods fail for electronic records. The discussion is illustrated through a diagram of a traditional archival model that includes records surveying, records scheduling, appraisal, accessioning, arrangement and description, preservation, and provisioning of access to records. Each of these steps and their deficiencies in relation to electronic records are detailed in the article. The article suggests that the archivist takes on much of the burden within this model.

This approach contrasts with the model presented by Osborne and Gaebler, who posit that governments must shift from "rowing" to "steering." That is, archivists should guide others on how to properly maintain records and leave some aspects of archival management to the creators. This is done through tactics such as creating legal rules and sanctions, regulation/deregulation, and monitoring and investigation. Ultimately, this empowers rather than services others. The authors also consider enterprising archives, customer-driven archives, and decentralized archives. In conclusion, the authors encourage archivists to consider serving as internal consultants, by defining recordkeeping regimes and tactics, and by avoiding the burden of custody or delivery of records through the use of information systems maintained with metadata.

Boadle, D. (2004). Reinventing the archive in a virtual environment: Australians and the non-custodial management of electronic records. *Australian Academic & Research Libraries, 35*(3), 242-252.

This article outlines the development and arguments of post-custodialism and non-custodialism in Australia. Ihe author briefly reviews the arguments of post-custodialists such as Bearman, Acland, McKemmish, Upward, and Stuckey. Steve Stuckey, then Assistant Director-General responsible for Standards and Access at the National Archives of Australia (NAA), argues that archives should only become custodians of electronic records if they satisfy a combination of four factors: they need to be retained in electronic form to enhance their value, they cannot be retained by transference to another format, they were records of a defunct agency, and the NAA was the only custodial institution placed to service. The authors follow with counter-arguments from custodialists such as Eastwood, who took issue with Bearman's focus on risk management; Nesmith, who saw the Monash recordkeeping theorists as giving accountability too narrow a definition; and Duranti, who linked accountability to custodial management.

The article includes a summary of findings of a report by the American Research Libraries Group's Task Force on Archiving Digital Information. The report states that information creators, providers or owners should have initial responsibility for archiving their digital information, but those agencies that do not have information management as a core function would do better through partnership or subcontracting to a certified digital archives.

The article concludes by outlining Australia's reversion to custodial ownership of electronic records after the year 2000. Notable is a reference to the Australian Public Service Commission's *State of the Service Report* issued in 2002, which states that the change led to a high degree of confusion amongst employees who were uncertain about their responsibilities with respect to the management of electronic records.

Callery, B. G. (2009). Custody and chain of custody. *Encyclopedia of library and information sciences* (3rd ed., pp. 1388-1394). New York: Taylor and Francis.

This encyclopedia entry highlights the cultural sensitivity surrounding both archival and museum collections and questions whether establishing custodianship over an object is the best approach. The entry also discusses the development of post-custodialism and argues that the main difference between custodialists and post-custodialists is the latter's involvement in the earliest stages of records creation. On the subject of archival custody, the entry offers an overview of the works of Jenkinson, Schellenberg, and Ham. Various perspectives of both custodialism and post-custodialism are briefly mentioned, along with the idea of distributed custody. This is followed by examples of challenges to custody in archives in the form of requests.

Cook, T. (2001). Archival science and postmodernism: New formulations for old concepts. ***Archives & Museum Informatics*****,** ***1*****, 3-24.**

The article explores the relationship between postmodernism and archival science. Cook begins by stating that archival science may no longer be as viable in a computerized and postmodern world. Cook speaks of postmodernism as having two main impacts on archival science, the first being a change in theoretical discussion and the second being speculation about the nature of historical and other texts. The constructed nature of archives is discussed at length. Cook outlines how archival focus has switched from preservation of records to their creation and appraisal. As he states:

> ...in a world of rapidly changing and very complex organizations that create voluminous and decentralized paper records, and in a world of electronic records with their transient and virtual documents, their relational and multi-purpose databases, and their cross-constitutional communication networks, no reliable record will even survive to be available to the archivist to preserve in the traditional way - unless the archivist intervenes in varying ways in the active life of the record (20).

This intervention on the part of the archivist involves changing organizational behaviour, work cultures, recordkeeping strategies, and systems design strategies.

In his closing comments, Cook elaborates on how postmodernism will impact eight key archival concepts: provenance, which will be linked to function and activity rather than structure and place; original order, where pieces of records are stored randomly, then recombined intellectually or functionally for different times and places; record, which will become a conceptual data "object" controlled by metadata; fonds, which will change from physical order to virtual relationships reflecting dynamic multiple creatorship; arrangement and description, which will maintain contextual understandings of multiple interrelationships; appraisal, which will change into macro appraisal analysis; preservation, which will focus on migrating and emulating concepts and interrelationships; and archives, which will change from physical locales to a virtual "archives without walls" existing on the internet.

Cook, T. (2007). Electronic records, paper minds: The revolution in information management and archives in the post-custodial and post-modernist era. *Archives & Social Studies: A Journal of Interdisciplinary Research*, *1*(0), 399-443.

This article examines the literature on post-custodial archives in conjunction with postmodern ideals. Cook argues that archivists can no longer afford to be perceived as custodians in an electronic world. He highlights the fact that behind each record lies the need to record. Cook proposes that archivists must shift their focus from looking after physical objects to focusing on the functional context in which records-creating activities take place. Cook explores the history of the archival profession, from ancient Egypt to World War II, when archivists were considered valuable and high-ranking officials in monarchies and governments. By contrast, post-World War II, Cook conjures up the image of archivists as administrators and less-influential decision-makers.

This discussion leads to the origins of the post-custodial "revolution." Cook cites Peter Scott in Australia as one of the first archivists to focus on mapping dynamic relationships rather than producing static cataloguing. In discussing post-custodialism, Cook suggests that archivists must transform our provenance-based ideas to a conception- and process-centered approach. He emphasizes the opportunities archivists have in creating value-added knowledge by mapping contextual pathways between electronic records. "Creatorship" is a more fluid process in the electronic environment, and internal computer instructions and protocols are stored in software-dependent metadata systems. The various components that go into making a single electronic record (for example an email with spreadsheet and word processing attachments) are considered. Cook then discusses how post-custodial theories are closely linked to postmodernist perspectives, including archives' role in society and in the formation of "official memory."

Cunningham, A. (1996). Commentary: Journey to the end of the night: Custody and the dawning of a new era on the archival threshold. *Archives and Manuscripts, 24*(2), 312-321.

This article focuses on four preceding articles in the same issue of *Archives and Manuscripts* (Duranti's "Archives as a place," Eastwood's "Should creating agencies keep electronic records indefinitely?" Upward's "Structuring the records continuum," and O'Shea and Roberts' "Living in a digital world"). Cunningham discusses his personal history in the custodial/post-custodial debate, which has led him to be, in his words, a "mildly enthusiastic post-custodialist." Cunningham notes the post-custodialist argument that it is undesirable and maybe even impossible to wait until electronic records become inactive before bringing them under archival control. Ultimately, he sees the merits of looking at the issue of custody through the lens of the continuum model, which he perceives as providing a rationale for creators to also be responsible when it comes to long-term archival considerations.

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

In this article, Duranti discusses the origins of traditional archival custody, beginning in Roman law, which she argues not only provided the foundation for common law in Europe, but also most of the western world. She discusses the Justinian Code and how an archive was a place of preservation under the jurisdiction of a public authority, providing documents with trustworthiness and the capacity to serve as evidence and continuing memory of action. She then analyzes the progression of custody and archives as a place to the middle of the 20th century. At this time, the concept of archives as the place that endows documents with authenticity and guarantees that their creators will remain accountable to themselves and society decreased, and the post-custodial understanding as a model for the defence of the record saw a rise. Duranti outlines that jurisdiction does not require physical custody. She also explains the characteristics of authentic records: transparency of records preservation, security (certainty that the records cannot be consciously altered), and stability (relationships are intact and the context is defined).

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

This article outlines some of the major issues for records that are processed in the cloud, primarily related to the authenticity of records. It begins by listing the five "essential characteristics" of cloud computing, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The Records in the Cloud project aims to address the questions surrounding the control and authenticity of cloud-based records in the context of an integrated legal, administrative and value organization. Multi-tenancy, for example, is one of the significant motivations for adopting cloud computing, yet becomes an issue when trying to destroy records. Encryption is another issue, since one must determine who holds the keys and codes to encryption. The article looks briefly at maritime legislation to highlight the parallels between cross-border data flow and goods traveling overseas. The authors raise the point that it is not enough to simply worry about where records end up in the cloud; how the records get there must also be examined, as records may travel through many countries before reaching a destination. Cloud service providers (CSPs) often remove themselves from liability and responsibility for such issues. Moreover, CSPs generally offer services for storing records only. All of the metadata generated by CSPs, such as location of storage and any changes made to the records, are considered to be the intellectual property of the CSP and are inaccessible. This is problematic because a tenet of authentic records is transparent preservation. Stability of the records is another concern. Near the end of the article, Duranti and Jansen argue that, “The role of the archives as a place is still relevant and necessary in a cloud based paradigm, if not as a physical institution providing storage then as a supervisory one establishing policy, providing inspections and enforcing rules and regulations” (p. 164).

Duranti, L., & Rogers, C. (2012). Trust in digital records: An increasingly cloudy legal area. *Computer Law & Security Review, 28*, 522-531.

Duranti and Rogers begin by highlighting the four types of knowledge needed to establish trust in records: reputation, which results from an evaluation of the trustee’s past actions and conduct; performance, which is the relationship between the trustee’s present actions and the conduct required to fulfil his or her current responsibilities as specified by the truster; competence, which consists of having the knowledge, skills, talents, and traits required to be able to perform a task to any given standard; and confidence, which is an “assurance of expectation” of action and conduct that the truster has in the trustee. The authors state that issues of trust are difficult to isolate because they are bound up with issues of privacy, security and jurisdiction. Several legal cases in which jurisdiction plays an important role are featured, the most pertinent being Google’s establishment of a blanket privacy policy for all materials on its cloud. It should be noted that the article only focuses on the North American legal tradition and is therefore not global in its analysis.

The second section uses archival science and digital forensics as frameworks for determining the trustworthiness of digital records. The third section examines the trustworthiness of digital documents as evidence in common law courts. Three rules are examined in detail: the authentication rule, the best evidence rule, and the hearsay rule. The fourth section deals specifically with trust in the cloud. In this section, cloud computing, the four deployment models for cloud architecture (private, public, community, and hybrid), and the three service models (SaaS, PaaS, and IaaS) are explained. Several questions are postulated, such as “In the event of litigation or other dispute, in what jurisdiction will [services] be governed?” and “How will cloud service providers protect content from data breaches?” A takeaway message from this article is that national and international standards of records and information management provide guidance, but adherence is not legally required in most sectors.

Eastwood, T. (1996). Should creating agencies keep electronic records indefinitely? *Archives and Manuscripts, 24*(2), 256-267.

This article is Terry Eastwood’s direct response to David Bearman’s 1991 article “An Indefensible Bastion.” Eastwood argues that originating agencies should not keep electronic records indefinitely and that archival institutions fail in their mission if they do not gain custody of electronic records. The article begins by restating the insights Bearman provided in his article, namely: that archivists occupy a weak position in the organization; that the custodial role defined by archivists is not professional; that the economic requirement for archives to migrate data will not be met; and that cultural changes have rendered the physical locus of information increasingly irrelevant.

Eastwood counters the first point by focusing on the important role of public archives in preserving an authentic and adequate account of public actions in support of a vital democratic virtue. A fundamental role of archives is to establish and reveal the connections between electronic and non-electronic records of agencies, which Eastwood observes is difficult if the agency itself remains in charge of the electronic records. With these points in mind, Eastwood dismisses Bearman's second claim, observing that archivists must also consider appraisal, acquisition, arrangement, description, and referencing. Bearman's third argument regarding economics appears to Eastwood as the most seductive. However, Eastwood retorts that it could be more expensive for the creator to maintain the records, as it would require each creator to hire archival professionals, purchase special equipment, and maintain storage space and devices. In response to Bearman's final argument, Eastwood states that record creators are unable, in the long term, to guarantee trustworthiness and authenticity.
Eastwood subsequently discusses the various kinds of accountability served by records. These include uses of the record in the current records environment, public accountability (public assurance that the creator is fulfilling their duties), and historical accountability (need of a society to know its traditions, accomplishments, and failures). Eastwood concludes that the three kinds of accountabilities can only be provided by archives and not records creators.

Franks, P., & Doyle, A. (2014). Retention and disposition in the cloud - do you really have control? In B. Endicott-Popovsky (Ed.), *International conference on cloud security management ICCSM-2014* (pp. 51-58). Reading, UK: Academic Conference and Publishing International Limited.

The article focuses on retention and disposition of records residing in clouds. Two questions driving the article are "How does the use of cloud services affect our capability to retain and dispose of records in accordance with the law and other applicable guidelines?" and "What can be done to mitigate any risks arising from the gaps between our ability to apply retention and disposition actions to manage records residing within the enterprise and those residing in the cloud?"

The literature review focuses on what are considered records in organizations and on requirements for records retention and disposition (focusing on management standards). In the latter section, questions are raised about the establishment, application, and execution of disposition authorities, documentation of disposal actions, and disposition review. Several overarching issues are mentioned, such as metadata control and ownership, records portability, and digital continuity.

In the section titled “Mixed Trust Response to Retaining Information in the Cloud,” the authors reference Wang et al. (2012), who state that complex technological, systemic, cultural and political aspects of large enterprises often result in trust barriers to cloud adoption. The authors conclude that retention and disposition in the cloud becomes complex due to multi-tenancy, cross-border legal issues, and required assurances that copies in multiple locations are destroyed. The article references the InterPARES Trust literature review for retention and disposition in a cloud environment.

Gatewood, B. (2009). Clouds on the information horizon: How to avoid the storm. *Information Management, 43*(4), 32-36.

This article looks at cloud computing from the perspective of the software-as-a-service (SaaS) model, with specific focus on where information and records are stored. The article examines various SaaS solutions in cloud computing including communications, document management, structured data services, and business continuity. Although these business solutions look appealing, the author warns of the potential risks in using cloud computing, such as legal and regulatory concerns. In terms of legal concerns, the 2006 update to the *U.S. Federal Rules of Civil Procedure* is explored. One update to the legislation (Rule 26(a)(1)(A)(ii)) stipulates that an organization must provide its opponent a copy - or a description by category and location - of all documents and electronically stored information in its possession, custody, or control for use of claims or defense. Another update states that there is a 14-day period in which this information and documentation must be brought forth. In terms of regulation, audits and privacy concerns are highlighted. The issue of second- and third-tier vendors is also highlighted as a potential risk in terms of not knowing who has access to the organization’s data. The article concludes by describing the difficulties in enforcing records management practices in a non-centralized environment. A checklist for evaluating cloud-based initiatives is provided, covering contracts, audit controls, integration points, policies and procedures, and mapping of where the data resides.

Ghering, C., Caruso, J. B., & Gift, D. (2010). Electronic records management: Today’s high stakes. *ECAR Research Bulletin, 8* (1-13).

This research bulletin focuses on the management of electronic records in academic settings, some of which are applicable to other organizational contexts. The findings of this article are based both on the authors’ experiences and on Ronald Yanosky’s 2009 ECAR research study, “Institutional Data Management in High Education.” The bulletin highlights five keystones for a strategy to implement good records management practices. These are: staff collaboration and shared responsibility, authority and governance structure, standards and common tools, records retention schedules, and preservation environment for electronic records. The impact of cloud computing is mentioned within the section on standards and common tools. Additionally, the issue of archival custodianship is briefly mentioned in the section on records retention schedules, simply stating that information professionals talk in terms of "curation" of digital material throughout all of the stages in the life of a record.

Ham, F. Gerald. (1981) Archival strategies for the post-custodial era. *American Archivist, 44*(3), 207-216.

In this article, Ham examines how technological changes in the early 1980s have brought about the "post-custodial era." Two important themes explored by Ham are the benefits and detriments of new technologies in light of the amount of records generated and managed, and the proliferation of archival programs and institutions since the late 1960s. Ham presents an agenda to solve potential issues arising from these new technologies and from the decentralization of archival collections. The two key strategies highlighted are inter-institutional responsibility and outreach.

Hedstrom, M. (1991). Archives: To be or not to be: A commentary. In D. Bearman (Ed.), *Archives and museum informatics technical report: Archival management of electronic records* (pp. 25-30). Pittsburgh: Archives and Museum Informatics.
Hedstrom comments on some of the advantages and disadvantages of electronic records for achieving archival objectives. The commentary focuses on the custodianship of electronic records. Hedstrom references Ken Thibodeau ("To be or not to be: Archives for electronic records"), who points out that records need to be protected from changes in their content and character that would diminish their ability to reflect the information available to an organization at the time it was acted upon. Hedstrom does not agree with Bearman's argument in his article "An indefensible bastion" that custodianship is incompatible with an expanded role for archivists. The author concludes with a list of criteria for archivists to consider when appraising electronic records.

Henry, L. J. (1998). Schellenberg in cyberspace. *The American Archivist, 61* (Fall), 309-327.

The author highlights some of Schellenberg's key concepts in light of electronic records. The majority of the article contrasts Schellenberg's approach to archives with that of the "new paradigm," as represented by Bearman. Henry explores key issues including the definition of a record, appraisal, the records continuum, and custody. With regard to custody, the author observes that supporters of the new paradigm for electronic records promote the idea of post-custodialism, which considers centralized archives as "an archives of last resort." Henry notes that no national archives in Europe has yet to adopt a non-custodial approach.

Jenkinson, H. (1937). ***A manual of archive administration*****. (pp. 8-11, 32-38). London: P. Lund, Humphries & Co., Ltd.**

This seminal text by Hilary Jenkinson presents the classic perspective on archival custody and authenticity. The main points from the text are as follows: a record's quality is dependent upon the possibility of providing an "unblemished line of responsible custodians" (p. 11); documents become archives when they are "set aside for preservation in official custody" (p. 9); the duty of archivists is to "safeguard the essential qualities" of records in their custody (p. 15); and one of the main features of archives is that they provide authentic representations of an event or transaction (p. 12). Jenkinson describes how documents have historically been tampered with and forged in his discussion.

Lee, C. A., & Tibbo, H. (2011). Where's the archivist in digital curation? Exploring the possibilities through a matrix of knowledge and skills. ***Archivaria, 72*****, 123-167.**

The authors focus on the development of a course on digital curation, defined as active involvement of information professionals in the management (including preservation) of digital data. The course is divided into six dimensions: 1) mandates, values, and principles; 2) functions and skills; 3) professional, disciplinary, or institutional/organizational context; 4) type of resource; 5) prerequisite knowledge; and 6) transition point in the information continuum. Each of these sections discusses particular archival concepts, most notably the custody of electronic records.

The dimension most pertinent to our research is dimension six, transition points in the information continuum. Archival custody is defined as residing within an environment devoted to long-term preservation, such as a government archives, manuscript repository, or scientific data centre. The transfer to archives is defined as the point of movement across the "archival threshold" that can be relatively direct and instantaneous, or that can involve extensive operations and one or more "staging areas." The authors discuss the importance of establishing policies around formal transfer of records and examine what objects pass through transition points.

Lee and Tibbo stress the importance of coordinating work across institutional, regional, disciplinary, organizational, and professional social boundaries. This speaks to the aspect of our project that examines perspectives of the various actors in records creation and maintenance. The authors suggest that professionals are increasingly discovering policy vacuums where no guidance exists for new issues. This aspect is only dealt with tangentially throughout the article, as the focus remains on the development of a digital curation curriculum. Additionally, the article examines models that could be incorporated into the curriculum of a digital curation program, such as the OAIS Reference Model. The authors also discuss the Pittsburgh Project and InterPARES, respectively. According to the authors, a common theme of both the OAIS Reference Model and archival literature is the importance of attending to the wider socio-technical systems in which electronic objects are embedded, which for the purposes of our project would be cloud computing.

The authors note that an implication of post-custodial and continuum approaches is the emphasis on archivists' understanding of and engagement in environments where records are created, as opposed to passive waiting of records to eventually cross the archival threshold. However, there remains ambiguity around whether archivists should take custody of electronic records. Likewise, the authors emphasize the importance of archivists acting upon frequent calls to collaborate with allied professionals.

Loewen, C. (1993). The control of electronic records having archival value. *Archivaria, 36* (Autumn), 64-73.

The article begins by asking several questions, among them, "Should archives be the official repositories of electronic records with archival value?" The author states that this question is being addressed by the profession, referencing the *Archives & Museum Informatics Technical Report No. 13*, which investigates different aspects of electronic record acquisition and custody from the perspective of the National Archives of Canada.

Loewen highlights three conclusions that have been made in regards to electronic records. First, that any treatment of electronic records having archival value requires an integrated approach. Second, that each archives needs to adapt existing procedures to meet its particular needs, while simultaneously building upon core principles. Third, that most electronic records cannot even be read or understood without some knowledge of the evidential and technical information, which is often found in supporting documentation.

Given that this article was written in the early 1990s, several points have become outdated. Nevertheless, there are some aspects that remain pertinent. For example, the article suggests that archivists can never be consistently ahead of rapidly changing technology, and considers the possibility of "live" accessions. There is discussion of how control mechanisms for electronic records facilitate their appraisal, since electronic records reveal a greater overlap of the two principal archival functions than do textual records.

The authors provide an outline of the meaning of control of electronic records and the various issues that appear at different aspects of the archival acquisition process for electronic records. Of most use is the discussion on who should be the archival custodian if archives acquire electronic records. The other aspects mentioned include appraisal, archives as repository, data files as discrete items, metadata, archival principles, media myopia (the separation of acquisitions by media type), and researcher access and use.

O'Shea, G., & Roberts, D. (1996). Living in a digital world: Recognizing the electronic and post-custodial realities. *Archives and Manuscripts, 24*, 286-311.

The article begins by highlighting the fact that digital records can be made available to anyone anywhere in the world. The authors discuss issues of technological change and authenticity as evidence. They explain that there are three phases in the archival management of electronic records: non-custodial, custodial, and post-custodial. Although the non-custodial era is hard to date, the authors cite the NARA program in 1968 as the beginning of the custodial phase. Australian archivists, beginning with Ian Mclean, have interpreted Jenkinson's vision in the wider recordkeeping context rather than in the purely custodial context (guardianship versus possession).

The authors describe the custodial approach and various pressures it faces in terms of electronic recordkeeping (such as technological change, misunderstanding the nature of records, and the role of the creating institution in maintaining access in the short, medium, and long term regardless of the ultimate custodian). Examples of post-custodial strategies employed in the U.S., Canada, the Netherlands, and Australia are presented. One example of note for our project is the United Nations Technical Panel on Electronic Records Management (TP / REM) in 1987.

Oliver, G., Chawner, B., & Liu, H. P. (2011). Implementing digital archives: Issues of trust. *Archival Science, 11*, 311-327.

This study examines issues around the implementation of a digital archive. In particular, it considers issues related to custody and occupational culture. The authors note that archivists have not progressed significantly since the introduction of computer-generated records. In terms of occupational culture, there is an emphasis on how occupational communities develop similar worldviews that cut across nations. The article focuses mainly on archivists and information and communication technology professionals, which is also relevant when considering international organizations.

The study includes a survey of New Zealand information and communication technology professionals. The survey reveals a low level of confidence over whether recordkeepers know the best storage conditions for digital records, as opposed to paper records.

Schellenberg, T. R. (1956). *Modern archives: Principles and techniques.* Chicago: Society of American Archivists.

In this text, Schellenberg offers a counterpoint to Jenkinson's view on custody (pp. 14-15) by arguing that the creation of records in modern administrations makes it extremely difficult to determine proof of "unblemished lines of responsible custodians," and therefore "unbroken custody" cannot be a test of archival quality. Rather, the integrity of records should be maintained by the following requirements: records given by an agency should be kept together as records of that agency; records should be kept, as much as possible, in their original order; records should be kept in their entirety without mutilation, alteration or unauthorized destruction of portions of them. Schellenberg states, "The evidential value of his materials [i.e. archival records] rests on the way they were maintained in the government office, and the way they came to the archival institution; not in the way in which individual documents were controlled within the government office" (p. 15). Schellenberg addresses the concept of custody by explaining that public records may be held in the custody of an agency, but they are not the property of the agency. When public records are transferred from one custodian to another, there is no transfer of ownership; the records continue to be the property of the state. The terms under which the records are held depend upon the statutory provisions that govern the transfer of records (p. 125).

Stancic, H., Rajh, A., & Milpsevic, I. (2013). "Archiving-as-a-service": Influence of cloud computing on the archival theory and practice. In L. Duranti, & E. Shaffer (Eds.), *The memory of the world in the digital age: Digitization and preservation* (pp. 108-125), UNESCO.

The article begins by examining the paradigms instilled in archival science, the notion of post-custodialism as presented by Gerald Ham, and the records continuum model. The first section notes that during our current time of technological change and proliferation of cloud services, post-custodial practices face a great challenge.

The second section discusses the digital preservation environment in the context of the three cloud-computing deployment models (SaaS, PaaS, IaaS) and the four service models (private, community, public, hybrid). The authors propose that archival and digital preservation services should be offered as components and features within the four models.

The third section outlines the transition to cloud services. In addition to the accessibility of cloud services via an internet connection, there is also the potential for cloud services to offer (semi)-automatization of digital preservation functionalities. This includes analytical tools to determine obsolete file formats, conversion of content into higher or more stable formats, and validation of authenticity of the content. The authors stress that the archival community should realize their potential influence within the realm of cloud digital preservation.

The fourth section details the move from custodialism to post-custodialism, and proposes that we are now entering post-custodialism 2.0. The provision of archival services in this regard consists in more than just providing a repository for digital objects, but should also include the archival management of digital objects. Management functions would include security mechanisms, protection of holdings and data assets, contextual links with creators, and long-term preservation mechanisms.

The fifth section of the article presents the results of a survey by the authors of a global corporation with offices in 58 countries. The survey questioned participants' familiarity with cloud computing, use of cloud computing, what kinds of sensitive materials are stored on their private cloud, and backup technologies used within their private cloud.

The sixth section imagines several cloud computing scenarios, including service providers being responsible for control of archived content, creators investing effort and additional control of non-standardized services, standardization of services through best practices, and/or archival community involvement in new archival practices and influencing cloud providers' services.

The final section provides conclusions and avenues for future work on this topic. In this section the idea of "post-custodialism 2.0" is clarified as being a reaction to the limited capabilities of the archivist to supervise archival procedure within creating institutions.

Thibodeau, K. (1991). To be or not to be: Archives for electronic records. In D. Bearman (Ed.), *Archives and museum informatics technical report: Archival management of electronic records.* Pittsburgh: Archives and Museum Informatics.

Thibodeau begins by stating that if the interdependencies of records are not transferred to an archival environment, preservation is irrelevant. Conversely, if records cannot be preserved, establishing archival control is futile. Thibodeau lists four motivations for creating and keeping records: to do business, to support the conduct of business, to document business, and to manage risks incurred by being in business. There is a difference between the operational and archival value of records. In order to ensure the intrinsically historical nature of archival value, records must be removed from the operating environment and transferred to an archival environment. Thibodeau also offers a brief discussion of archival experience in preserving electronic records.

Much is made of the issue of transferring automated data files (such as database management systems) to an archival repository, since it preserves the record in a flat file format rather than in the original dynamic format generated by the creator. Thibodeau asserts that in order to preserve electronic records, it is sometimes necessary to alter their technological characteristics. Electronic records migration, relational database data, and Open System Interconnection (OSI) standards are discussed in this light. The transfer of data in a relational database to an archival environment necessitates defining the tables to be transferred, specifying the links between tables, and removing them from the operating environment.

From his analysis of relational database archival preservation, Thibodeau concludes that the operational environment is not enhanced by imposing a requirement for archival preservation, and warns that inefficiencies will inevitably occur. Although it is difficult for archives to acquire, preserve, and provide access to a range of collections from different sources, it is simpler than maintaining archival records as part of active databases. Elements within databases may change (eg. more columns could be added to a table), which affect the records generated but not the contents of the records. Therefore, records generated before design changes should be separated from those records generated after any changes.

Tough, A. G. (2004). The post-custodial/pro-custodial argument from a records management perspective. *Journal of the Society of Archivists, 25*(1), 19-26.

The article begins by examining arguments for both post-custodialism and pro-custodialism in archival terms. The cited authors include Upward, O'Shea, Duranti, and Hedstrom. Tough notes O'Shea's suggestion that the duty of the archivist is to manage records in an accountable manner no matter where they are located. This is countered by a quote from Luciana Duranti on the importance of migration by a neutral party to a permanent repository. The article discusses the 'metadata systems approach,' which proposes the inclusion of descriptive elements in the design of metadata systems.

This analysis leads the author to conclude that there are two issues with the post-custodial/pro-custodial debate. The first issue is the assumption that archival interests can and should dictate records management policy. The second issue is that the discussion has been conducted at a highly theoretical level with little reference to empirical evidence. Tough subsequently analyzes the debate from a records management perspective. In this analysis, Tough states that the post-custodial approach is particularly well-suited to some kinds of records, such as large databases.

In the section entitled "The future," Tough describes the "Create Once, Use Many Times" project based out of Monash University's School of Information Management and

Systems, which uses the metadata systems approach. He also references ISO 15489 (a guidance standard based on records continuum thinking) and the American DoD 5015.2 (a compliance standard based on post-custodial thinking).

Upward, F., & McKemmish, S. (1998). ***Somewhere beyond custody.***

Upward and McKemmish offer a brief introduction to post-custodial theory, which has a discourse and provenance theory rooted in a new language where traditional concepts can have more than one meaning. The authors briefly outline some of the basic features of the theory, including: a re-definition of records and recordkeeping as a starting point; the power of provenance; the focus on appraisal and documentation; the functional requirements for recordkeeping systems; and the importance of metadata.

The section entitled "The International Literature" begins with the example of a 1990 report produced by the UN Advisory for the Co-ordination of Information Systems (ACCIS) entitled *Management of Electronic Records: Issues and Guidelines*. Much of the content of the report, Upward and McKemmish state, reflect the views of David Bearman, one of the main authors of the report. Emphasis is placed on the records systems, the capture of records, and the need for metadata. Australian coalface literature is described, which focuses on the transactionality of records and the dangers of mistaking the principles and practices of data management, information management, or document management for records management principles and practices.

In the conclusion, the authors note that at the time of publication, post-custodialism was still in the process of defining itself. They provide a list of basic features of post-custodialism, such as the redefinition of records and recordkeeping, appraisal based on functions and activities rather than on the physical record, the principle of provenance, the importance of metadata, the archival institution as a hub or node in a network, and an emphasis on the outcomes (accountability through time and space) of archival work rather than its outputs.

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.

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

The author reports on the status of records and archives management (RAM) in the United Nations, based on the results of a 2012 review by the UN Joint Inspection Unit. The review aims to determine whether effective management of records and archives is enabled by the current set of UN policies, procedures, and related instruments pertaining to archives and records management. The review refers to the standard ISO 15489 as a basis for evaluation.

Findings from the review result in six recommendations directed to the United Nations Group. A major observation of the report is the lack of a unified approach to records and archives management across UN entities, leading to variations in regulatory frameworks within the UN. Policies are often unaccompanied by provisions to carry out the work that is mandated, and practical guidelines and clarity regarding corporate roles and responsibilities is also needed. The report recommends the development of an overarching policy and principles framework unifying the various RAM instruments across all UN entities.

Records and archives management 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). Despite this, records and archives management is often not integrated with other information management functions, such as knowledge management (defined as "the capture, dissemination and updating" of key organizational knowledge) and information technology ("technical and operational effectiveness") (p. 29). Moreover, records and archives management ("the organization of information and compliance rules") is perceived as having secondary importance, a status partially attributed to the recruitment of chiefs of archival units within middle management (staff classification P5), rather than senior management (D1 or D2).

In general, two emerging models for RAM in the UN are observed. The first is a centralized approach consisting of a dedicated corporate unit staffed by professional archivists and records managers, exemplified by ARMS in the Secretariat, and the Records and Archives Section (RAS) at the Office of the United Nations High Commissioner for Refugees (UNHCR). The second model is a decentralized approach characterized by corporate stakeholders, such as administrative and information technology divisions, among others, that undertake RAM functions. This is the predominant model in UN funds and programmes. Additionally, fourteen record centres support recordkeeping for UN missions, yet handle only paper records, while digital records are managed by information technology units. The Archives and Records Management Section (ARMS) at Headquarters is working with the Department of Peacekeeping Operations (DPKO) and the Department of Field Support (DFS) to address these issues.

The author recognizes the trend in the adoption of new technologies such as cloud computing by various UN entities. Digital records need to be better managed, as there is currently no cohesive digital recordkeeping and preservation strategy. The use of digital technologies and remote and collaborative platforms reinforces the need, among other recommendations, for an overarching policy and principles framework for UN records management.

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.

This report by the Joint Inspection Unit (JIU) outlines recommendations to the United Nations (UN) as a whole on the adoption of enterprise resource planning (ERP) systems. ERPs are those systems that deal with human resources and system management. As such, issues including centralization, financial costs, data conversion and updating, and hosting are discussed.

The review highlights the UN's implementation of its ERP project Umoja. Umoja is an ERP that will aim to cover all human resource management for the UN. It is still in its deployment phase, with all UN Secretariat entities having deployed the technology in November 2014. For the purposes of this report, the JIU surveyed UN entities on what ERP systems they have implemented. From the information provided, it is clear that not all units are using the same base systems (divided between Oracle, SAP, and Agresso respectively). It is also noted that the transition to a single system is not an information and communication technology (ICT) project, but rather a "major business transformation."

The report discusses different implementation methods (the all-at-once "big bang" approach versus a piecemeal approach). Other aspects of ERP adoption are discussed, including the selection process (mostly through a competitive bidding process), project staffing (fear of staff leaving after the initial implementation phase is complete), training and support, jurisdictional concerns, and data archiving.

The report describes some of the issues surrounding cloud computing. First, it states security and data confidentiality concerns complicate the challenges. There is mention that UN-Habitat is negotiating to procure a cloud-based system for project management while waiting for Umoja to be implemented. The experience of other international organizations with ERP systems, including cloud computing, is mentioned. In particular, the experiences of the IMF and World Bank are highlighted. The report ends with a comprehensive chart outlining each of the UN units' experience with ERP technology, including implementation dates and specific uses.

***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.**

This Communication is part of the Digital Initiative for Europe, itself an initiative within the Europe 2020 Strategy. The Communication introduced both the European Interoperability Strategy (EIS) and the European Interoperability Framework (EIF). The interoperability in question refers to interoperability between Member States of the European Commission, rather than interoperability of the communication software itself. However, Digital Initiative provides some insight into to why cloud computing is difficult to initiate in international organizations. For example, challenges include the different legal environments of Member States, lack of common infrastructures, multilingualism, and lack of agreement on the format of information.

The Communication subdivides the EU into separate sectors, indicating a somewhat fractured approach to the topic. However, the experience of each sector is shown as positive in regards to interoperability between Member States. The EIS itself includes public service delivery through appropriate government organisation and processes, and trusted information exchanges enabled by commonly-agreed interoperability initiatives. Specific activities include: trusted information exchange, interoperability architecture, and assessment of the ICT implication of new EU legislation. These activities are explained in detail in the document. The EIF adopts an agreed-upon approach to interoperability for organisations. It includes the 12 underlying principles, a conceptual model for public services, four levels of interoperability (legal, organisational, semantic, and technical), and the concept of interoperability agreements.

Overall, the aim of this document is to instill in Member States the reasons for developing interoperable communication technologies with their counterparts. As this Communication was made in 2010, some of the dates have passed. For instance, the Ministerial Declaration on eGovernment stated that by 2013 national interoperability frameworks will be aligned with applicable European frameworks.

***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**

This bulletin issued by the United Nations General Secretariat 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 bulletin defines archives as “records to be permanently preserved for their administrative, fiscal, legal, historical or informational value” belonging to the United Nations, “regardless of physical location, [including] paper-based and electronic records” (p. 1). 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 the development of procedures for the “appropriate identification, handling and management of sensitive records” (p. 4).

Responsibilities of staff members include the requirement to recognize that all documents created for work purposes are the property of the UN and are not to be destroyed, altered, lost, or rendered unusable unless mandated by a retention policy approved by ARMS. As well, before leaving the service of the UN, staff members should make arrangements for the transfer of records to ARMS, but are permitted to keep private papers and to make copies of unrestricted records within reason. Among the responsibilities of work units is the development of a retention policy and retention schedule approved by ARMS, and the preparation of records for transfer to ARMS according to established guidelines.

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.

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.

This article proposes that the assessment of security risks involving cloud computing should involve both the cloud client (CC) and the cloud service provider (CSP). It begins by establishing the functionality of cloud computing and pertinent regulations and research. In comparison to the public, community, and hybrid models, trust in the private cloud is highest because in the latter, infrastructure and assets are managed and used by well-known entities.

The author describes the steps involved in performing a risk assessment. In the case of a security breach, it is the CC who knows the true value and the real potential consequences. The CC’s involvement in all of the risk assessment steps will unnecessarily complicate the assessment itself. Therefore, CCs should only be involved in parts, and not the whole of the assessment.

The second section of the article outlines several information security risk assessment approaches. This includes the National Institute of Standards and Technology Guidelines, The International Organization for Standardization Standards, and Control Objectives for Information Related Technology.

The third section delves into the specificities of risk assessment in cloud computing. Many reports are references in this section and may provide guidelines for how to approach the perception of risks. For example, risks are often subdivided into categories, such as policy and organizational risks, technological risks, legal risks, company (organization) risks, and cloud service provider risks.

The fourth section proposes a framework for assessing risk in cloud computing environments. Since the authors of this paper do not wish to complicate the assessment by involving CCs in every aspect of the assessment, they limit their contribution to three tasks: defining legal and regulatory requirements, identifying security risk factors, receiving feedback from the CSP and applying the required security tasks. The author provides a detailed outline of what is involved in performing the risk assessment and the conclusion.

Australasian Digital Recordkeeping Initiative. (2010). *Advice on managing the recordkeeping risks associated with cloud computing* (No. ADRI-2010-1-v1.0). Council of Australian Archives and Records Authorities.

This advice piece was developed by the Australasian Digital Recordkeeping Initiative working group of the Council of Australasian Archives and Records Authorities. It provides a list of benefits, barriers, and concerns that governments need to consider when adopting cloud computing. The document outlines how to identify different risks, how to assess risks for different records, and stresses the importance of being diligent when entering into agreements with cloud computing service providers. The appendix features a checklist for government organizations considering the adoption of cloud computing. Overall, this is a great cursory document for those not aware of the risks in cloud computing.

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.

This article focuses on one way of ensuring security in PaaS cloud computing, that of information flow control. Information flow control (IFC) is a data-centric security mechanism that tracks and enforces information flow.
The article begins by highlighting the different security concerns between PaaS, IaaS, and SaaS models of cloud computing. The authors continue by outlining the concept of IFC. IFC is a type of Mandatory Access Control (MAC), meaning that access is defined for the entire system, unlike Discretionary Access Control (DAC), wherein permissions are modified at the discretion of the owner of the data. The authors state that IFC can be used to enforce general policies by using appropriate labelling and checking schemes. An example is adding a system of privileges to introduce carefully controlled additional components into the Trusted Computing Base. A decentralised IFC system (DIFC) is one in which a central authority is not needed, and thus would be ideal for a cloud computing environment. The section includes examples from the American military, where this method was first used. However, some crosscutting technical security concerns for a DIFC in cloud computing include the regulatory framework, multitenancy, access control enforcement, and accountability. Within the section on regulatory framework, issues such as data protection, compliance, and the location of data are mentioned.

The third section of the article deals with information flow control design and provides different methods dependent on the system operation status, data isolation, how the system tracks data flow, and how the system uses data flow tracking to enforce data flow. The fourth section deals with threats to IFC systems, not including malicious intent on the part of the developer. The fifth section outlines how to implement DIFC systems.

Chen, L. S. (2010). The impact of perceived risk, intangibility and consumer characteristics on online game playing. *Computers in Human Behavior, 26*(6), 1607-1613.

Chen defines perceived risk as “the degree to which the consumer feels the uncertainty and consequences associated with their actions and play a critical role in consumer decision-making” (1608). Perceived risk appears when an individual is involved in a situation where the outcomes are uncertain and is worried about the consequences of an unsuitable decision. The article examines perceived risks of online game playing in light of intangibility and consumer characteristics, which is not relevant to our research.

Dorofee, A. J., Walker, A. J., Alberts, C. J., Higuera, R. P., Murphy, R. L., & Williams, R. C. (1996). *Continuous risk management guidebook*. Carnegie Mellon University, Pittsburgh: Software Engineering Institute.

This text describes the Software Engineering Institute’s Continuous Risk Management (CRM) approach to mitigating risks. The authors describe examples of CRM implementation, explain how to start CRM, and provide forms and templates for CRM activities. CRM is an ongoing process and a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to: assess continuously what could go wrong (risks); determine which risks are important to deal with and implement strategies to deal with those risks (p.4). The functions, or steps, within CRM are: identifying risks, analyzing risks, planning for risks, tracking risks, controlling risks and communicating risks. The guidebook details the activities, principles and methodologies associated with the steps of CRM and how best to implement the functions and principles into everyday practices.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21*(1), 119-134. http://www.jstor.org/stable/2489744

This article offers a study of different factors influencing consumer's perceived risks related to purchases, and describes average versus alternative product selection and how those two ideas affect consumers' information-search behaviours. The authors conclude that more searching is performed in high-risk purchasing situations.

The article begins by providing a brief overview of literature on risk and perceived risk. There are two specific aspects of perceived risk in purchasing: the magnitude of consequences and the probability that the consequences may occur if the product is acquired. Therefore, the consumer's knowledge of and experience with the product is paramount in decision-making. Search activities, such as the gathering of colleagues' opinions) are influential in the purchasing/adoption process. Table 1 of the article deals with the attributes used to describe the product. Although these attributes are specific to the study (the purchasing of a dress), it highlights the various types of consequences the purchase may have, such as psychological, social, monetary, and functional.

Additionally, Exhibit 1 states the operational definitions for variables in the risk-handling model. These include product attributes, purchase goal, purchase situation, monetary costs of replacement, overall perceived risk, situation-specific risk, product-category risk, acceptable risk, benefits of search, cost of search, and search strategy use. These factors highlight that risk perception contains a cognitive and an affective component. The article concludes by stating that future research is necessary to support the theory that consumers search until they are able to reduce their specific risk to a level below their acceptable risk.

Overall, this article provides a framework in which to measure perceived risk, which may be useful in determining who in the IOs are most concerned with cloud adoption. It also illustrates variables that can be considered when analyzing interview responses.

Eggert, A. (2012). Relationship between intangibility and perceived risk: Moderating effect of privacy, system security and general security concerns. *Journal of Consumer Marketing, 29*(3), 176-189.

The article focuses on the perception of risk in terms of online shopping, and outlines three kinds of intangibility: physical, mental, and general or specific. Physical intangibility relates to the five senses, while mental intangibility concerns the ability to understand a product (in our case cloud-computing services), and general or specific intangibility refers to how abstract the benefits of the product or service are (a CD versus a carpenter). The article features a diagram explaining the relationship of intangibility to perceived risk.

The study found that high levels of privacy concern generated a stronger relationship between mental intangibility and financial and psychological risks. Perceived risk is increased when two negatively loaded pieces of information are processed.

Kalyvas, J. R., Overly, M. R., & Karlyn, M. A. (2013). Cloud computing: A practical framework for managing cloud computing risk - part I. *Intellectual Property & Technology Law Journal, 25*(4), 19.

Part One of this two-part article recommends clauses that businesses should include in their contracts with cloud service providers. According to the authors, businesses that move to use cloud computing should assess the attendant risks based on two factors, the "criticality of the business process being supported," and the "sensitivity of the data" to be stored in the cloud. Because hardware, software, and user data are hosted by the cloud service provider, the concerns in a cloud computing environment are on service availability, service levels, data security, and control. The authors recommend clauses related to the first two issues, including provisions for disaster recovery; backups and copies; data ownership; access to data; termination rights; a prohibition on withholding of services by the provider; availability of services; and limitations on allowable downtimes for the provider, among other clauses. The authors urge users, as much as possible, to fix the contract terms, since such terms are often internet- or cloud-based and providers often change the terms of service without notifying users. A discussion of how cloud computing differs from ASP (Application Service Provider) and SaaS (Software as a Service) service models is also included.

Kalyvas, J. R., Overly, M. R., & Karlyn, M. A. (2013). Cloud computing: A practical framework for managing cloud computing risk - part II. *Intellectual Property & Technology Law Journal, 25*(4), 19.

The second article of this two-part series recommends cloud computing contractual provisions to support data security and control for the customer. To ensure data security, the authors recommend that customers undergo 'due dilligence' research on their prospective cloud service providers by investigating where their server centers are located, who may have access to them, and who operates them. Customers can include a clause confining data flow to their own country (in this case, the United States). The authors suggest specific contractual clauses that could be included if the provider is using a third-party host for customer data, and recommend being aware of the provider's "baseline security measures" and security policies. They also provide sample provisions for some of the issues they raise. Other issues the authors address include; data redundancy, data ownership and use rights, data conversion, insurance, indemnification, intellectual property, fees, exclusivity (when the provider demands that customers cannot use other cloud service providers), negotiating power, evaluation of services, and more. The authors conclude by emphasizing the risky nature of cloud computing, but reiterate that the customer can mitigate risk by focusing on "service availability, performance, and the security and control of the customer's data" in drawing up contractual terms.

Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud computing risk assessment: A systematic literature review. In J. J. Park, I. Stojmenovic, M. Choi & F. Xhafa (Eds.), *Future information technology: Future Tech, 2013: Volume 276 of the series [Lecture Notes in Electrical Engineering](#)*. (pp. 285-295). http://link.springer.com/chapter/10.1007/978-3-642-40861-8_42.

This chapter provides an overview of literature produced between 2009 and 2013 on the subject of risk assessment in cloud computing. The authors divide the literature into two research questions: risks from the cloud service providers' perspective and risks from the cloud customer perspective. The two questions are addressed by examining risks to data security and privacy, technology, physical security, organization, and compliance and audit. It should be noted that organizational risk is only addressed from the point of view of cloud service providers and not from that of cloud customers.

Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to internet and e-commerce usage. *Qualitative Market Research: An International Journal, 5*(4), 291-300.

Liebermann and Stashevsky focus on the adoption of internet and e-commerce practices among employed adults in the early 2000s. As with other studies, perceived risk is stated as having a multidimensional nature. Privacy and security are defined as components of perceived risk. Miyazaki and Fernandez (2001) are view perceived risk as a derivative of the novelty of internet use, but the authors of this article view novelty as an independent risk component. Liebermann and Stashevsky also investigate in detail demographic differences, including age, gender, marital status, and education. Demographic differences feature in the authors' model of factors affecting perceived risk elements.

McKemmish, S. (2013). Recordkeeping and archiving in the cloud. Is there a silver lining? *INFuture 2013: Information Governance,* 17-29.

This paper focuses on developments in the National Archives of Australia (NAA), the Public Record Office of Victoria, and the Cloud for Europe initiative. McKemmish begins by establishing basic concepts of cloud computing, including what it is and the different services it can provide. This is followed by an in-depth survey of Australian responses to cloud computing.

For the most part, the survey focuses on the NAA's provisions for risk assessment, including a checklist developed in 2011. Seven risk categories and two checklists have also been developed to assist Australian government organizations planning to put their records in the cloud, particularly the public cloud. The risk categories include location and legal jurisdiction, transparency accountability governance, protection of rights in records, recordkeeping functional requirements, digital continuity, vendor lock-in, and commercial continuity. These categories are outlined and examined in detail throughout the article. McKemmish notes an article by Stančić, Rajh and Milošević (2012) that introduces the concept of Archiving-as-a-Service (see Stancic, Rajh, and Milosevic in "Archives and Custody").

Mitchell, V. (1995). Organizational risk perception and reduction: A literature review. *British Journal of Management, 6*, 115-133.

By focusing on the effects of perceived risk to an organization rather than to an individual, this article differs from most other literature on risk perception. The article begins with a literature review presented as an extensive list of factors that can affect an organization's risk perception. Although the majority of the listed factors are clearly present in individual consumers as well, certain factors such as job function, approved supplier list, company size, and decision-making unit are all unique to the organizational perspective. This list of factors is followed by eleven comments, criticisms, and questions. These include: the fact that most of the studies have focused on profit-making organizations; that this is not an exhaustive list; that questions can be raised as to the types of loss that exist for organizations; and how risk varies over time. This is followed by a list of possible risk-reducing strategies for each of the factors outlined in the literature review.

The article provides a good framework for future research into organizational risk perception. However, only the manager's view in organizational risk perception is thoroughly examined. Although there is a section on Group Decision Making, there is no discussion on how the individual employee's professional experience and knowledge affects this process.

Munnukka, J., & Järvi, P. (2014). Perceived risks and risk management of social media in an organizational context. *Electronic Markets, 24*, 219-229.

Like Mitchell's "Organizational Risk Perception and Reduction," this study focuses on whether social media strongly influences the adoption and use of any new product, service, or medium of marketing communication (p. 219). The study includes "content sharing" as part of social media, though from a marketing point of view and not as part of an internal workflow. Munnukka and Järvi express a continuing need to focus on an organization's perception of risk, the forms and types of risk, and the means of managing risk in the context of adopting new services (p. 220). They conceive of seven dimensions of organizational decision-making risk: technical, financial, delivery, service, personal, relationship, and professional (p. 220-1). Importantly, iindividuals within an organization have varying degrees of influence on other members of the organization (p. 221). Procedural control (including policies, procedures, and informal 'rules of thumb') and proactive focusing (establishing objectives and plans) are postulated as having a significant effect on an organization's perception of risk and its decision-making process (p. 221-2).

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27*, 245-253.

This article outlines specific risks that governments must consider when implementing cloud computing. The majority of the article focuses on the United States. The authors briefly discuss the concepts of risk, risk management, and cloud computing before exploring governmental use of cloud computing, focusing on U.S. federal adoption and use of cloud computing. Cloud adoption has outpaced the implementation of policies and regulations. Risks examined in the context of government adoption of cloud computing include access, availability, infrastructure, integrity, and intangible risks.

Slovic, P. (2000). Perception of risk. In P. Slovic (Ed.), *The perception of risk*. London: Earthscan Publications Ltd, pp. 230-231.

This chapter outlines the basics of risk perception, from the concept itself to then-current research being conducted. It argues that one strategy for studying perceived risk has been the development of a taxonomy of hazards. The most common approach with respect to this has been the psychometric paradigm which uses psychophysical scaling and multivariate analysis to produce quantitative representations. Slovic then concludes, through his own research and the research of others, that psychometric techniques can be appropriate to identify similarities and difference regarding perceptions of risk. They have also shown that the concept of 'risk' can mean different things to different people. This leads to a discussion of how experts' perception of risk differs from that of laypeople: whereas experts base their perception of risk on annual fatalities, laypeople tend to consider other hazard characteristics such as catastrophes or threat to future generations.

The article also discusses accidents as signals of future catastrophe. In this section, Slovic points out that if an accident takes place as part of a familiar and well-understood system will produce less social disturbance than a small accident in an unfamiliar system. For the purposes of our research, cloud-computing can be considered as the system.

Slovic, P., Fischoff, B., & Lichenstein, S. (1982). Why study risk perception? *Risk Analysts, 2*(2), 83-93.

The authors address seven major questions related to risk perception: what are the determinants of perceived risk; how and why do laypersons' perceptions of risk differ from those of experts; what information is needed to foster enlightened individual and social behaviour with regard to risk issues; what is the role of judgement in technical assessments of risk; how do people perceive the benefits of risky technologies; what determines the acceptability of hazardous technologies; and what makes a risk analysis acceptable.

The research conducted for this article resulted in seven generalizations. First, perceived risk is quantifiable and predictable. Second, "risk" means different things to different people. Third, even when a group disagrees on the overall riskiness of specific hazards, they generally rate the characteristics of those hazards similarly. Fourth, risk characteristics (knowledge, controllability, dread, catastrophic potential) are highly correlated with each other across a wide domain of hazards. Fifth, many of the various characteristics of risk correlate highly with a layperson's perception of risk. Sixth, people's tolerance for risk appear related to their perception of benefit. Seventh, accidents serve as signals regarding the probability and magnitude of further mishaps. For instance, if the situation is seen as common, such as a train crash, then risk perception would not change. However, if the situation is not common, then risk perception would change from low to high.

The authors present a critique of risk-perception research. Virtually anything can be a determiner of risk perception, and the use of psychometric methods tacitly accepts the notion that there is a level of acceptable risk. The authors describe the implications of the research in policy formation and analyze how people compare risks. They conclude that perceptions of and attitudes towards risk are determined not only by uni-dimensional statistics, but also a variety of quantitative and qualitative characteristics, including a degree of controllability, the dread it evokes, its catastrophic potential, and the equity of its distribution of risks and benefits (p. 91). Overall, the article provides a firm basis for further research into risk perception and shows some of the scientific methods involved in determining perceptions of risk.

Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. *European Journal of Marketing, 27*(3), 39-50.

The article begins by examining the development of risk perception studies across various fields, from its origins in consumer behaviour research in the 1960s to economics, psychology, and statistical decision theory research in the 1980s. One important idea brought forth is that outside of marketing literature there is a distinction made between "risk" (the number of possible events exceeds those that will or can occur) and "uncertainty" (when no probabilities can be attached to each possible outcome). The study itself addresses three hypotheses. First, that the six dimensions of risk (financial, performance, physical, psychological, social, and time) will explain a highly significant portion of overall risk. Second, that psychological risk will be correlated with the other dimensions of perceived risk. Third, that the dimensional structure of risk is such that the various risk dimensions are mediated through individual psychological risk to influence overall risk. Support was found for the second hypothesis; however, the first and last hypotheses were only partially supported. This may be due to the nature of the method employed, where not all dimensions played an equally significant role in the decision-making process.

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.

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

Chapter 6 of this text by Ademola Abass situates international organizations in their legal context and identifies their rights and duties, including jurisdictional immunity and inviolability of premises and archives. Abass differentiates between various types of international organizations and summarizes their differences in Table 5.1, "Typologies of international organizations," and discusses some of their similarities (p. 161). The chapter focuses exclusively on public international organizations such as the United Nations (hereinafter referred to as "international organizations"). Abass concludes that the best definition of international organizations is articulated by the International Law Commission (ILC), which acknowledges, where other definitions fail to do so, that IOs may be established by other instruments besides treaties, and may have non-State members (p. 159).

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 (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 (p. 167-68). 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" (p. 174).

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' (p. 191). Jurisdictional immunity refers to "immunity from prosecution or jurisdiction," which allows international organizations to "function independently and without fear of judicial harassment on the territory of its host State," including exemption from court summons and property seizure (p. 191). Inviolability is typically written into treaties, such as the UN Headquarters Agreement with their United States host, and the 1946 UN Immunities Convention. Abass notes that inviolability is an absolute term and applies not only to documents owned by international organizations, but to documents "held" by them, suggesting that all documents in custody, whether or not they belong to the organization, are inviolable (p. 197-98). In practice, enforcing inviolability is problematic since international organizations "are not sovereign entities, and...do not have their own bodies of laws such that apply to day-to-day transactions" (p. 198). Therefore, an international organization 'may suffer wrongs without remedies' (p. 198).

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

In *The Legal Position of Intergovernmental Organizations* Peter Bekker sets out to approach the question of the legal status of international organizations from a functional necessity lens and clarify an understanding of this body of knowledge as separate from "other branches of public international law," particularly sovereign immunity law (p. 5). Bekker explains that even though the law of immunities of international organizations shares some of the principles of sovereign and diplomatic immunity law, especially that of functional necessity, there are significant differences between the law of immunities of international organizations and the aforementioned related fields.

Bekker argues that the functional necessity approach focuses on an organization's functions and purposes and thereby leads to a theory "that is characterized by the consistent use of terminology proper to international organizations and that does justice to the principle of the *specialty* of the international organization" (p. 5). He adds that the functional necessity test is "relative" rather than "absolute," making it possible to tailor the functional needs and purposes of international organizations on a case-by-case basis (p. 5). Bekker goes on to point out that "there is an indefinite variety of such [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).

Bekker offers a three-step approach using a "functional typology" to determine the legal position of international organizations: "*identification* [emphasis added] of the entity concerned, by studying its legal status, i.e., its personality, capacity and competence (powers) by reference to an organization's purposes and functions, in order to assess whether it has a functional need for protection by way of privileges and immunities"; application of "the *basis-element* [emphasis added] of functional necessity in monitoring and selecting privileges and immunities for a given organization"; examination of "the value of the functional necessity concept as a yardstick for determining the *scope or extent* [emphasis added] of selected immunities" (p. 6).

Bekker is clear that the privileges and immunities of international organizations can only be justified and granted on the basis of "certain basic considerations and principles," most importantly that of functional necessity (p. 96). Bekker goes on to explain the relationship between privileges and immunities and functional necessity in more detail: "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 outlined in this study" (p. 96-97).

The author also goes into detail about the relationship between functional necessity and political independence of the international organization. He argues that the idea of functional necessity is "based on the idea of independence of international organizations from any one of its member states or any one bloc of its member states" (p. 100). Bekker continues by offering the notion of "functional independence," which he argues "can be ensured by the granting of such privileges and immunities as may be necessary to enable the organization to exercise its functions in the fulfillment of its purposes" (p. 100).

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

Won-Mog Choi investigates how the internet has changed the way that diplomatic missions and consulates communicate and function, and calls for updates to international law to reflect those changes. The article is divided into four sections: the first and second sections investigate general and specific effects of the internet on diplomacy; the third section looks at implications of internet technology on international law and customs relating to "inviolability of premises, inviolability of documents and archives, freedom of official correspondence, privilege of tax exemption, and immunity from judicial jurisdiction" (p. 117); and the last section provides a summary and recommendations for the future. Although the article is not specific to international organizations, the author addresses diplomatic missions and the principles of inviolability and jurisdictional immunity in the context of twenty-first century technology.

Choi studies articles in the Vienna Convention on Diplomatic Relations (VCDR) and the Vienna Convention on Consular Relations (VCCR) to determine the applicability of the inviolability concept to new forms of internet-based "disaster" situations, such as cybercrimes and cyber attacks taking place within diplomatic and consular premises. According to Choi, the VCCR could be interpreted to permit entry into consular premises by State agents without the consent of consular officials, while the VCDR, which has a stricter understanding of inviolability, would not permit entry into missions even in the case that a cyber crime is being committed on the premises. In general, Choi suggests that these instruments "may be extended to apply to 'cyber crimes' committed inside the premises" (p. 131). Elsewhere, Choi recommends that the inviolability principle should apply to 'all types of "electronic documents,"' (p. 131) including "disposable files…web-pages or binary codes saved in the main system computer of the mission or post" to prevent them from being "opened, searched, or requisitioned against the will" of officials (p. 123). Laws concerning free communication of diplomatic and consular agents also need to reflect the rise of email communication, which is replacing "diplomatic bags or messages in cipher" as primary means of communication (p. 124). Therefore, the VCDR and VCCR should be updated to include the notion of a diplomatic or consular "cyber bag" to "designate a cluster of electronic files or information" transmitted electronically, which, like its physical counterpart, would have "a visible external mark of its character" and enjoy special protection and inviolability (p. 127).

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

This article examines the extent of the inviolability of diplomatic archives, and considers inviolability as it is applied under international law (p. 26). Diplomatic archives refer to the archives of nations that are located outside of the home state, rather than to the archives of international organizations. However, many aspects of the principle of inviolability in diplomatic archives are also applicable to the archives of international organizations (see also Díaz-González, Leonardo, *(Consolidated) Fifth report of the Special Rapporteur on relations between States and international organizations*, 1991). The inviolability of diplomatic archives can be traced as far back as Cicero, who stated that the inviolability of ambassadors is conferred "both by divine and human law" (p. 28). Inviolability is important not only for the preservation of records by their creating government, but for "the integrity and sanctity of the informational content of those records" (p. 27). Colket studies the features of inviolability of diplomatic archives, observing that the principle applies whether documents are in transit or at rest, and "physical location or time" do not change the nature of such archives (p. 28). In Colket's view, protection of the informational content of diplomatic archives is of primary importance, while preservation of the documents is secondary (p. 47).

Colket's main finding is that the degree of inviolability of diplomatic archives varies according to the circumstances. She provides case studies for various situations specific to an era of paper records transmitted by telegraph and courier, as well as earlier eras. These include: "unprotected diplomatic correspondence in transit; diplomatic papers in transit protected by seal; diplomatic papers protected by courier," among others (p. 30). Interestingly, the author concludes that diplomatic correspondence in transit via telegraph, cable, and wireless cannot be 'adequately protected' by international law (p. 31). Among other factors, degrees of inviolability may depend on the location of archives: ambassadorial or ministerial buildings are given the highest protection, while "the mission itself" is considered practically sacred (p. 46). However, when a state has decided to violate archives, no distinction is made between records that are sealed, locked, or open.

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**

The first of two parts of this report by the International Law Commission (the Commission) focuses on the archives of international organizations and their inviolability. The second part in the same report, which is not addressed in this annotation, examines publications and communications facilities. The author of the report, Diaz-Gonzalez, describes the archives of international organizations (IOs) as "a body of documentation" that includes correspondence and files created in the functioning of the organization, and identifies various international legal instruments that employ similar wording to describe archives. The report examines relevant articles on the inviolability of archives in the Vienna Convention on Diplomatic Relations (VCDR) and the Vienna Convention on Consular Relations (VCCR), emphasizing the duty of the host state to protect archives. Although the VCDR and the VCCR refer to diplomatic archives on foreign soil, Diaz-Gonzalez asserts that "there is no valid reason for not applying [inviolability] to the archives of international organizations" (p. 96).

In identifying the characteristics of inviolability, Diaz-Gonzales notes that the principle is absolute, since it applies even in war and in the event that diplomatic relations are broken (p. 96). In fact, the ILC argues that inviolability for international organizations should be "even stricter" than the principle applied to states, noting that Jenks supports this view (p. 97). Various legal precedents relating to inviolability and to the disclosure of information are examined, as are rare instances when inviolability is contravened. However, the Commission maintains that the principle is universally accepted (p. 97). 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 (p. 99). The ILC concludes that "international instruments" and customary state practice "fully support the principle of the inviolability of the archives of international organizations" (p. 99).

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

This report by the International Law Commission (the Commission) examines the relationship between States and international organizations (IOs) with regards to their privileges and immunities. While expressing the Commission's desire not to be bogged down by a theoretical discussion, the author, Diaz-Gonzalez, begins by clarifying the meaning of the term 'international organizations.' In the language of the United Nations, 'international organization' refers specifically to intergovernmental, rather than non-governmental, organizations (106). The 1969 Vienna Convention on the Law of Treaties echoes this terminology (p. 106). However, in the commentary to the draft article of the Vienna Convention, the Commission stated that while international organizations are "composed mainly of States," "in some cases [they have]...members which are not yet States or which may even be other international organizations" (p. 106). The report adopts the terminology of the UN in using 'international organization' to mean intergovernmental organization.

The report discusses the legal capacity of international organizations. Although the first subjects of international law were States, international organizations are also now recognized under international law. 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" (p. 107). For this to be possible, States must "relinquish certain prerogatives of sovereignty" so that IOs can act independently. A statement issued by the Swiss Federal Council to the Federal Assembly of the Confederation highlights States' "corresponding obligation embodied in international law" to allow IOs to fulfill their functions on host territories (p. 108).

The respective issues of legal capacity and privileges and immunities are addressed in Articles 104 and 105 of the UN Charter. Likewise, the constitutions of most intergovernmental organizations carry similar provisions (p. 108). In some cases, unilateral decrees may recognize the legal personality of international organizations, such as the *International Organizations Immunities Act* of the United States. The latter grants international organizations the right to 'contract; acquire and dispose of real and personal property; and to institute legal proceedings' (p. 109). The 1946 UN Convention on Privileges and Immunities outlines the same privileges (p. 109). However, the extent of the legal capacities of international organizations is debated, and State recognition of it also varies (pgs. 109, 110). As well, there are limitations to the rights of IOs, and "their powers are functional" (p. 110). A number of legal cases are examined to provide context for the discussion.

Hupkes, S. D. 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

This report analyzes the legal rights and obligations between international organizations and their host states, and provides a detailed discussion on the inviolability of premises of international organizations. The report is the culmination of a research project, Secure Haven, by Campus Den Haag/Leiden University, Capgemini and TNO Defensie en Veiligheid (see https://openaccess.leidenuniv.nl/handle/1887/14119). The author uses the example of The Hague as a host city to a multitude of international organizations. The introduction to the report provides background information on the Secure Haven project and a discussion of the definitions and classifications of international organizations. Part I examines the development of diplomatic and organizational immunities, noting that there are both differences and similarities between the two situations. The report explains that privileges and immunities of international organizations evolved and draw from those of diplomatic missions. The primary basis for privileges and immunities of international organizations stems from the concept of functional necessity, which "entails that an IO enjoys all privileges and immunities which it needs in order to be able to function effectively" (p. 30). The author provides a "diagram of categories of privileges and immunities" illustrating the immunities of the main subjects of international immunities, states and international organizations (Figure 2, 24). The inviolability of premises and archives stems from the immunities of the organization itself, as opposed to persons within the organization (p. 24).

Part II focuses on legal particularities related to the inviolability of premises of international organizations. The 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, despite the fact that archives are also located on the premises of an organization (p. 48). Therefore the report only considers the inviolability of premises of international organizations, but in great detail. The author examines the physical boundaries, terminology of legal instruments relating to inviolability, duties of the host State regarding inviolable premises, and reasons for inviolability, among other issues. In regards to the host state, the author states that "the premises of an International Organization are still under the jurisdiction of the host state. As such, it is no different from any other part of the territory of the host state. The only significant legal difference is that the host state is not allowed to exercise (or enforce) this jurisdiction" (p.45). The author also considers exceptions to the inviolability principle, such as emergency situations, and alternative models to inviolability, including the concept of "internationalized territory" first conceived of by Wilfred Jenks (p. 62). Part III considers the duty of states to protect international organizations, and the report ends with a summary of conclusions and recommendations.

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

Jenks' aim in *International Immunities* is to review the law of international immunities across various international agreements and international organizations. He explains that the law of international immunities has arisen out of a need to specify the "functional needs" of international organizations (introduction, xxxviii), and he begins by summarizing four key characteristics in the contemporary development of these immunities: the total number of individuals protected by international immunities has greatly increased; the individuals protected are no longer located almost exclusively in Geneva or The Hague but in major cities all over the world; the law of international 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"; and, finally, that "while those immunities which have been thought essential have been placed on a much clearer basis…, the general trend has been to restrict the scope of immunities granted to individuals and to limit strictly, on a basis of function and status, the number of persons who are granted full personal immunity (introduction, xxxv)."

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 (p. 1). After 1945 and the proliferation of international organizations, scholars and lawmakers were required to distinguish between the characteristics of diplomatic immunities and international immunities, such that by the time of the publication of *International Immunities* it was standard for the constitutions of international organizations to contain provisions conferring certain immunities on the organizations themselves, representatives of their member states, and employees of the organization. These constitutions, adds Jenks, "are supplemented by headquarters and host agreements with governments on whose territory international organizations maintain headquarters or other offices (p. 3)."

Jenks explains the rationale for international immunities by summarizing three foundational principles of international immunities outlined in the International Labour Organization (ILO) Memorandum: international organizations should have a special status protecting them from state control or interference; states should not benefit financially from "common international funds"; and the ILO should be provided with the facilities for carrying out its business as would be typically accorded to a member State (p. 17). Jenks specifies that the theory undergirding these principles applies to institutions rather than individuals, so that international organizations may be granted "functional independence" that frees them from "national control" and "enable[s] them to discharge their responsibilities impartially on behalf of all their members" (p. 17).

Chapter Seven 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. For each part, Jenks lists the corresponding article in the UN General and Specialized Agencies Conventions, as well as examples from various agreements between IOs and their host states. Jenks observes that the inviolability of premises of IOs may enjoy greater immunity than "parliamentary buildings and courts of law," according to some state practices (p. 46). In regards to the inviolability of property and assets, Jenks notes that although this article falls under the same provision as the inviolability of premises in the UN General Convention, it is a distinct form of the principle extending to the immunity of premises (p. 53). This is demonstrated by the fact that some IOs are conferred inviolability of property and assets even if they are not accorded inviolability of premises, such as the Bank for International Settlements (p. 53). In his brief discussion of the inviolability of archives, Jenks states that no special issues on the matter have arisen, and that the purpose of protecting archives is to promote "safe-keeping" of documents and "confidentiality" of information therein (p. 54). On a broader level, the inviolability of archives ensures the "freedom and independence" of IOs and their staff to function (p. 54).

Miller, A.J. (2009). The privileges and immunities of the United Nations. *International Organizations Law Review*, *7*(1), 7-115.

The purpose of this article, written by a former Principal Legal Officer in the United Nations Office of Legal Affairs, is to chronicle the practice of the UN relating to its privileges and immunities. The article is intended as a reference for attorneys working in international organizations in the area of privileges and immunities, and for claimants who wish to better understand decisions made by international organizations based on those privileges and immunities. Following the introduction, Section 2 of the article addresses the principle of functionality, which forms the basis for all of the privileges and immunities of the UN. Miller provides a description of the historical development of the concept arising from the League of Nations, and explains the intent of the drafters of the

Charter of the UN and the 1946 Convention on the Privileges and Immunities (the "General Convention"). Section 3 provides a discussion of the legal personality and particular capacities of the UN. In Section 4, Miller focuses on the immunity of property, funds and assets of the organization and the scope of immunities from legal process.
In section 5, Miller turns to the principle of inviolability of the premises of the UN, delineating its scope and how it is used or waived in practice. He also studies how local laws apply to the organization, noting that the UN does not have criminal jurisdiction, and that local laws are applicable unless they interfere with the functions of the organization (p. 50). Notably, the inviolability of the premises of the UN is based not on ownership, but on occupancy—even for short durations—and/or custody of premises and assets (p. 46-47). Section 6 deals with the inviolability of the archives of the UN, outlining the scope of the principle applied to archives, and noting especially the proviso in the General Convention which allows for inviolability of archives "wherever located" (p. 53). The archives include documents held, but not necessarily owned, by the organization, thereby encompassing documents given to the UN by third parties (p. 54). Miller notes that the General Convention does not define archives so as to account for technological changes, including records in both physical and electronic form (p. 54). As inviolability applies to the information contained in records, Miller points to various cases and responses by the UN when information is requested by court order in different legal situations. The rest of this substantial article deals with other UN privileges and immunities in the areas of tax exemptions, communications, funds and currencies, and waivers of immunity.

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

Muller's first task in this study is to define his understanding of international organizations. He characterizes '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). The purpose of the text is, however, not to act as a "comparative study" between a selection of international organizations and their host states. Instead, Muller's purpose "is to define *how* and in *what context* the legal relationship between the two entities is regulated" (p. 14). To this end, the sources of law that can be identified in this relationship and the factors that underlie and influence the legal status of an international organization and its host state are considered.

Muller provides a lengthy overview of host arrangements, explaining that there are a variety of legal instruments that international organizations and their host states use to regulate their relationship. He points out that frequently "the host agreement is but the basic document, which, implicitly or explicitly, in turn refers to or relies on, other sources of law" (p. 26). Muller identifies many other legal instruments that exist in addition to host agreements: constituent treaties, multilateral conventions on privileges and immunities, supplemental and additional agreements to the host agreement, rules of customary international law and decisions of international tribunals, and national legislation and decisions of national tribunals (p. 26). While Muller spends a great deal of time examining each of these legal instruments, one of his most insightful points is that the "constituent treaty determines that the organization is entitled to the legal status and privileges and immunities which it needs to function effectively, and the host agreements and multilateral conventions work this out" (p. 30-31).

In his chapter on the legal personality of international organizations, Muller summarizes Benedek's distillation of the three main theories on international legal personality, noting that "[the] second and third theory are the most pragmatic and widely adopted" (p. 74). These are the functional theory, "which states that an international organization derives its legal personality from the tasks it has been set to perform," and the objective approach, which "has engendered certain objective criteria for the possession of legal personality" (p. 74). Muller specifies that for both the functional and objective theories, the need to fulfill "the purposes of the organization as laid down in its constituent instrument" bestow on the organization a special status and establish the scope of its legal capacities" (p. 75). Muller argues that the national legal personality of international organizations is implied in the granting of international legal personality, which is "best described as an extension to the national level of the international organization's capacity to act on the international plane" (p. 116).

In his chapter on the immunities of international organizations, Muller identifies functional necessity as the theory underpinning immunities, asserting that international organizations would be "hampered seriously if...the host state could freely institute legal proceedings against them, thus allowing national courts to make pronouncements over the organization's policy decisions" (p. 151). Muller points to the "inherent conflict" between the independence of international organizations from the laws of their host states and "the ever widening scope of their activities," which "demand some form of supervision and means of redress for third parties dealing with the organization" (p. 151). Muller's conclusion is that at its best, the functional necessity theory provides a framework to address questions that arise from this conflict (p. 154).

Comparing the inviolability of premises, assets, and archives with the freedom of communication of international organizations, Muller notes that both sets of privileges are designed "to protect the 'private life' of the organization" (p. 212). From the point of view of the host state, there exists the "duty...to *abstain* from interfering" and the "active duty" of protection (p. 212). On the subject of freedom of communication, Muller questions how technological advances have impacted the relationship between international organizations and host states. Technological advances have "internationalized the flow of information," thereby "decreas[ing] the control national state authorities can exert over it" (p. 212). However, in spite of the challenges of technological advances, "[whether] the information is carried by a trans-Atlantic glass-fibre cable or a diplomatic bag," there should be no tampering by the host state (p. 220).

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).

Andrews, D. C., & Newman, J. M. (2013). Personal jurisdiction and choice of law in the cloud. ***Maryland Law Review*, *73*****(1), 313-384.**

The authors seek to answer the question of whether or not current laws apply in a cloud computing environment, and if so, which laws apply. The article begins with a set of norms to work towards and an overview of cloud computing technology, followed by an analysis of current laws and suggestions for policy reforms. Andrews and Newman note that cloud computing poses several legal problems, and that the law has yet to fully catch up with advances in technology. Many individuals use cloud computing on a day-to-day basis, yet are unaware that the technologies they are using could be considered cloud computing.

The authors note that "from a legal perspective, the cloud embodies a new template for interactions" (p. 327), and assert that all interactions in the cloud are contract-based. Myriad legal issues have arisen from the use of the cloud, with several examples provided from American case law. The differences between 'choice of law' and 'jurisdiction' are examined. The discussion on choice of law examines the First, Second, and Third Restatements of Conflict of Laws.

The authors observe that the dynamic nature of cloud computing renders it relatively "uncharted territory" (p. 348), and globalization fosters cross-border transfers. Any legislation for cross-border transfer and cloud computing must be predictable, open, transparent, and objective. Three solutions for personal jurisdiction in the cloud are proposed, including caveat maleficus, the cloud as its own jurisdiction, and a new legislative and regulatory scheme. The authors present lessons learned from jurisprudence on the Internet, and note that in addressing current issues, there may not be a single overarching solution.

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**

This report contributes to a discussion initiated by the United Nations Secretary-General's Special Representative on human rights and transnational corporations and other businesses. The objective of this report is to determine the circumstances in which states can extend their extraterritoriality to handle issues on human rights abuses conducted by businesses. The report states that extraterritoriality "is a situation in which state powers (legislative, executive, or juridical) govern relations of law situated outside the territory of the state in question" (p. 1). The report highlights three principles governing extraterritoriality rules in public international law: sovereignty, non-intervention and cooperation (p. 2).

Some activities may take place outside the territorial boundaries of a state, but it may result in extraterritorial effects. For example, French criminal law tends to extend extraterritorial jurisdiction to a victim that has French nationality (p. 4). The author concludes by stating that countries tend to develop laws which have an extraterritorial scope and effect and this can be illustrated in criminal law, civil, tax, banking and environmental law (p. 15).

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

This paper focuses on international policies towards the implementation of public-model cloud computing in financial and governmental contexts. The paper begins by establishing what cloud computing is, the various models, and the types of cloud services. The paper discusses leading cloud computing providers and their various interests in cloud computing, be it hardware or IT support. It also presents projections for the market value of cloud computing in 2015 (the paper was written in 2012). Most notable in this section is the mention of the United States Federal Cloud Computing Strategy, which estimates that one-fourth of federal IT spending could be moved to the cloud. Discussion turns to U.S. cross-border exports of public cloud services in terms of revenue generated from those ventures.

Three policy issues are highlighted: data privacy, security, and localization requirements (restrictions on where data are housed). Data privacy is examined through EU (including the EU Data Privacy Directive 1995) and U.S. regulations. Other countries have not adopted comprehensive, mandatory regulations. A section on “International organizations’ efforts to address data privacy” outlines the development of a shared set of principles for data privacy by the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation’s (APEC). The Madrid Resolution, adopted by about 50 countries (not including the United States) in 2009 at the International Conference of Data Protection and Privacy Commissioners, is touched upon.

The paper discusses the inclusion of security frameworks, the U.S. Patriot Act, and groups interested in clarification of existing legislation. Cloud service providers are concerned over “location independence,” while financial and government industries have an interest in maintaining localized cloud computing. The authors examine cloud computing in international trade agreements, both multilaterally (at the World Trade

Organization) and bilaterally (through free trade agreements). Finally, there is a section on developing countries in cloud computing, with a focus on China and India.

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

This article is divided into three parts. The first part examines jurisprudence in Australia, Canada, and the United States concerning extraterritoriality, while the second part examines the concept of extranationality as it applies to indigenous groups within a nation's borders. The third part compares the two concepts. For the purposes of our study, the first section and parts of the third section are useful.

Clopton examines several different pieces of case law in the three countries, including America's Charming Betsy case, and discusses the commonly-held 'presumption against extraterritoriality.' This presumption assumes that statutes that are ambiguous in their scope do not apply extraterritorially. This is based on the notion that, in the U.S., Congress generally only addresses domestic issues and strives to avoid international conflict. A litigant wishing to bring an extraterritorial suit must prove the extraterritorial nature of the case and that the focus of the applicable statute is an extraterritorial act. Similar provisions apply in Canada and Australia.

Clopton provides a detailed comparative examination of legislation in the three nations. Following a discussion on the applicability of legislation extranationally, Clopton compares extraterritorial and extranational jurisprudence, and provides recommendations for legislators in a 'roadmap' for both extraterritoriality and extranationality. He highlights the work of Professor Rosenkranz in the U.S., who has suggested that a federal interpretation act be introduced to make a general presumption either in favour of, or against, the extraterritorial application of laws. In his discussion on American statutes, Clopton examines the Third Restatement of Foreign Relations law, noting that prescriptive jurisdiction may be based on territoriality, nationality, objective territoriality, passive personality, and universal jurisdiction.

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.

The authors provide a detailed examination of extraterritoriality, including legal status, jurisdiction, causation, division of responsibility, and remedies and accountability. The book begins with a detailed discussion of terminology regarding extraterritoriality and transborder obligations, and continues with a focus on extraterritoriality in the Canadian context.

The authors provide a detailed discussion of extraterritorial obligations and how to determine when a State has the obligation to intervene extraterritorially. They note that globalization has led to a renewed consideration of extraterritorial rights, although there is a distinction between when a nation can exert extraterritorial rights, and when it should exert such rights. The authors note that there are cases when it is unclear where jurisdiction lies, or where multiple jurisdictions may apply. The article provides a discussion on how to determine jurisdiction and provides an overview of prescriptive, judicial, and enforcement jurisdiction.

The authors note that "the Internet requires a revisiting of the principle of territoriality, as many transactions or interactions over the internet are 'both here and there'" (p. 40). After providing the example of WIPO and intellectual property, the authors assert that many transborder issues are likely to be addressed through international cooperation.

The authors provide a framework for deciding when to act extraterritorially and note that enforceability of legislation is crucial, as unenforceable laws may only serve to antagonize other nations. The authors note that legislators must ask if extraterritoriality should be used, and they provide a template to guide users. The article provides a list of key policy objectives for Canada and concludes by stating that, "the edifice of territoriality is being slowly dismantled by globalization" (p. 78).

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.

The purpose of this article is to examine how the principles of territoriality continue to be applicable to the Internet. The authors propose developing policy principles to guide issues relating to international law norms on the Internet. The legal literature on the Internet is primarily divided by specific domain areas, such as cyber-crime and commercial transactions, and there is a need for a cross-domain approach to how states govern their jurisdiction on the Internet.

Jurisdiction is defined as the "ability of the state to exercise some form of power, coercive or otherwise, over persons, places, things (including property) and events" (p. 1017). It is essentially a public law concept. In contrast, criminal law is the area where international law of jurisdiction initially emerged. In the area of criminal jurisdiction, a crime may take place in more than one state but it has effects in another state. Such an effect is known as qualified territoriality. There are four major principles governing extraterritorial action. Firstly, the nationality principle outlines that states can exercise jurisdiction over its nationals, regardless of where the action takes place. Secondly, the protective principle outlines that states can exercise jurisdiction on actions committed abroad but has implications on its security and independence. Thirdly, the universal principle outlines that states can exercise jurisdiction over criminal offences that contravene international conventions or norms. Finally, the passive personality principle outlines that states can exercise jurisdiction over acts that injured their own nationals, even if those acts take place outside the territory of the state.

The authors make a distinction between an exercise of extraterritorial jurisdiction and an action that results from extraterritorial effects. For example, the European Union (EU) Data Protection Directive (1995) states that data can only be processed in a third country only if there are measures for adequate protection. Although the Directive by itself is not extraterritorial in nature, it has extraterritorial effects as countries enact data protection legislation in order to continue trading with EU member countries. The authors propose that the international community should evolve towards global governance through the formation of supranational institutions. Such a collective form of governance should not be driven by nation states but involves greater engagement between both the public and private sector.

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

This document provides an overview of the laws and principles involved with extraterritoriality. These include civil law, criminal law, anti-trust (competition) law, securities law, territorial principle, nationality principle, protective principle, and the universality principle.

The report takes case studies from the EU and the U.S. to illustrate the extraterritorial nature of legislation. The section entitled “The Protection of Intellectual Property on the Internet” focuses on U.S. legislation such as PIPA, SOPA, and the OPEN Act. A description of the EU Emissions Trading Scheme offers a great discussion on the extraterritoriality of an international organization’s legislation.

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

The author traces the concept of territorial spatiality based on cartography and on the concept of extraterritorial jurisdiction. The term jurisdiction first used in the 14th century meant, "extent or range of administrative power," while the term ‘territory’ which was used in the 15th century meant "land under the jurisdiction of a town, state etc." (p. 205). According to the Oxford English Dictionary, the term territory "means to frighten, to terrorise, to exclude" and in modern terminology, territory means "land organized and bounded by technical juridical and military means." In other words, the concept of jurisdiction need not be tied to the boundaries of a territory. The author's analysis may have implications for UN agencies which are not tied to a particular territory.

The author cites Robert Ford's premise about the scope of territorial jurisdiction based on modern cartography. According to Ford, jurisdictions are an abstract concept and "actual social relations and the distribution of resources are invisible from the perspective of the abstract map" (p. 206). In other words, nation states need to construct the concept of community for the purposes of governing a jurisdiction. Authors such as John Perry Barlow, David Johnson and David Post argue that cyberspace is not a physical space and as such, concepts of geographical borders and territorial jurisdiction are not applicable, since the "effects of any particular behaviour" "restricted by physical proximity does not hold" (p. 202). Other authors such as Julie Cohen reject the distinction between physical and cyber space, while noting that there is a "rich variety of entanglements between virtual and physical spaces that are real to the extent that they generate real consequences" (p. 203). The author cites Grotius's premise that the high seas lie outside the space of territoriality sovereignty and thus, the right of innocent passage is free and open to all people and countries to use. The author proposes investigating how cyberspace can be the equivalent of Grotius' premise of the high seas and how the concept of spatiality in cyberspace can be conceived as a form of "spatiality different from that of the territorial state" (p. 213).

The author concludes by raising the question on whether cyberspace as a passage and a global commons can be reconciled with the concept of territorial jurisdiction. She notes that the main challenges would be to introduce universal concepts of safety, freedom and respect for human rights in cyberspace based on a legal framework that cannot be "grounded in the monopolistic spatiality of territorial sovereignty" (p. 224).

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 discusses the recent Google Spain case and notes that the decision has left several unanswered questions. The author analyzes the implications of the ruling for data privacy law.

Kuner notes that there was some disagreement as to whether search engines are data controllers or processors. The article highlights three significant legal issues raised by the judgement: the material scope of the law, the territorial and extraterritorial scope of the law, and the threshold for invoking the law. The author remarks that "the judgement …does not address the extent to which the right applies outside the EU" (p. 14). This has led to the assumption that almost any data subject worldwide could request the suppression of their data, regardless of whether or not they are EU citizens. Kuner argues against this unintended consequence and states that there should be reasonable limits placed on its territorial scope, as well as a decision made on when the law does not apply, while maintaining a fair balance in the spirit of the law.

The article addresses several higher-level issues, including those of a jurisprudential nature. In critiquing the style of judgement, Kuner notes that the ruling has clear extraterritorial implications, but that the CJEU declined to comment on its global impact. The Article 29 Working Party has indicated that the Directive may "persuade non-EU data controllers to comply with EU data protection law, even when it may not be possible to enforce the law against them" (p. 26). Kuner concludes in stating that the judgement has demonstrated the Directive's application to the Internet, yet notes that if the territorial scope is not further refined, it will become unenforceable.

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's article, published in two separate parts, examines issues of jurisdiction and territoriality. In the first part, Kuner demonstrates how extraterritoriality can cause significant problems for businesses, as in many cases they do not know to which laws they must adhere. Kuner examines instances where both the European Union and the United States have complained about the extraterritorial scope of the other's data laws, and notes that expansive interpretations of legal instruments lead to increased jurisdictional scope. Kuner defines 'jurisdiction' as "the State's right under international law to regulate conduct in matters not exclusively of domestic concern" (p. 178-179). He notes that the distinction between the terms "jurisdiction" and "choice of law" is becoming increasingly vague, and analyses Article 4 of the European Data Protection Law to further his assertion.

Kuner provides a discussion on jurisdictional rules as they apply in international law, which he divides into three categories: legislative or prescriptive jurisdiction, adjudicative jurisdiction, and enforcement jurisdiction. He examines the Lotus case, and notes that there are four widely accepted jurisdictional bases: territoriality, personality, the effects doctrine, and the protective principle. He discusses the accountability approach employed by the APEC Framework and further analyses Article 4. Kuner discusses selected regional approaches from the European Union, North America, and Australia.

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 addresses the concept of 'exorbitant jurisdiction,' a term which he has chosen to use in place of 'extraterritoriality'. He notes that the term 'extraterritorial jurisdiction' appears to have different meanings in different legal systems. Kuner addresses different conventions and protocols, which recognize 'exorbitant jurisdiction,' and provides a lengthy discussion on jurisdictions over foreign entities. He discusses foreign websites, and notes that EU law often discusses 'equipment,' which overlooks other technologies such as cookie use. Kuner points to the SWIFT case as an example of EU extraterritorial jurisdiction. While some have asserted that concerns over online data protection have been exaggerated, Kuner provides a more detailed analysis of the subject.

Kuner notes that it is perhaps impossible to attain perfect compliance with the law, but that so-called 'soft' penalties such as damage to an organization's reputation may serve to increase observance of the law. The author addresses the fact that data protection may fall under multiple jurisdictions and that "several States [may] assert such grounds" (p. 237). Due to this, it is necessary to implement a solution that will allow multiple jurisdictions to co-exist. Kuner addresses various links in data protection cases, including the data controller's place of establishment, the place where data is processed, the place where the wrongful act occurs, the residence of the data subject, use of cookies or similar technologies, continued application of data protection law, and extraterritorial enforcement. He provides a discussion on the evaluation of jurisdictional grounds, and provides a list of steps to reduce jurisdictional disputes. Kuner concludes by noting that the field itself is still largely in its infancy and that it is unsurprising that there are jurisdictional uncertainties.

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.**

The authors remark that the extraterritorial scope of data privacy laws deserve increased scholarly attention. They briefly discuss existing legal instruments that demonstrate extraterritoriality, including legislation originating from Singapore, Malaysia, Australia and the European Union, and why these laws are of growing importance. Reasons include: the globalization of human interaction, an increasing emphasis on data as many companies find themselves built on it, the increasing governmental interest in data access and/or processing, the increase in voluntary data sharing among users of social networking sites, the increased commodification of personal data (often seen in "free" social media services), an increased use of cloud computing involving data storage in an unclear geographic location, and a growing emphasis on privacy as a human right (p. 147).

Kuner et al note that most online businesses deal with some degree of personal data. As data can be stored 'in the cloud,' businesses risk exposure to the data privacy laws of countries other than their own. Kuner et al assert that "extraterritorial jurisdictional claims are reasonable," as data protection laws must be extended to foreign parties in order to "provide effective protection for their citizens" (p. 147). However, another view acknowledges such extraterritorial claims as unreasonable, since businesses and individuals cannot be expected to modify their online behaviour simply to comply with all data privacy laws in all jurisdictions. The authors conclude that nations must strive to cultivate international understanding regarding online behaviour, since, in an extreme scenario, misunderstandings may eventually lead to conflicts between nations.

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.

This article explores the basis of extraterritoriality when it comes to the European Court of Human Rights and the European Convention on Human Rights (ECHR). Section 2 outlines the European Court's inconsistent reasoning behind having extraterritorial powers. There are four exceptional categories of extraterritorial jurisdiction: effective control, extraterritorial effects, extradition, and diplomatic and consular actions (p. 1225). The major theme of the article is the concept of jurisdiction being territorial. However, the author highlights several cases in which functional sovereignty, when states exercise functions in another state's territory that are normally associated with the acts of a sovereign state on its own territory, takes precedence. Miller discusses the idea that 'control entails responsibility' and describes cases in which states have 'effective control' over another territory.

The article only partially explains the extraterritorial nature of the European Court of Human Rights in terms of its rulings in certain cases. It does not explain the extraterritorial power of the Court itself, only its rulings and its member states. The article provides many examples of European Court of Human Rights cases that have an extraterritorial nature, and it details the categories of extraterritorial jurisdiction.

Narayanan, V. (2012). Harnessing the cloud: International law implications of cloud-computing. ***Chicago Journal of International Law, 12*****(2), 783-809.**

In this article, the author argues that as the demand for cloud technologies grows, cloud computing will increasingly fall under governmental regulations in an effort to ensure that citizens' data are protected. Narayanan attempts to analyze, and provide a resolution for, the legal implications of cloud computing. The author identifies two possible equilibrium states of cloud computing: firstly, that nations employ data-protection laws extraterritorially; and secondly, that nationals work towards international cooperation and a global solution.

The article provides a background on cloud technologies before discussing international legal jurisdiction. Narayanan notes that "individual protection regimes must establish extraterritorial jurisdiction under international law" in order to guarantee a degree of stability (p. 789). The author provides three preliminary assumptions for jurisdictional analysis, including the assumption that extraterritorial jurisdiction is permitted unless explicitly prohibited, which has a basis in the Lotus case. The author also discusses the effect of the Third Restatement on Foreign Relations Law, and analyses the territorial and objective territorial principles. The article goes on to examine the passive and protective principles before moving to a discussion on international cooperation and harmonization. Finally, the author concludes with an analysis of 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.

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*** **[panel], pp. 1-19.**

The authors provide a historical background to "jurisdictional alternatives to territory" (p. 2) with a focus on community-based systems, and attempt to draw parallels between the situation online and historical examples. The article seeks to map the rise of nation-states throughout the early modern period and to explore how "community-based alternatives to territoriality have returned… in the Internet era" (p. 3).

The authors quote Paul Schiff Berman, who notes that due to migration, many individuals no longer belong solely to one territorial entity, but rather to multiple communities. Ryngaert and Zoetekouw assert that globalization has minimized the need to emphasise territoriality as our main organizational principle. As the authors note, an entirely territorial model would have difficulty addressing crimes that occur solely online. In instances such as these, a community-based model would be more appropriate. As the authors note, “in a more extreme version of a community-based jurisdictional order, the State disappears and corporations and communities regulate themselves, and constitute their own jurisdictional order” (p. 9). Others have suggested a move towards a community of corporations or organizations rather than the current model of territoriality, and the authors note that this can already be seen in the workings of sites such as eBay and EVE-online gaming.

The authors turn to the challenges that virtual communities pose to territoriality, and discusses the myriad of problems that have arisen between both Google and the European Union, and private taxi company Uber and German and Dutch privacy laws. Furthermore, there has been discussion of “Seasteading,” or creating autonomous communities in the ocean in order to experiment with diverse legal and political systems. In their conclusion, the authors note that online communities and the Internet present unique issues that may “necessitate a paradigmatic shift in how we conceptualize spatiality…and the exercise of jurisdiction” (p. 18).

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

This article focuses on the European Union’s (EU’s) regulations in terms of their extraterritorial or territorial extension nature. The article defines extraterritoriality as “the application of a measure triggered by something other than a territorial connection with the regulating state.” Territorial extension is defined as “the application of a measure...triggered by a territorial connection but in applying the measure the regulator is required, as a matter of law, to take into account conduct or circumstances abroad” (p. 90).

Scott notes that outside the field of competition (also known as anti-trust) law, there has been virtually no analysis of the territorial reach of EU law (p. 93). The EU only exceptionally engages in extraterritoriality, except where it is nationality-based (p. 94). The article explores extraterritoriality, effects-based jurisdiction, and territorial extension. Scott focuses on five policy domains (climate change, environment, maritime transport, air transport, and financial services regulation) to illustrate the EU’s use of territorial extension. There is discussion on how different spheres of regulatory intervention (transaction, firm, country, globe) interact with EU law (pp. 106-7).

Scott points out that “while the EU sometimes does exercise extraterritorial jurisdiction, it does so - with very few exceptions - only when a clear, internationally recognized, alternative to territory provides the jurisdictional basis” (p.115). Therefore, international standards are secondary in the EU’s regulations to national territorial jurisdiction. This article does not explain the extraterritoriality of the EU per se, but rather the extraterritorial nature of their regulations.

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

The objective of this study is to highlight information-sharing between the EU and the United States relating to counter-terrorism cooperation and conflict. Extraterritoriality is defined as the "direct authority over entities in foreign jurisdictions" (p. 773). In the past, extraterritoriality was used to apply domestic laws over nationals in foreign jurisdictions, while now extraterritoriality is exercised as a means to "assert regulatory control over the behaviours of entities in foreign jurisdictions" (p. 773). For example, the United States has made extraterritorial claims on various issues including intellectual property, money laundering, and securities exchange. Foreign countries subjected to extraterritorial claims typically react to extraterritoriality measures positively, negatively or have no reaction.

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

This article analyzes the application and legal basis of extraterritoriality in the EU Data Protection Directive and proposed revised Regulation, and discusses the legal status of extraterritoriality in data privacy law in general. The author notes that data privacy legislation is being created worldwide, much of it influenced by the DPD and spurred by technological advances. Yet a ‘conundrum’ of extraterritoriality in data privacy law rests in the fact that 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. Svantesson includes a brief discussion of jurisdiction and extraterritoriality, outlining four types of jurisdiction exercised by states, and identifying issues relating to extraterritoriality. He describes six grounds for jurisdictional claims, noting that of the six, the principles of objective territoriality, passive personality, and the effects doctrine are the most controversial. As well, the effects doctrine overlaps with the former two principles. In later sections, Svantesson studies the jurisdictional grounds for EU data protection laws and notes that extraterritorial claims exist in several data privacy laws worldwide. He also lists a number of legal cases in which judgements regarding extraterritorial claims have been adjudicated.

Svantesson, D. J. B. (2015). A jurisprudential justification for extraterritoriality in (private) international law. *Santa Clara Journal of International Law, 13*(2), 517-571. http://digitalcommons.law.scu.edu/scujil/

In this article, Svantesson considers extraterritoriality in a private law context, focusing on internet-related cases in private international law disputes in which State extraterritoriality becomes a factor. He observes that the challenges of enforcing extraterritoriality is cited as a "heavy and influential argument against" it (p. 2). However, much of the article attempts to address "the absolutely fundamental question of whether practical enforceability of jurisdictional rules is a necessity" (p. 3). In section 2, the author offers a discussion of the concept of extraterritoriality. Notably, he makes a distinction between "the exercise of jurisdiction being extraterritorial as such" (relating to activities taking place outside a state's borders), and "the exercise of jurisdiction…[having] extraterritorial effect or implications" (relating to activities not necessarily taking place outside a state's borders, but involving international elements) (p. 5). Svantesson highlights the perspectives of prominent legal theorists, including Fuller, Kelsen, Hart, Goldsmith, and Posner, whose ideas are relevant to a discussion of extraterritoriality.

In his analysis, the author identifies specific issues including: the 'dual role of law' as both enforcer and "as a means of social control," or "as a tool to control, to guide, and to plan life out of court," which "does not necessarily depend on enforcement" (p. 28); the 'reputational dimension of extraterritoriality,' which refers to the negative perception others may have of law breakers, but to which the author adds that this perception can be positive or negative depending on the 'moral justifiability' of the law (p. 29); 'domestic enforceability of extraterritorial claims' through 'market destroying measures,' that is, through indirect measures such as sanctions; and 'bite jurisdiction versus bark jurisdiction,' the former referring to enforceable jurisdiction, and the latter to law that acts more as a deterrent to certain types of behaviour or activities. The author concludes that the 'legitimacy' and 'practical utility' of extraterritorial claims are not contingent on enforceability and furthermore, on a domestic level, the enforcement of extraterritoriality can be supported by sanctions (p. 3). He also proposes eight principles for determining whether an extraterritorial claim has legal validity, which he describes as "essentially…a theory of morality about the circumstances in which something ought or ought not to happen" (p. 40).

Swanson, S. (2011). Google sets sail: Ocean-based server farms and international law. *Connecticut Law Review, 43*(3), 709-750.

The objective of this article is to examine the legal implications of the provision of server farms by service providers. For example, Google has filed for a patent in the United States to develop a data centre in the ocean. The author attempts to examine whether the UN Convention on the Law of the Sea (UNCLOS) adequately addresses unanticipated issues relating to the rapid advance of technology, such as the jurisdiction of server farms over the high seas.

Swanson highlights the general principles of jurisdiction under international law. The first is the territorial principle, which is "prescriptive jurisdiction over persons, locations or activities within its territory" (p.721). Nation states have used the territorial principle to exercise jurisdiction on issues that may take place outside the state but which has effects within the state. The second principle is one of nationality; nation states can pass laws on its nationals that are on board a foreign ship or carrier. The third is the protective principle, which enables states to exercise jurisdiction over foreign nationals whose acts affect the security of the nation state, such as laws relating to environmental regulation and anti-terrorism (p. 723). Finally, the principle of universal and passive personality involves state attempts to exercise control over foreign nationals who engage in activities that are not endorsed by the international community, such as piracy and war crimes and taking hostage of its citizens. Swanson states that it is in the interest of data center owners to seek flag state protection for their servers in the high seas, since possessing a nationality protects the ship from other state jurisdictions. Moreover, there is currently no existing law based on UNCLOS or the Convention on Conditions for Registration of Ships, which prevent a data centre ship from obtaining a flag state status.

Swanson highlights the case of pirate radio broadcasting located in high seas during the 1960s. The European Economic Community members brought this issue to the attention of UNCLOS, who in turned passed an article prohibiting "unauthorised broadcasting from the high seas" (p.740). In addition, there are international agreements signed by various nation states which criminalise the activity of pirate broadcasting and communication. Swanson suggests that the pirate ship example illustrates the possibility of an international body addressing the issue of data centre ships (p. 741).

Van Alsenoy, B., & Koekkoek, M. (2015). Internet and jurisdiction after Google Spain: The extraterritorial reach of the 'right to be delisted'. *International Data Privacy Law, 5*(2), 105-120.

Van Alsenoy and Marieke Koekkoek explore the ramifications of the Court of Justice of the European Union (CJEU)'s ruling on the right to be delisted from internet searches. The article focuses on Article 4(1) of the Data Protection Directive (Directive 95/46/EC) of the CJEU. Issues that arise in Article 4(1) are the location of the 'controller,' the location of the 'equipment' being used, and the 'context of activities' performed.

The majority of the article deals with the specific case of Google Spain, which is a subsidiary of Google Inc., based in the United States. The basis of jurisdictional claims in international law usually follow the territoriality principle (p. 4). The authors discuss how to legally deal with multiple versions of the same service (i.e. Google Spain, Google Canada, etc.). Although the article is specific to transnational search engines, it does provide some information on the extraterritorial issues at play. It highlights an instance of a ruling by an international organization that affects those outside its membership. This article could also be cross-listed under "Data Protection and Privacy Legislation."

Zerk, J. A. (2010). Extraterritorial jurisdiction: Lessons for the business and human rights sphere from six regulatory areas (Working Paper No. 59). Cambridge, MA: *Harvard Corporate Social Responsibility Initiative.* http://www.hks.harvard.edu/m-rcbg/CSRI/publications/workingpaper_59_zerk.pdf

The objective of this study is to examine exteritorial issues in the areas of anti-corruption, securities, anti-trust, criminal law, civil cases, and the environment. Globalizations in the areas of information communication technologies, international trade, and travel have resulted in overlapping jurisdictional claims. States generally adopt two strategies to handle issues which have extraterritorial effects. First, they impose control over their domestic companies, persons, or acts. Second, they exercise extraterritorial jurisdiction in areas such as terrorism, money laundering, and human rights breaches.

Extraterritorial jurisdiction is defined as the "ability of a state, via various legal, regulatory and judicial institutions, to exercise its authority over actors and activities outside its own territory" (p. 13). There are different types of extraterritorial jurisdiction. Prescriptive jurisdiction "concerns the ability of states to prescribe laws for actors and conduct abroad" (p. 13). Enforcement jurisdiction "concerns the ability of states to ensure that their laws are compiled with" (p. 13). Adjudicative jurisdiction "concerns the ability of courts to adjudicate and resolve private disputes with a foreign element" (p. 13). A distinction needs to be made between domestic laws that have extraterritorial effects and laws that have "direct extraterritorial jurisdiction over actors and activities abroad" (p. 16).

International law is governed by a number of areas of jurisdiction. The concept of territoriality operates under the principle of subjective and objective territoriality. Subjective territoriality provides the state with the right of jurisdiction over a conduct that happens in the state but that is completed in another state. Conversely, objective territoriality allows a state to take control over a conduct that started in another state but is completed within their own territory (p. 19). The principle of subjective territoriality is also known as the effects doctrine (p. 19). A second aspect of international law is the nationality principle, which enables states to "exercise jurisdiction over their own nationals wherever they are in the world" (p. 19). A third type of jurisdictional law is the protective principle, which allows that "states may exercise some jurisdiction in relation to an actor or conduct abroad that threatens their vital (usually security) interests" (p. 28). An example of the protective principle is the passive personality principle, where a state can exercise jurisdiction over other nationals and states when its own citizens have been injured outside their country. Finally, the principle of universality allows states to exercise jurisdiction in international crimes such as war crimes, crimes against humanity and genocide (p. 20).

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 medium-sized enterprises "likely ignore the restrictions on cross-border data transfers either altogether or to a large extent" (Parker, 2012, p. 7).

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.

This article by Kamlesh Bajaj, the CEO of the Data Security Council of India (DSCI), describes a case study of an industry association taking on a self-regulating role to promote data security and privacy standards among its member IT service providers. The author believes that this model can help to ensure greater protection of personal information for transborder data flows. The article focuses on data security and privacy in the private sector, but presents an interesting case study from the point of view of the security industry and internet service providers.

The article begins with a review of the global regulatory environment for data protection, noting differences between the European Union and United States environments. Bajaj observes a pattern of privacy regulation development from self-regulation—in the "absence of a regulatory framework"—resulting in codes of practice, to privacy standards, and eventually to the development of privacy laws, as in the case of Canada and Australia (p. 132). Bajaj describes five kinds of privacy codes: the "organizational code, the sectorial code, the functional code, the technological code, and the professional code" (p.133).

In relation to transborder data flows, the author asserts that contracts have been used as an effective mechanism promoting data protection, on a case-by-case basis, where privacy legislation is absent (p. 134). He describes contracts as "the most versatile instrument in transborder data flows," used by countries in the EU such as France (134). Bajaj states that "if organizations, either voluntarily or due to public pressure, want to mandate high data protection for their contractors, they can insist on incorporating standard data protection clauses into their business agreements" (p. 134). The EU Data Protection Directive 95/46 enables public bodies to certify "private self-governance instruments" that regulate data protection and privacy (p. 134). Bajaj proposes that industry associations can play a leading role as self-regulating organizations. In India, the National Association of Software and Services Companies (NASSCOM) has taken on such a role by establishing the Data Security Council of India (DSCI). The DSCI has developed a privacy framework, composed of nine privacy best practices that emphasize risk identification and mitigation and "information visibility" in transborder data flows (p. 137). As well, the DSCI has created a security framework constituting 16 best practices. Bajaj acknowledges that the success of the DSCI "depends on the voluntary acceptance of codes of practice and standards" (p. 138) by industry members, which requires training and awareness initiatives by the DSCI.

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

This article focuses on trans-Atlantic disputes over the regulation of electronic data, particularly between the United States and the European Union, through the analysis of three case studies. The case studies date from the mid-1990s and include the Safe Harbor agreement, the dispute over passenger name records (PNR), and the SWIFT case relating to financial transaction data. The author, Andreas Busch, offers an analysis based on a social science method known as 'framing,' which he maintains complements the constructivist approach that dominates the political science literature on trans-Atlantic personal data regulations (p. 314, p. 324). The author observes that since the terrorist attacks of 9/11, a change in focus from economic to security interests has occurred in the area of personal data, and further regulatory differences have resulted between the U.S. and EU (p. 314).

Busch begins with an overview of the development of the Internet, which was originally conceived as a "truly global communications network that would be devoid of state influence and regulation" (p. 314). However, the increasing use of the Internet brought with it state regulation. A notable feature of the Internet is therefore "the tension between a communication structure designed and implemented to be global, and the largely territorially-based rules of nation states and international organisations" (p. 316). In the next section, Busch identifies the main differences between U.S. and EU regulation of personal data. In the U.S., regulation of data protection is not integrated and the main feature is self-regulation by industry (p. 317). By contrast, in the EU, regulation exists both on the national and supra-national level through the Data Protection Directive 95/46/EU (p. 318).

In his analysis of the Safe Harbor agreement, Busch notes that the agreement constituted a new approach to data regulation, and that it was neither a turn towards the U.S. approach by the EU, nor a move towards the EU system of "formal legislation and institutionalization" by the U.S. (p. 319). In the case of the use of flight passenger or PNR data by the U.S. in its 'fight against terrorism,' Busch points out that the dispute with the EU resulted in an intra-EU disagreement, which revealed differences in "interests and positions" in data protection within the EU (p. 327). In his analysis of the SWIFT case, Busch emphasizes the disregard of EU regulations and concerns by the U.S. in their secret acquisition of global financial transaction data. Subsequently, the author identifies the changing institutional actors in both the U.S. and the EU, and three 'frames' for concretizing the problem: economic interests, security interests, and civil rights interests. Post 9/11, the dominant frame in data regulation has shifted from economic to security interests (p. 329). In conclusion, Busch holds that a unitary approach to data protection is far from being achieved, but his analysis has helped to show the historical roots that have led to the current 'constellation of actors' (p. 328) and approaches towards data regulation that exist today.

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

Cate et. al describe the OECD Guidelines as an attempt to strike a balance between use and privacy since they were first published in 1980. The authors argues that the Guidelines were uniquely successful and used a comprehensive approach that addressed data collection, quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The article provides a brief overview of data protection since the 1970s, noting that the OECD Guidelines have formed the basis for many data privacy rules worldwide. The article provides a discussion of recent privacy dialogues.

The authors note that data subjects frequently give their consent simply in order to use a service, or because a power imbalance exists between the subject and the data controller. Thus, Cate et. al conclude that a revised system of privacy protection is needed, one that shifts the responsibility away from data subjects towards data controllers and collectors.

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.

The author provides an in-depth analysis of Article 4 of the European Union's Data Protection Directive, and questions whether the Article's extraterritorial scope "makes the Safe Harbor program irrelevant for US companies seeking to comply with the EU data protection rules" (p. 203). Colonia notes that a Safe-Harbor compliant organization may still be found liable under Article 4. The article provides a background of the Safe Harbor program and notes that the 'adequacy' requirement essentially grants the EU Data Protection Directive a degree of extraterritoriality. Some have even suggested that the EU "has encroached upon the sovereignty of…nations" (p. 204) by encouraging non-EU states to implement laws that would bring them into a state of equivalency with the EU.

Colonna discusses distinguishing applicable law in the context of data protection and addresses the definition of "jurisdiction." The author addresses the ways in which the EU claims extraterritoriality, and discusses how the physical place of data processing is less important than the place of establishment. Colonia addresses the issue of "context of activities" through the lens of the Google Spain case. She notes that the proposed changes make a fairly significant change from the Directive with regards to extraterritorial application. Furthermore, the concept of an 'EU data subject' is so broad as to include anyone vacationing in the EU. Colonna discusses the concept of data 'transfer' and notes that perhaps the entire notion should be abandoned. Furthermore, Colonna notes that the potential scope and applicability of Article 4 is so broad as to render it nearly unenforceable.

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.

This article examines issues related to ‘processing’ and ‘transferring’ of data within the framework of the European Data Protection Directive, and the new Regulation proposed in 2012 to replace the Directive. According to the author, Samson Joseph Esayas, the term ‘cross-border’ is preferred to ‘transborder’ since the meaning of the latter is limited to transfer from state to state, while the former refers to transfer across a border regardless of the destination. Therefore, the term ‘cross-border’ encompasses “international spaces such as high seas” or international organizations (p. 664). Esayas analyzes situations that may be considered to constitute transfer of personal data to a third party, stating that the specification of ‘third country’ in the Directive does not allow for situations in which data is transferred to non-state parties or locations. He notes that Chapter V of the proposed new Regulation takes into account transfer of data to international organizations (p. 664). He also notes that the understanding of ‘transfer’ of data in the Directive does not account for cloud computing infrastructures, but is situated in a ‘traditional’ model of transfer from one party to another, and requires location of the data to be known. This raises the question whether “the legal bases to justify the processing and the transfer to a third country would apply to the cloud” (p. 664).

The various cloud-computing situations examined that would constitute cross-border flow of personal data include when servers are located within the European Economic Area (EEA) versus when they are located outside the EEA. Other factors considered include whether the provider is categorized as a ‘controller’ or ‘processor.’ A comparison with the meaning of cross-border flow in the Australian federal Privacy Act of 1988 is briefly considered. The final section of the article examines the legal bases for employing cross-border cloud services under the Directive. The author concludes that the criteria to determine what constitutes cross-border flow in a cloud-computing environment needs to change from an assessment based on location to one based on risk-analysis of unauthorized access, which should also consider not only ‘cloud-processed’ but ‘cloud-generated’ data (p. 668, p. 676). According to Esayas, data encryption or data anonymization would be adequate to mitigate the risk of unauthorized access and should not be deemed as constituting a cross-border transfer to a third party under the Directive (p. 668).

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.

The article provides an overview of non-EU data privacy laws and compares many of them to existing EU standards. Greenleaf notes that 89 countries worldwide have enacted data protection laws, and that in the near future, the majority of such laws will actually be found in non-European countries. The author compares and contrasts differences between the EU Directive, Convention 108, OECD Guidelines, and the APEC framework. He attempts to define ten key components of European standards, and discusses their global influence. Greenleaf also identifies ten key components of global standards.

Greenleaf examines the American approach, and asserts that "the USA's standards are fundamentally lower than Europe's," as much of the legislation is sectorial (p. 70). Greenleaf examines 33 non-European data protection laws and compares them to the European standard. The article provides an examination of the APEC guidelines and looks at international agreements outside of Europe.

Greenleaf examines the EU adequacy mechanism and 'border control', and states that "there could be significantly more adequacy findings outside Europe if the EU was more pro-active and more transparent about its processes" (p. 78). The article discusses the Council of Europe Convention 108 and notes that it contains almost every element that is now accepted as core data protection. Greenleaf discusses the modernization of Convention 108, its complications and risks, and highlights issues with the standards for accession. Greenleaf looks at the advantages and disadvantages of accession for non-European states, and compares these with a discussion on the advantages of non-European nations' accession for European nations.

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

The authors note that personal data issues are increasing, and that there is a rise in calls for data protection laws. Further exacerbating issues with data protection and privacy risk is the convenience offered by transborder data flows. The authors note that there is a need for increased cooperation in order to best protect privacy, and provide a brief overview of the Hague Conference's Conventions and the instruments with which they attempt to comply. The article provides a background on a decade of international data protection, with mentions of the OECD guidelines, the EU Data Protection Initiative, and the EU-US High Level Contact Group. However, despite the efforts outlined in the summary, the authors note that very little progress has been made in identifying a solution for cross-border data flow. The authors discuss the Madrid International Conference of Data Protection and Privacy Commissioners, which hosted a presentation entitled, "We Cannot Help You: Your Data are in International Waters" (p. 10) as well as the fact that, with the increase in conflicting regimes, "some legislators have attempted to delimit the (extra)territorial application" of regimes. (p. 7).

The authors provide an examination of cross-border conflicts and note that the current "protective regime" may have a "chilling effect." (p. 6). The articles examines Article 4 of the EU Data Protection Directive and notes that it is not always clear where the EU Act applies, particularly as technology evolves. The authors note that the issue of transborder data flows is one which would benefit from increased international cooperation and that the Hague Conference could play an active role. Furthermore, they note that it would be useful to contribute to the ongoing debate about whether or not it would be desirable to create additional multilateral instruments.

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.**

The Working Paper discusses possible implications for cloud computing services in the context of the proposed recent EU Data Protection Regulations. The authors suggest recommendations to make the proposed Regulations more applicable to cloud computing while ensuring that data protection and privacy are secured.

The paper provides an overview of the Data Protection Directive, the process of legislative reform, and discusses the impact of the proposed reforms on cloud accountability. The authors discuss specific issues of cloud accountability and the appendix provides further background to the EU Data Protection reform process. The authors note that the article was designed to make recommendations for changes to the proposals specifically aimed at improving cloud accountability. The authors discuss the positions taken by the LIBE Committee of the European Parliament to the Commission Draft and the Council to the Commission Draft regarding different aspects of the proposed changes. They also provide their own in-depth analysis, summary and recommendations.

An EU Directive does not automatically apply to Member States, and local legislation must be passed in order to actively implement it. The Article 29 Working Party was struck to address the issue of the proposed reform on cloud accountability. The proposed regulations would enhance the powers of DPAs and would actually serve to further restrict transborder data transfers. The authors recommend that a better definition of "transfer" be reached, and in the course of a lengthy discussion, address different approaches that could be taken with regards to transborder data transfers.

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.**

In this article, the authors test the definition of ‘personal data’ under the EU Data Protection Directive (DPD)—which only applies to personal data—by examining the extent to which the following security factors may render data ‘personal’ under EU rules: anonymization/pseudonymization, encryption, and sharding. Each factor is studied in detail in the article, which constitutes the first in a series of four articles focusing on various aspects of data protection in cloud computing. In their analysis, the authors point to the nature of cloud computing infrastructure, which increasingly employs ‘layers’ of cloud providers building services on top of other cloud services, such as Dropbox, an SaaS that is layered on top of an Amazon-based IaaS (p. 6). Customers contribute to this layering effect in their tendency to integrate various cloud-based services and applications. In the view of the authors, data that has been securely encrypted or anonymized should not be considered ‘personal data’ under the DPD. However, a principal observation of the article is that whether data is deemed personal or not under the DPD depends on a number of factors and is conditional on context. In particular, the same dataset could be considered personal or not depending on the actors and their ability to access and identify the content of the data. The authors call for a shift in focus from a definitional basis of ‘personal data’ as a trigger for data protection, to a focus on an analysis of the risks of data identification, and potential harm and extent of harm that identification of the data may pose to an individual. An appendix to the article suggests specific revisions to the DPD based on the arguments presented in the article.

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

This paper constitutes the second in a series of four papers examining the practical issues related to the regulation of personal data applied to a cloud computing environment under the EU Data Protection Directive (DPD). In Part 2, the authors focus their lens on the framing by the DPD of cloud service providers as either ‘controllers’ or ‘processors.’ The authors contend that the distinction sets a binary that fails to reflect the complex reality of cloud computing, which is “blurring the distinction between data controllers, processors and data subjects” (p. 9). For example, a single entity may be both a ‘controller’ for one set of operations and a ‘processor’ for a different set of operations. The status of a provider depends on the data it is handling or the part in an operation that it manages within a given instance. ‘Data subjects’ themselves, rather than service providers, are often processors of their own data. Moreover, cloud computing often employs “chains of cloud service providers [and] sub-providers, and possibly other actors such as mere infrastructure providers or communications providers,” such that the precise role and control exercised by each party is unclear (p. 24). As per a report by the Article 29 Working Party, WP169, efforts to fix the status of a provider in the contract terms are inadequate for this reason. The authors assert that Infrastructure-as-a-Service providers in particular, who merely provide virtualized infrastructure for consumers to process their own data, should not be perceived as processors of data (p. 23). However, if the provider stores the data, the status of the provider as controller or processor would depend on the degree of security of the data (ie. whether it has been encrypted), and whether the provider has mirrored the data (which would be considered processing) or has made it available to third-parties. As the authors state: “mere hosting of data, without knowledge as to its 'personal data' nature, should not render the provider a processor, and even more so with encrypted data” (p. 18). However, the privacy risks attendant with using Software-as-a-Service, including social media, are greater and the status of such providers needs to be considered distinctly and further clarified. The authors propose “an end to end accountability approach to data protection responsibilities” which would employ “a continuum or spectrum of parties, only some of whom may be considered to be processing personal data through the data life cycle, with varying degrees of obligations and liabilities under data protection law” (p. 28). Their second proposal is to exclude ‘passive’ service providers who merely host virtualized computing platforms from liability as controllers or processors of data, and instead apply the EU Electronic Commerce Directive (ECD) to these entities.

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).**

Part three of this four-part series produced by the Cloud Legal Project at Queen Mary, University of London focuses on jurisdictional issues of cloud computing under the EU Data Protection Directive (DPD). It addresses the determination of the applicability of DPD for non-EEA (European Economic Area) users and providers “as a result of either using EEA data centres or EEA cloud providers, or saving cookies etc. on the equipment of EEA residents” (p. 5). The provisions related to jurisdiction and applicability of the DPD are found in articles 4 and 17(3). A major issue relating to the application of the DPD to non-EEA entities is the lack of ‘harmonization’ of national laws, since each EU member state implements its own laws under the DPD. For this reason, “the jurisdictional scope of the DPD is in dispute” (p. 6). The report acknowledges that although a revision of the DPD is underway, the current DPD remains in force until the year 2016 at least. Article 4(1)(a) states that if a data controller has an ‘establishment’ in an EEA state, and “processes personal data” then the DPD applies to the controller, regardless of where it is based. Article 4(1)(c) states that a non-EEA data controller is subject to the DPD if it uses ‘equipment’ on the territory of an EEA state (p. 13). The authors examine the meanings of the phrases ‘establishment’; ’in the context of activities’; and ‘equipment.’

In the latter half of the article, the authors analyse specific cloud computing scenarios to determine whether they would trigger DPD regulation, including if a provider “which is a data controller saves cookies or other data, or runs scripts or programs, on the computers, mobile phones or other equipment of its EEA-based users,” or if “a data centre located in an EEA Member State is used” for cloud computing services (p. 16). The authors conclude that the DPD applies to non-EEA entities with headquarters outside the EEA in two general situations: when data processing taking place within the EEA and is considered to be ‘in the context of activities’ of that entity; or if data processing takes place using equipment within the EEA, even if there is no ‘establishment’ within the EEA. Therefore, the “territorial link” is to an establishment or to equipment within the EEA (p. 37). The authors present recommendations for improvement and clarification of the EEA, and provide a summary table in the appendix outlining the various situations discussed, and whether the concepts ‘establishment and context’ or ‘equipment’ would apply, thereby triggering DPD regulation.

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

The final article of this four-part series analyzes provisions restricting the export of data under the EU Data Protection Directive (DPD), and identifies ways that data deployed to cloud computing may be transferred outside the European Economic Area (EEA). The authors principally argue that the notion of ‘location’ has become irrelevant in a cloud computing context, and “what matters most is not where information is stored, but who can read it, i.e. who is able to obtain access to it in intelligible form” (p. 53). Following a discussion of data export restrictions under the DPD, the authors turn to the question of what constitutes a ‘transfer’ of data. They note that cloud computing “by its very nature is based on data transfers from the user to the cloud (and vice versa), and automated data transfers within the cloud” (p. 31). Interestingly, the authors claim to debunk a popular myth that “in cloud computing data moves around the world continuously and almost randomly,” while in reality, “In most cases, data are usually copied or replicated to different data centres, for business continuity/backup purposes, rather than being “moved” by being deleted from one data centre and re-created in another” (p. 32). Furthermore, “the primary copy of a set of related data” is often stored within the same data centre closest to the user, or the data may be stored in fragments in different devices within the same data centre (p. 32). The provider will ‘often’ know where the same user’s data fragments are located, “at the data centre if not equipment level” (p. 32-33). The authors note that the literature on the verifiability of data location by users is growing (p. 33, note 32). Additionally, “the relevant data centre location would be that of the data centre ultimately used by the sub-provider in the lowest layer of the cloud 'stack'" (p. 33).

In their consideration of situations that would constitute data 'transfer,' the authors examine the implications of the Lindqvist case, while noting that the DPD does not define 'transfer.' As well as studying exceptions to data transfer restrictions, the authors offer possible alternatives to the 'adequacy' requirement in article 25(1) that would enable legal transfers of data, such as binding corporate rules, model clauses, regional clouds, the Safe Harbour framework, and other options. In their conclusion, the authors state that the DPD should focus on "restricting unauthorised access, rather than restricting data export" (p. 53). In an appendix, the authors provide a table of scenarios listing whether data export would be permissible under the DPD.

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.

This article presents a series of questions and answers regarding updates and modernizations that may be applied to Convention 108. The updates are to be applied in order to account for the new challenges in the field of data protection, and include the addition of principles of privacy by design and proportionality. The article notes that Convention 108 is "the only legally binding international treaty dealing with privacy and data protection" and that it "provided the legal framework for the EU Data Protection Directive 95/46" (p. 223). The questions presented in the article were posed by the Computer Law and Security Review, the International Association of IT Lawyers, and the Institute for Law and the Web. They address matters such as the object and scope of the Convention, the need for broader or narrower definitions of terms, new principles that are to be included in the Convention, various rights and obligations (including those of data controllers), sanctions and remedies, data protection authorities, and transborder data flows. On this subject, the article notes that "it remains appropriate to require an adequate level of protection as a condition of cross-border transfer" (p. 232). The authors note that, thus far, 'adequacy' has frequently been taken to consider 'equivalency'. Importantly, the article notes that "the current European approaches towards transborder data flows are not working effectively," and that the regulations are "burdensome" (p. 233). Part of the goal in revising the Convention is to increase its attractiveness to non-Member States. The consensus is that a global standard that applies equally to private and public bodies should be established.

Kirby, M. (2011). The history, achievement and future of the 1980 OECD guidelines on privacy. *International Data Privacy Law, 1*(1), 6-14.

The author of this article served as the chairman of the OECD expert group on transborder data flows and protection of privacy in 1979-1980, and the article acts as a retrospective on the history of the OECD guidelines. It outlines the influences of the Guidelines, looks at approaches that were adopted in 1980, and finally examines contemporary issues with the Guidelines. Kirby notes that changes in technology have made it difficult to have purely national solutions to data protection, and that legislation is becoming increasingly extraterritorial.

The OECD Guidelines were founded out of concern for barriers to economic growth, and Kirby notes that the Guideline's achievements fell into four categories. These include the fact that while they built on their predecessors, they added seven key points of added value, and were flexible to implement. Furthermore, Kirby points to the Guidelines' survival over several decades as proof of their efficacy. He notes that in the future, legislators must be realistic, particularly in light of changing technology, and Kirby highlights issues with search engines. He notes that, as in 1980, privacy should be protected, and stresses the importance of basing any revisions to the Guidelines in a thorough understanding of relevant technologies. He notes that there are several new challenges, such as mass surveillance, privacy-enhancing technologies, cross-border cooperation, the fact that end users often do not fully understand the implications of their actions on social media, and the fact that the OECD Guidelines may not be doing enough to fully address values of developing nations.

Koops, B-J. (2014). The trouble with European data protection law. *International Data Privacy Law, 4*(4): 250-261.

This article asserts that one of the greatest challenges in updating the European Data Protection Law has been maintaining its currency in the face of technological change. Koops argues that the law's objectives are founded on several major fallacies, including "the delusion that data protection law can give individuals control over their data….and the assumption that data protection law should be comprehensive" (p. 3).

Koops addresses the issue of informed consent, highlighting the fact that many individuals provide consent simply because they wish to use a particular service, and suggests that "data processing in most online contexts should be based on grounds other than consent" (p. 4). The author highlights the Google Spain case as an instance in which individuals actively asserted their rights.

Koops asserts that too much faith is placed in the actions of data controllers. He notes that data protection laws are increasing in complexity and that their translation into real-world situations is difficult. He argues that current DPIAs risk being relegated to the mere function of checklists. Koops notes that, while the updated Data Protection Law removes some former administrative burdens, it adds new ones.

Koops addresses the general trend to regulate all issues with a single law, noting that there is a significant disconnect between law and reality, and that the Law has done little to curb the development of massive databases. He asserts that the European law applies an overly black-and-white a view to data and has been poorly communicated to relevant stakeholders.

In his conclusion, Koops notes that Europeans are surrounded by data protection law, but that it does little for them. He argues that a different approach is necessary, and that we must simplify legislation and focus on underlying principles. Koops provides suggestions for solutions.

Kuner, C. (2009). Developing an adequate legal framework for international data transfers. In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne & S. Nouwt (Eds.), *Reinventing data protection* (pp. 263-273). Netherlands: Springer.

This article examines the basic framework of the EU Data Privacy Directive in an effort to determine if, after a decade, it does what it was designed to do. Kuner asserts that the framework currently used to determine the adequacy of a third state for cross-border transfers is inadequate, he calls the approach “cumbersome, expensive, slow,” and notes that it “sends the wrong message to third countries” (p. 263). Kuner first approaches the issue mathematically and notes that it would take a minimum of 130 years to approve all possible third states for cross-border transfer. He suggests four key improvements to the adequacy rule, namely the investment of additional human and financial resources into the adequacy framework, better communication of adequacy procedures to third states, the need to establish best practices and different tools such as checklists, and the use of sectorial decisions, which would result in certain territories or organizations receiving an adequacy judgement rather than an entire country.

Kuner suggests accountability as a suitable alternative for the adequacy test. Such a system has several advantages, as suitability would be determined for each individual data transfer. Accountability would ensure that there is always a party in the originating country that is liable for the data, and such an approach would avoid attempts at forcing the rest of the world to fall into line with EU data standards. The accountability principle is already recognized in some data protection laws and is already accepted by many third countries, which means that it is more likely to be accepted on a global scale. Kuner notes that aspects of accountability can be worked into the adequacy system. He concludes by stating that accountability would likely be more efficient than the current adequacy framework, which he notes is inadequate given the rapidly evolving nature of technology and the Internet.

Kuner, C. (2014). The European union and the search for an international data protection framework. [University of Cambridge Faculty of Law Research Paper No. 48/2015] ***Groningen Journal of International Law, 2*****(2), 55-71.**

Kuner re-examines issues discussed in his 2009 work, and turns his focus to recent EU laws which he calls the "most influential body of data protection law worldwide" (p. 1). He asserts that businesses find data protection laws frustrating and complicated, particularly in light of the fact that there is little to no harmonization of legislation across jurisdictions. Furthermore, as a result of the globalization of data processing, individuals are often unsure about their rights.

Kuner asserts that all existing data protection instruments have flaws, and notes that international human rights legislation is not detailed enough to provide guidance for individual cases. He briefly examines calls for an international framework, including the 2005 Montreux Declaration, the 2007 Google call for international standards, and the 2009 Civil Society Declaration. He stresses that the EU has pushed for the international adoption of their standards and notes that, due to its extraterritorial nature, the EU Directive nearly fulfills the need for a global framework, particularly as amendments would bring global service providers under its scope if the provider interacts with an EU resident.

Kuner notes that data privacy legislation can either be legally binding or non-binding, international or regional, and institutional or ad-hoc. He highlights ongoing challenges to the creation of a global framework, which have not changed significantly since 2009. Currently, there is no consensus on whether a framework would be legally binding, whether existing legal instruments could be modified or if entirely new ones would be required, what the scope of such guidelines would be, or which body would oversee the process. If standards are too vague, they will not be consistently enacted, but if they are too specific, they may clash with existing legal systems. He notes that "the possibility of a global, legally-binding data protection instrument being enacted in the foreseeable future remains elusive" (p. 6).

Kuner provides an overview of recent Court of Justice of the European Union (CJEU) cases that reinforce the global application of the Directive, including the *Lindqvist*, *Kadi*, *Digital Rights Ireland*, and *Spain v. AEPD and Mario Costeja Gonzalez* cases, and suggests following the judgement of *Schrems v. Data Protection Commissioner*. Kuner notes tensions between global values and the EU directive, which emphasis EU values at the expense of global ones. The proposed 2012 Regulation omits any provision for the

Commission to account for regional data protection legal instruments when assessing cases.
He concludes by noting the push towards a "data Schengen" zone, which would allow EU companies to store their data within the EU. Kuner asserts that Convention 108 is likely the best treaty-based possibility for a global framework as it offers a high level of protection and is based on existing instruments, although interpretation by different states may lead to a lack of harmonization. The EU should consider the impact of its policy on non-EU states, assist developing third countries in establishing data protection legislation, and establish jurisdictional boundaries and an interface to facilitate harmonization of different regional standards.

Kuner, C. (2013). *Transborder data flow regulation and data privacy law*. Oxford, United Kingdom: Oxford University Press.

In this work, Kuner examines the impact of transborder data flows and the legal questions surrounding them. He provides a brief background and situates the topic in a broader social and historical context. Kuner notes that there is limited empirical research on the growth and volume of transborder data flows, and states that it may be difficult to do such a study due to the difficulty of tracing data. He discusses various legal challenges that have arisen from transborder data flows and provides an overview of existing legislation and guidelines regulating such flow. He highlights several issues with the use of terminology, and indicates that there is very little in the way of standard definitions.

Kuner provides an analysis of similarities and differences that have arisen between different legal instruments and asserts that "the main reason for the enactment of transborder data flow regulation has been to ensure data protection rights and protect privacy" (p. 28). The author continues his detailed discussion on differences between regulatory system by highlighting the major approaches to data; that is data protection as a human right versus geographically or organizationally based approaches. He also looks at private sector initiatives as well as 'protection by design' measures for emerging technologies. He underscores the fact that, overall, approaches to data protection and privacy are fractured and lack harmonization.

Kuner examines the risks and benefits of transborder data flows, as well as underlying policies. He examines the advantages and disadvantages of enacting regulation and discusses the difficulty in asserting data-related laws extraterritorially. He notes that extraterritoriality has "often been cited as an important policy rationale underlying regulation of transborder data flows." (p. 116). Kuner also examines how regulation of transborder data flow may, in some cases, be used as a way of protecting a State's informational sovereignty, and has therefore been used to further economic and political interests.

In an examination of existing regulations, Kuner notes that the terms “applicable law” and “jurisdiction” may become conflated (p. 121) and discusses difficulties with territorial legislation, as it is often difficult to know the precise moment when data crosses a territorial boundary. Due to this difficulty, Kuner notes that some nations have applied their laws extraterritorially if the subject of the data in question is one of their nationals. Kuner provides a discussion on the conflict of laws involving transborder data flow regulation, and examines the extraterritorial application of the ‘fundamental rights’ law. Kuner notes that “transborder data flow regulation performs much the same function as applicable law rules; namely extending the protection of national law extraterritorially” (p. 141).

Kuner examines levels of compliance with regulations and informational requirements. He concludes with a broad overview of major trends and issues over the last several decades, and a discussion of the advantages and disadvantages to a legally pluralistic approach. He suggests ways in which regulatory frameworks can be improved, and ways of promoting interoperability of international laws and regulations. He notes that there is a need for jurisdictional restraint and greater acceptance of international values.

Kuner, C. (2011). ***Regulation of transborder data flows under data protection and privacy law: Past, present and future (OECD Digital Economy Paper No. 187).*** **Organisation for economic Co-operation and Development. http://dx.doi.org/10.1787/5kg0s2fk315f-en**

The author conducts a global survey of transborder data flow regulation. Kuner focuses on examining the rules relating to transborder data flows arising from data protection and privacy law, both in the public and private sectors. He examines international regulatory instruments such as the OECD Guidelines, the EU Data Protection Directive, and the Madrid Resolution. He also surveys “voluntary and private sector mechanisms” (p. 4) such as the APEC Privacy Framework, and practices such as binding corporate rules (BCRs) and contractual clauses. Kuner observes that regulation of transborder data flows is rooted in various cultural understandings and legal traditions. In some regions, data protection and privacy law take the form of legally-binding human rights instruments (eg. EU Directive). Elsewhere, regulations aim to enable the free flow of data, based on a recognition of the economic benefits of transborder data flows (eg. APEC Privacy Framework). Four motivations for the regulation of transborder data flows are identified: “preventing circumvention of national data protection and privacy laws; guarding against data processing risks in other countries; addressing difficulties in asserting data protection and privacy rights abroad; and enhancing the confidence of consumers and individuals” (p. 7). Kuner advocates for a recognition of both the benefits and risks of transborder data flows, both of which he outlines in the article (pp. 22, 24).

The author notes that there are two “default positions” found in regulations: one position assumes that data flows should be allowed but in certain circumstances should be regulated; while the other position assumes that transborder data flows should not be allowed without existing legal provisions for it. There are advantages and disadvantages to each approach, and many instruments show a combination of the two default approaches. Another distinction between regulations is that some are geographically based, while others operate on an accountability principle. For example, some regulations restrict the flow of data to foreign jurisdictions unless jurisdictions are deemed to provide ‘adequate’ data protection. The accountability principle puts the onus on organizations to prove that they comply with data protection regulations.

The regulation of transborder data flows supports the principles of data protection and privacy, but “is not itself a fundamental principle of the law” (p. 7). This type of regulation was first introduced to prevent circumvention of national data protection laws, but the reasons for such regulations have changed. While global harmonization of data protection and privacy law would reduce the need for regulation of transborder data flows, the likelihood of such an instrument being achieved is low, given the complexity and fractious nature of the current regulatory environment. Other highlights of the article include Kuner’s outline of the ways in which data processing has changed since the adoption of the OECD Guidelines in 1980 (p. 10-11), and his recommendations for the future (p. 26-30).

Marcinkowski, B. M. (2013). The second wave of global privacy protection: Privacy paradox(es): In search of a transatlantic data protection standard. *Ohio State Law Journal, 74*, 1167-1335.

This article seeks to provide an introduction to data protection standards. It provides a basic description of terminology, compares and contrasts American and European data protection standards, and highlights possible areas of convergence. At the core of the article, Marcinkowski argues that, despite many differences, the values that American and European data protection standards seek to protect are the same.

Marcinkowski notes that both the EU and the American models wish to become the global standard. In a comparison of the models, Marcinkowski highlights the fact that the EU standard is precise and specific, whereas the American model is flexible, based on principles of the self-regulating free market, and is segmented and sector-based. The author provides a detailed examination of the differences between the two models, and evaluates the advantages and disadvantages of both.

The article provides a discussion on the OECD guidelines and the HEW report, and provides a comparison table (p. 1180) of the principles established in both. Furthermore, Marcinkowski briefly discusses the North Atlantic Treaty. Marcinkowski highlights the emergence of two privacy paradoxes. He notes that both the US and the EU share a common values system but carry out privacy protection in two very different ways, and also notes that both systems are changing and becoming less rigidly defined, with aspects of one model blending into the other.

The author concludes by stating that the two models are diverging, yet highlights the need for transcontinental solutions. He suggests that standards be overseen by data protection authorities within existing administrative bodies, and that in the event of the unavailability of civil law measures, international FIPPs principles should apply.

Organization for Economic Co-operation and Development. (2013). ***OECD guidelines governing the protection of privacy and transborder flows of personal data (The OECD Privacy Framework).*** **Organization for Economic Co-operation and Development.**

This document outlines the Organization for Economic Co-operation and Development's guidelines for privacy and transborder data flow. The principles outlined in the Guidelines include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness principle, individual participation, and accountability. The first part of the package outlines the recommended guidelines and provides definitions. The Guidelines explicitly recognize that member nations have an interest in protecting privacy, but that the free flow of information can potentially have social and economic benefits. The Guidelines provide recommendations and invite the participation of non-member states.

Part three of the document addresses implementing accountability and outlines what should be included in a privacy management program. Part four discusses the free flow of information and legitimate restrictions, and notes that "a data controller remains accountable for personal data under its control without regard to the location of the data" (p. 16). Part five addresses national implementation and part six discusses international co-operation and interoperability.

The document discusses other recent privacy protection initiatives, including Binding Corporate Rules and the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System. The authors note that many of the current guidelines and legal instruments are being refined. The Guidelines address issues surrounding data security breaches, privacy enforcement authorities, and notes that data flows were less sophisticated in 1980 than they are today, which necessitated the revision. A further discussion on how the current revisions differ from the original 1980 Guidelines follows.

Parker, N. (2012). EU proposed data protection regulation: Less than adequate - cross-border data transfers under the proposed regulation. ***Allen & Overy LLP: In Focus*****, 1-8.**
http://hb.betterregulation.com/external/Less%20than%20adequate%20-%20cross-border%20data%20transfers%20under%20the%20proposed%20Regulation.pdf

The article provides a brief look at the proposed changes to the EU Data Protection Directive and addresses the adequacy principle. The authors proceed with a discussion on the most significant aspects of the proposed regulations and briefly examine the implications of these proposed changes. The authors also provide an overview of possible problems and note that while transborder data transfers are necessary for business, data is at risk every time it is transferred. While harmonization across member states is important, some nations oppose such measures because the laws may dilute their own national legislation. The authors examine the reform of conditions that must be met to prove adequacy and discuss the role of Binding Corporate Rules.

Finally, the article suggests that most people have a tendency to ignore the restrictions in whole or in part. While larger businesses will surely attempt compliance, smaller organizations may not be able to invest sufficient resources into meeting the requirements. While the authors acknowledge the positive changes made by the proposed updates to the Directive, they also note that the proposals do not achieve a serious overhaul that many people feel is necessary.

Poullet, Y. (2007). Transborder data flows and extraterritoriality: The European position. ***Journal of International Commercial Law and Technology, 2*****(3), 141-153.**

The purpose of this article is to highlight the impact of extraterritoriality and transborder data flows on the EU Directive on Data Protection (1995) and the Directive on Electronic Communications and Privacy (2002). According to the Council of Europe, human rights and the right to privacy are fundamental rights encompassing all personal data, including those of a public nature. TBDF takes place in two types of situations. The first type of situation occurs when the person or entity located in Europe exports data to a third country. According to the EU Data Protection Directive, EU member states must ensure that the country that processes data from the EU has an existing legislation that establishes the same equivalent of adequate data protection norms as the EU. Even though the EU Directive does not have an extraterritorial scope of application, the use of such a Directive provided a basis for countries like Canada to enact the Personal Information Protection and Electronic Documents Act. The second type of situation occurs when a data processor outside Europe manages to take control of the equipment in Europe without proper authorisation and, in the process, obtains the data of EU citizens. Such a situation can happen through the use of certain applications or with the use of cookies or spyware. The author concludes by recommending global norms for privacy to deal with transborder data flows, with the acknowledgement that privacy is dependent on the cultural and historical context of the society.

Svantesson, D. J. B. (2013). A 'layered approach' to the extraterritoriality of data privacy laws. *International Data Privacy Law, 3*(4), 278-286.

The author argues that while extraterritoriality in jurisdictional claims protects the citizens of nation states, a widespread extraterritorial application of state law may make it difficult for businesses to operate across borders. The authors highlight the problem that countries are either enacting or revising their data protection laws; however, these laws are introduced in isolation and in an uncoordinated manner. The author proposes the development of a layered approach to developing a model for extraterritoriality claims relating to privacy. The layers include abuse-prevention, rights and administration. The author argues that one limitation of this layered approach is that it splits human rights into "different levels of obligation" (p. 281).

Victor, J. M. (2013). The EU general data protection regulation: Toward a property regime for protecting data privacy. *Yale Law Journal*, *123*(2), 513-528.

The article examines the 2012 proposed updates to the EU Data Protection Directive and asserts that the Directive treats personal data as a commodity, or as property. It has been suggested that the proposed amendments may impede policymaking between the U.S. and the EU.

Treating data as property is achieved through granting individuals rights to their own data, by the fact that data “carries a burden that ‘runs with it’ and binds third parties, and through remedies grounded in “property rules” (p. 515). The article is divided into two sections; the first examines data privacy and property generally, and the second examines the draft regulation as a property regime. In Part One, Victor discusses at a very broad theoretical level the idea of data as a commodity, and examines the work of Lawrence Lessig, Paul Schwartz, Edward Janger, and Vera Bergelson. Victor discusses the advantages and disadvantages of viewing personal data as a commodity rather than as a fundamental right. Part Two examines various specific Articles of the proposed changes to the EU Data Protection Directive and describes how they demonstrate his assertions. Importantly, the proposed Regulations state that if data is a commodity that changes custody, the data subject or “owner” should have the ultimate right of erasure. Victor notes that, unlike physical property, data owners cannot forfeit their rights through contract, a move which is similar to the treatment of moral and intellectual rights. Finally, Victor examines remedies that would be allowable under the proposed Regulations if data owners found that their data was being treated in a manner with which they were unhappy.

Wiebe, A. (2015). Data protection and the internet: Irreconcilable opposites? The EU data protection reform package and CJEU case law. *Journal of Intellectual Property Law & Practice, 10*(1), 64-68.

This article begins by analyzing the Court of Justice of the European Union's (CJEU) ruling in *Google Spain and Google v AEPD*. The author discusses how data protection law is based on traditional categories of computer data-processing: storage, modification, transfer, blocking and deletion. The rest of the article focuses on user consent and the principle of "location" in section 1(5) of the German Federal Data Protection Act (BDSG). The principle of "location" includes both the location of the branch establishment and whether data-processing relates to the offering of goods and services to persons within the EU. Cloud computing is discussed in the context of draft legislation wherein non-EU providers would be required to appoint a company data protection officer, who in turn would be supervised by European authorities. The article criticizes CJEU's *Google Spain* ruling, citing the fact that the ruling risks creating an "EU internet," in light of the fact that there is no "global law" of the internet.

Cybercrime

Keeping records in the cloud 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).

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**

This report is an outcome of the work by the Transborder Group of the Cybercrime Convention Committee. The objective of the group is to examine challenges in investigating transborder criminal cases on the Internet, including regulating transborder search and seizure (p. 6). The report outlines a number of law enforcement challenges, including the use of cloud computing, which moves data among different jurisdictions at the same time, thus making it difficult for users and law enforcement officials to track criminal activities conducted remotely in a third state. Since data is not tied to a specific territory, law enforcement officials have difficulties in applying the principle of territoriality to conduct a search or to seize digital evidence. The report also highlights the difficulties service providers encounter due to conflicting national laws from various states. For example, French law prevents any person residing in France from sharing information that is "capable of harming the sovereignty, security or essential economic interests of France or contravening public policy" (p. 14). However, French service providers may receive court orders from other countries to reveal such information. The report raises questions regarding how the principle of territoriality is applied when no one knows where the data is physically stored and when there are multiple copies of data stored in different states, or when data is moved between different states. Data may also be compiled from various sources hosted or stored in different states.

The report proposes using the power of disposal, which links the data to 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" (p. 50). In other words, “if the location of the data is not known, but the person having the power of disposal of the data is physically on the territory of, or a national of the searching State, the LEA of this State may be able to search or otherwise access the data” (p. 50). Provisions could also be included under the Budapest Convention on Cybercrime to allow parties to access stored digital data for criminal investigations through "lawfully obtained credentials," through "good faith," and in urgent situations in order to "prevent imminent danger, physical harm, the escape of a suspect or similar" (p. 49).

Cybercrime Convention Committee (T-CY): Ad-hoc Sub-group on Jurisdiction and Transborder Access and Jurisdiction. (2013). ***Report of the transborder group 2013*** **No. T-CY (2013(30)). Strasbourg: Council of Europe. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2930_Final_transb_rep_V5.pdf**

The Transborder Group (full name: Ad-hoc Subgroup on Transborder Access and Jurisdiction) is a subcommittee of the Cybercrime Convention Committee (T-CY), established in 2011. The Group was tasked with producing an instrument to further regulate transborder data flows while facilitating transborder investigations for law enforcement authorities (LEA). The "Report of the Transborder Group for 2013" summarizes the activities of the Group in that year. The annual activities consisted of first steps towards implementing recommendations from a report submitted by them and adopted by the Committee in 2012, "Transborder access to data and jurisdiction: what are the options?"

The 2012 Report offered three recommendations. The first recommendation is for better implementation of the Convention on Cybercrime (also known as the Budapest Convention), which is a multilateral treaty that addresses the use of electronic evidence in cybercrime investigations and proceedings. The Convention encourages international cooperation in cybercrime investigations and enables government LEAs to share data through a combination of formal mutual assistance as well as expedited provisional measures to secure electronic evidence. The report noted that while there is an increased need for transborder access, the Convention has not been widely implemented amongst parties to the Convention. The second recommendation of the report is for the creation of a Guidance Note on Article 32 of the Convention on Cybercrime. Article 32 addresses transborder access to stored electronic information. The Guidance Note would provide clarification on Article 32b, which states that a party may: "access or receive, through a computer system in its territory, stored computer data located in another Party" with the "lawful and voluntary consent" of the relevant "lawful authority" (Convention on Cybercrime). As explained by the Transborder Group, "Article 32b is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual assistance under limited circumstances" (p. 9). The Guidance Note would facilitate and encourage implementation of Article 32b. The third recommendation of the report is for the establishment of an Additional Protocol to the Convention on Cybercrime, which would address specific situations outlined in its published list "Elements of a Protocol" (p. 11).

The 2013 activities of the group included working on a draft of the Guidance Notes and convening a Public Hearing in June 2013, attended by 35 representatives of private sector, civil society and academic entities, and 55 members, observer States, and organisations of the T-CY. The goal of the hearing was to identify solutions enabling transborder access to data, while at the same time articulating concerns regarding the rights of individuals and the protection of personal information. The hearing demonstrated that the issues are complex and disagreement exists between involved parties, with some believing that transborder access should not be allowed, and others emphasizing the need for transborder access due to technological changes and increased cybercrime. In 2014 and 2015, the Transborder Group will continue to take steps for implementation of the three recommendations of the 2012 report.

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.**

The National Institute of Standards and Technology (NIST) has drafted a guideline identifying 65 forensic challenges specific to cloud computing. The challenges are considered to be either “unique to” or “exacerbated by” cloud computing, and are grouped into three general categories encompassing technical, legal and organizational challenges. The NIST Cloud Computing Forensic Science Working Group (NCC FSWG) acknowledges that solutions cannot be developed in a single area, but must be cross-disciplinary. In particular, they point to technology- and standards-based approaches for addressing the issues. A taxonomy of nine categories identifying types of challenges are identified. A detailed table describing each challenge, along with any of the five relevant characteristics of cloud computing from which each challenge is derived (taken from the NIST cloud computing definition: on demand self-service, broad network access, resource pooling, rapid elasticity, measured service), and the relevant category of challenges is provided in Appendix B.

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**

According to the author, the main effect of cloud computing technology on cybercrime investigations is on the “acquisition of evidence” (p. 5). This is largely due to a “loss of location” of data, because, in a cloud computing environment, data is constantly being moved amongst different servers that may exist in different countries. Due to this inherent state of flux, including the movement of data across borders, even the cloud service provider may be unable to confirm where data stored in the cloud is located at a given moment. The loss of data location translates into an inability to determine the jurisdiction of data that law enforcement authorities (LEAs) need to access. The determination of jurisdiction is important because LEAs need to abide by the principle of "territorial sovereignty," according to which "no state may enforce its jurisdiction within the territory of another sovereign state" (p. 5).

Article 32 of the Budapest Convention on Cybercrime is one instrument that addresses the issue of location of data in cloud computing. Parties to the Convention agree to allow state authorities access to "stored computer data" regardless of where the data is located, so long as consent is given by the "lawful authority" with the right to "disclose the data" (p. 7). The latter can refer to a cloud service provider. However, there are two major limitations to Article 32: 1) the cloud service provider may decide to protect the privacy of its clients by not granting consent; and 2) the data itself may not be held in the territory of any party to the Convention. Moreover, Article 32 could be considered a "procedural error" because it may not be possible, as discussed earlier, to confirm the location of the data.

The question becomes not whether "a crime can be prosecuted within a certain country at all, but whether...certain procedural actions can be taken regardless of location" (p. 8). This eliminates the effects principle and "other factors used to prioritize conflicting jurisdictional claims" as "model[s]...for data in the clouds" (p. 8). The author eliminates the flag principle, which holds that "crimes committed on ships, aircraft and spacecraft are subject to the jurisdiction of the flag state, regardless of their location at the time of the crime" (p. 8). In summary, the flag principle does not adequately "circumvent the principle of territoriality to access data in the clouds" (p. 8). The author also dismisses the principle of nationality, which "uses the nationality of the perpetrator...to establish criminal jurisdiction" (p. 9). However, this is inadequate since a crime might have been committed by a foreign national. Moreover, "nationality is not a quality attributable to data;" instead, it is an individual that needs to be connected to the data in question, and therefore the nationality principle falls short (p. 9). The author concludes that the "power of disposal as a legal connecting factor" could address the problem, since it would "connect any data to the person or persons that obtain sole or collaborative access and that hold the right to alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever" (p. 10). However, the author does not define or explain the "power of disposal" principle and therefore the meaning of this principle remains unclear.

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/TCY 2012/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.